DERECHO DIGITAL APLICADO

2.0

2ª EDICIÓN (En Español)
REVISADA, ACTUALIZADA Y AMPLIADA

OBRA COLECTIVA

Autores: Patricia Peck Pinheiro, Leandro Bissoli, Sandra Paula Tomazi Weber, Márcio Mello Chaves, Milena Mendes Grado, Victor Auilo Haikal, Caroline Teófilo da Silva, Victor Varcelly Medeiros Farias, Luiz Philippe Moura, Aristides Tranquillini Neto, Rafael Mott Farah

Coordinadora de la Obra: Patricia Peck Pinheiro

El presente libro fue traducido del portugués al español con el apoyo y patrocinio de la FEDERACIÓN LATINOAMERICANA DE BANCOS (FELABAN) y de su Comité Latinoamericano de Derecho Financiero (COLADE).

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Las opiniones expresadas en el libro corresponden exclusivamente a sus autores y no comprometen a FELABAN ni a sus funcionarios, miembros o directivos.

INDICE DE LA OBRA

SOBRE LOS AUTORES

Dra. Patricia Peck Pinheiro

Formación: graduada de Derecho de la Universidad de Sao Paulo, donde es doctoranda en Derecho Internacional, investigadora invitada del Instituto Max Planck de Hamburgo y Múnich, investigadora invitada de la Universidad de Columbia NYC, profesora invitada de la Universidad de Coímbra. Posee formación en Gestión de Riesgos por la Fundación Dom Cabral, en Negocios por la *Harvard Business School* y en Inteligencia por la Escuela de Inteligencia del Ejército Brasileño. Programadora desde los 13 años, autodidacta en Basic, Cobol, C++, Html.
Carrera: Socia fundadora del Bufete Patricia Peck Pinheiro Advogados y de la empresa de cursos Patricia Peck Pinheiro Treinamentos.
Premios: Abogada Más Admirada en Propiedad Intelectual en 2010, 2011, 2012, 2013, 2014, 2015 y 2016; *Security Leaders* en 2012 y 2015; La Nata de los Profesionales de Seguridad de la Información en 2006 y 2008; Excelencia Académica – Mejor Docente de la Facultad FIT Impacta en 2009 y 2010.
Condecoraciones: Medalla del Pacificador otorgada por el Ejército en 2009, Medalla Tamandaré otorgada por la Marina en 2011, Medalla Orden del Mérito Militar otorgada por el Ejército en 2012.
Cargos: Árbitro del Consejo Arbitral del Estado de Sao Paulo – CAESP, Vicepresidente Jurídica de la Asociación Brasileña de los Profesionales y Empresas de Seguridad de la Información – ASEGI y profesora del postgrado en Gestión de la Innovación y Derecho Digital de la FIA.
Obras: Autora del libro Derecho Digital (6ta edición) y de más de 17 obras sobre Derecho y Tecnología.
Responsabilidad Social: Creadora del Instituto iStart.
Idiomas: Portugués (lengua materna), inglés (con fluidez), español (con fluidez) e italiano (básico).
Currículo Lattes: http://lattes.cnpq.br/0172053105577577
LinkedIn: https://br.linkedin.com/in/patriciapeckpinheiro

Dr. Leandro Bissoli

Formación: Abogado graduado de la Facultad de São Bernardo do Campo y con postgrado en Negociaciones Económicas Internacionales del Programa San Tiago Dantas. Posee especialización en Política Comercial Internacional por la Fundación

Getúlio Vargas y Cooperación Internacional para el Desarrollo por la Universidad de Sao Paulo.
Carrera: Socio director del Bufete Patricia Peck Pinheiro Advogados.
Certificaciones: *Sun Microsystems* en los cursos SL-110, SL-275, OO-226, SL-285 y SL-314; *ICS Professional* a través de *Impacta Certified Specialist*; *Cutting Edge Hacking Techniques* (GHTQ) y certificado por la *Global Information Assurance Certification* (GIAC), arquitectura y administración de bases de datos como MSSQL, MYSQL y ORACLE.
Cargos: Miembro de la HTCIA – *International High Technology Crime Investigation Association* y del Instituto Brasileño de Derecho Digital (IBDDIG), y profesor del postgrado en Gestión de la Innovación y Derecho Digital de la FIA.
Obras: coautor del audiolibro Elecciones Digitales y del libro Derecho Digital Aplicado.
Idiomas: Portugués (lengua materna) e inglés (nivel intermedio).
Currículo Lattes: http://lattes.cnpq.br/2474658806979652
LinkedIn: https://br.linkedin.com/in/leandro-bissoli-4538949

Dra. Sandra Paula Tomazi Weber

Formación: Graduada de Derecho de la Facultad de Derecho de Joinville, perteneciente a la ACE (Asociación Catarinense de Enseñanza), tiene postgrado en Derecho Contractual por la Pontificia Universidad Católica de Sao Paulo y en Derecho Civil y Empresarial por la Pontificia Universidad Católica de Paraná. Concluyó los cursos de extensión sobre Derecho de la Tecnología de la Información en la Fundación Getúlio Vargas de Río de Janeiro, y Contratos de Consumo y Actividad Económica en la Fundación Getúlio Vargas de Sao Paulo. También posee formación técnica en Informática por la Escuela Técnica Tupy.
Carrera: Socia del Bufete Patricia Peck Pinheiro Advogados.
Cargos: Miembro de la Comisión de Ciencia y Tecnología de la OAB/SP y del Instituto Brasileño de Derecho Digital (IBDDIG).
Obras: Coautora del libro Derecho Digital Aplicado, del audiolibro Derecho Digital Corporativo y de la compilación Derecho y Salud – 2012.
Idiomas: Portugués (lengua materna) e inglés (nivel básico).
Currículo Lattes: http://lattes.cnpq.br/1601203522999450
LinkedIn:https://br.linkedin.com/in/sandra-paula-tomazi-weber-17418792

Dr. Márcio Mello Chaves

Formación: Abogado formado en la Facultad de Derecho Milton Campos, con más de 15 años de experiencia jurídica en Sao Paulo, Río de Janeiro y Belo Horizonte. Máster en Propiedad Intelectual por la *World Intellectual Property Organization – WIPO Academy* (Ginebra) y *Università Degli Studi di Torino* (Turín). Posee curso de extensión en Derechos Autorales Avanzados en la *WIPO Academy*, en Derecho de los Medios en la Fundación Getúlio Vargas de Río de Janeiro y en Derecho de Informática en la Facultad Minera de Derecho de la PUC Minas.

Carrera: Socio director del Bufete Patricia Peck Pinheiro Advogados.

Cargos: Profesor en los cursos de postgrado de Seguridad de la Información del Centro Universitario UNA y de Gestión de la Innovación y Derecho Digital de la FIA. Vicepresidente de la Comisión de la Sociedad de la Información y Crímenes Electrónicos de la OAB/SP, miembro de la Comisión de Tecnología de la OAB/SP, del Capítulo Brasileño de la *Internet Society* - ISOC-Brasil, del Instituto Brasileño de Derecho Digital (IBDDIG), y del *Workgroup* de Formación de Líderes *Experts* en Ciberseguridad del "Cibermanifiesto: un Manifiesto por Cambios".

Obras: Coautor del libro "WIPO IP Research Papers" por la *World Intellectual Property Organization – WIPO Academy*, 2010.

Idiomas: Portugués (lengua materna), inglés (con fluidez), español (nivel intermedio) e italiano (nivel intermedio).

Currículo Lattes: http://lattes.cnpq.br/0553083517733293

LinkedIn: https://br.linkedin.com/in/marciomellochaves

Dra. Milena Mendes Grado

Formación: Abogada formada en la Pontificia Universidad Católica de Sao Paulo, con más de diez años de desempeño en las áreas de Derecho Público, Propiedad Intelectual y Medios y Entretenimiento. Con postgrado en Derecho Electoral por el Instituto Brasiliense de Derecho Público, en Derecho Procesal Civil por la FADISP y en Propiedad Intelectual por la Fundación Getúlio Vargas de Sao Paulo. Cursó también extensión universitaria en "Internet y Sociedad: Tecnologías y Políticas de Control" en la *Harvard Extension School* y en Propiedad Intelectual en la *World Intellectual Property Organization – WIPO Academy*.

Carrera: Socia del Bufete Patricia Peck Pinheiro Advogados.

Idiomas: Portugués (lengua materna) e inglés (con fluidez).

Currículo Lattes: http://lattes.cnpq.br/1556307696692580

LinkedIn: https://br.linkedin.com/in/milenagrado

Dr. Victor Auilo Haikal

Formación: Abogado graduado de la Universidad Presbiteriana Mackenzie. Maestrando en Derecho Civil en la Universidad de Sao Paulo y *Master of Science* en Seguridad Cibernética de la *University of Maryland University College*.

Carrera: Socio del Bufete Patricia Peck Pinheiro Advogados.

Cargos: Miembro de la Comisión de Ciencia y Tecnología de la OAB/SP y del Instituto Brasileño de Derecho Digital (IBDDIG) y profesor del postgrado en Gestión de la Innovación y Derecho Digital de la FIA.

Obras: Autor invitado de los libros Marco Civil de Internet, Derecho Digital Aplicado, RT 937 y RT 944.

Idiomas: Portugués (lengua materna), inglés (con fluidez) y español (con fluidez).

Currículo Lattes: http://lattes.cnpq.br/3873890089976773

LinkedIn: https://br.linkedin.com/in/victor-auilo-haikal-a4556226

Dra. Caroline Teófilo da Silva

Formación: Formada por el Centro Universitario FIEO, con más de seis años de experiencia en Seguridad de la Información, incluyendo el área financiera. Especialista en Derecho Empresarial por la Fundación Getúlio Vargas de Sao Paulo y certificada en *Information Security Foundation*, basada en la norma ISSO/IEC 27002 por la EXIN.

Carrera: Socia del Bufete Patricia Peck Pinheiro Advogados.

Cargos: Miembro de la Comisión de la Asociación Brasileña de Normas Técnicas (ABNT).

Idiomas: Portugués (lengua materna) e inglés (nivel avanzado).

Currículo Lattes: http://lattes.cnpq.br/4487508837710718

LinkedIn: https://br.linkedin.com/in/caroline-teofilo-da-silva-60238229

Dr. Victor Varcelly Medeiros Farias

Formación: Abogado formado por la Universidad Federal de Río Grande del Norte. Maestrando en Comunicación y Contemporaneidad de la Facultad Cásper Líbero y con postgrado en Derecho Digital Aplicado y en Mediación de Conflictos por la Fundación Getúlio Vargas de Sao Paulo.

Carrera: Socio Investigador de Patricia Peck Pinheiro Treinamentos.

Cargos: Miembro de la Comisión de Estudios de Medios y Entretenimiento del Instituto de los Abogados de Sao Paulo (IASP).

Idiomas: Portugués (lengua materna) e inglés (con fluidez).

Currículo Lattes: http://lattes.cnpq.br/3599267214342900

LinkedIn: https://br.linkedin.com/in/victorvarcelly

Dr. Luiz Philippe Moura

Formación: Abogado formado por la Universidad Presbiteriana Mackenzie. Con postgrado en Derecho Digital Aplicado por la Fundación Getúlio Vargas de Sao Paulo.
Carrera: Abogado especialista en Derecho Digital del Bufete Patricia Peck Pinheiro Advogados.
Idiomas: Portugués (lengua materna) e inglés (con fluidez).
Currículo Lattes: http://lattes.cnpq.br/7486759717976058
LinkedIn: https://br.linkedin.com/in/luiz-philippe-moura-a420b2a6

Dr. Aristides Tranquillini Neto

Formación: Graduado de la Pontificia Universidad Católica de Sao Paulo y con postgrado en Derecho Digital Aplicado en la Fundación Getúlio Vargas de Sao Paulo. Participó en el seminario "*Understanding U.S. Intellectual Property*" de la Universidad de Stanford y del curso de extensión "*Introduction to U.S. Legal System*" de la Universidad de Yale, además de los cursos online "*Internet Giants: The Law and Economics of Media Platforms*" de la Universidad de Chicago e "*Internet History, Technology and Security*" de la Universidad de Michigan.
Carrera: Abogado especialista en Derecho Digital del Bufete Patricia Peck Pinheiro Advogados.
Premios: Ganador de la "Mención Honorífica" de la Pontificia Universidad Católica de Sao Paulo con la monografía presentada, titulada "*Digital Rights Management e Fair Use*".
Obras: Publicación del artículo "*Digital Rights Management e Fair Use*" en la Revista de los Tribunales 966 y en la Revista de la ABPI. Coautor del capítulo brasileño del compendio "*World Intellectual Property Rights and Remedies – Laws with Commentary*" preparado por el *Center for International Legal Studies* y publicado por Thomson Reuters.
Idiomas: Portugués (lengua materna), inglés (con fluidez), español (nivel básico), alemán (nivel básico) y chino (nivel básico).
LinkedIn: https://www.linkedin.com/in/aristides-tranquillini-neto-2754b368

Dr. Rafael Mott Farah

Formación: Abogado formado por la Universidad Presbiteriana Mackenzie, con curso de extensión en Derecho Procesal Civil y especialista en Derecho Digital por la GVLaw – Fundación Getúlio Vargas.

Carrera: Abogado especialista en Derecho Digital del Bufete Patricia Peck Pinheiro Advogados.

Idiomas: Portugués (lengua materna), inglés (nivel avanzado) y español (nivel intermedio).

LinkedIn: https://www.linkedin.com/in/rafaelmfarah

PRESENTACION

Tenemos el gusto de poner a disposición de la comunidad financiera latinoamericana, la traducción del libro "Derecho Digital aplicado 2.0. ", obra colectiva coordinada por la doctora Patricia Peck, como un aporte a la literatura jurídica relacionada con los aspectos legales del mundo digital, tema crucial para la banca de la región en el actual entorno competitivo y de negocios.

Uno de los mayores desafíos que enfrenta la banca de la región en la actualidad, es pasar de la banca tradicional a la banca digital integral, por lo cual el derecho tiene el enorme reto de acompañar adecuadamente este trascendental proceso.

En este entorno, es imprescindible para los juristas de hoy estar permanentemente actualizados sobre esta temática, a lo cual esta obra, sin duda, contribuirá de forma importante.

Agradecemos a la doctora Patricia Peck y a los demás autores del libro por esta valiosa contribución académica. Así mismo, agradecemos a nuestro Comité Latinoamericano de Derecho Financiero y a su Junta Directiva conformada por los doctores Jorge Alvarado, Presidente, Ricardo Carbonell, Primer Vicepresidente y Belisario Castillo, Segundo Vicepresidente, impulsores de esta iniciativa.

Los invitamos pues, a consultar el libro "Derecho Digital aplicado 2.0. ", esperando que el mismo les sea de utilidad como material de estudio y actualización jurídica.

GIORGIO TRETTENERO CASTRO
Secretario General
FEDERACION LATINOMERICANA DE BANCOS – FELABAN
Bogotá, Noviembre 2017

AGRADECIMIENTOS

El Derecho Digital en Brasil viene desarrollándose y madurando desde inicio de los años 90, cuando comenzaron a surgir las primeras obras sobre el tema en portugués, la mayoría aún en recintos académicos. Por ello, primeramente, me gustaría agradecer a todos los jóvenes alumnos que están en las facultades de derecho del país investigando los temas que conectan al derecho con la tecnología a través del cambio de comportamiento y del modelo socioeconómico de la sociedad actual.

Agradezco a la Federación Latinoamericana de Bancos, FELABAN, en las personas de su Presidente Dr. José Manuel López Valdés, de su Secretario General, Dr. Giorgio Trettenero Castro y de su Directora Jurídica Dra. Claudia Díaz-Granados Ortiz, a los miembros del Comité Latinoamericano de Derecho Financiero, COLADE y especialmente el apoyo del doctor Ricardo Carbonell por haber viabilizado el proyecto de traducción de esta obra al español, para que podamos compartir el conocimiento sobre el Derecho Digital aplicado al Mercado Financiero con todos los colegas de América Latina. Ya hacía algunos años que en nuestros encuentros en los eventos anuales de FELABAN hablábamos del anhelo de tener una obra en español y este sueño fue realizado a partir de esta iniciativa y de su incansable colaboración.

Aprovecho para hacer un especial agradecimiento al ilustrísimo amigo, profesor Dr. Coriolano Almeida Camargo, Presidente de la Comisión de Derecho Digital y *Compliance* de la OAB-SP y profesor del centro Damásio Educacional, que mucho nos honró haciendo el prefacio de esta obra.

Aprovecho, también, para agradecer a mis socios y demás abogados integrantes y a los que en algún momento ya integraron el cuerpo jurídico

del bufete, por mantener la disciplina de escribir y compartir el conocimiento aprendido, con especial mención a los Doctores Leandro Bissoli, Sandra Paula Tomazi Weber, Victor Auilo Haikal, Márcio Mello Chaves, Caroline Teófilo da Silva, Milena Mendes Grado, Aristides Tranquillini Neto, Rafael Mott Farah, Luiz Philippe Moura y Victor Varcelly Medeiros Farias.

Esta publicación es una forma de reconocer la dedicación y el trabajo de todos los que piensan el Derecho Digital, que dirigen sus esfuerzos a crear soluciones muchas veces inéditas, abordando una realidad disruptiva y cambiante, compuesta por fronteras informacionales y activos intangibles. Es un contexto social extremadamente desafiante, donde todo está interconectado, exigiendo creatividad, osadía y visión crítica.

No fueron pocos los cambios en este período, que exigen cada vez más multidisciplinariedad y transversalidad a los profesionales. Agradecemos el empeño diario y continuo de nuestro equipo, que además de la actualización técnica y jurídica, lleva adelante la premisa de compartir el conocimiento a partir de la elaboración e intercambio de contenidos que reúnen reflexiones y experiencias vividas en la aplicación del Derecho Digital.

Agradecemos, también, a todos nuestros clientes por los comentarios, cuestionamientos, sugerencias e indagaciones durante reuniones, así como a nuestros alumnos de clases, eventos y conferencias, y a todos los seguidores que tenemos en las redes sociales, por todas las interacciones recibidas y que hoy se configuran como un importante *feedback* en este pensar jurídico de las nuevas relaciones cada vez más digitales.

También recordamos el empeño de nuestra periodista Priscilla Auilo Haikal, que trabajó en la selección del material y en la revisión editorial de esta obra, así como en la adaptación al español, de conjunto con nuestro traductor Yadir González Hernández, cuyos aportes fueron esenciales para viabilizar esta edición especial en español.

Por último, por su importante y fundamental cooperación, que fue esencial para hacer viable este proyecto, agradecemos a Thomson Reuters, editorial que nos apoyó de manera incondicional para la publicación de este libro, y que autorizó la traducción al español de este proyecto en colaboración con FELABAN.

Dra. Patricia Peck Pinheiro
PhD Derecho Digital y Propiedad Intelectual
Universidad de Sao Paulo
Columbia University
Max Planck Institute

PREFACIO

Economía Digital. Fundamentos jurídicos y modelos de negocios en Internet. _Disruptiva. Informatizada. Cibernética. Digital. Son muchos los adjetivos que intentan contemplar las características de la realidad actual. No es nada simple intentar definirla, ya que los avances tecnológicos son constantes y provocan transformaciones continuas. Imagine entonces cuán desafiante es regular ese contexto innovador y cambiante que deconstruye una serie de paradigmas y pone en jaque una estructura consolidada a lo largo de muchos años.

Por la lectura de la obra, me parece que fue este el núcleo de la propuesta capitaneada por la Abogada Patricia Peck Pinheiro y su equipo. No es tarea fácil. En Estados Unidos, el tribunal de Apelaciones del Distrito de Columbia acaba de decidir que el suministro de Internet de banda ancha puede ser definido como un servicio público y no como una mercancía común.

Es notorio el impacto de la tecnología en la economía. Nuevos modelos de negocio han sido creados, generando embates en todos los sectores de actividad, incurriendo en la ponderación de principios y garantías constitucionales como la libre iniciativa y la libre competencia. En la mayoría de los sectores económicos (incluyendo el financiero, el minorista, el de bienes de consumo, entre otros) predomina la migración del punto de venta y de relación con clientes hacia plataformas on-line y de *e-commerce*. Podemos considerar el conocimiento Jurídico, sentido ético aliado a otras certificaciones y cursos web como la gran tendencia. Temas igualmente abordados en esta Obra.

Siendo así, es imprescindible analizar el contexto histórico, técnico y jurídico para que se entienda los rumbos que cada país ha tomado ante el surgimiento de nuevos productos y servicios tecnológicos y los respectivos impactos en la sociedad y en el mercado.

Se cita, como ejemplo, los estudios y los respectivos fines involucrando *big data* e inteligencia artificial*,* los que generan consecuencias, aunque

indirectas, para todos los individuos en términos de salud, patrones de consumo, publicidad, marketing, política y protección de datos[1].

Para comprender la amplitud de esa nueva realidad, se debe entender el surgimiento de las grandes compañías, como Microsoft, IBM e Intel, así como el de los procesadores y semiconductores, la capacidad de almacenamiento de los *hardwares* y la llamada Ley de Moore.

Concomitantemente, se observan diversas discusiones que involucran al ramo de las telecomunicaciones y de internet. Es el caso de WhatsApp y otros servicios de VoIP (*Voice Over Internet Protocol*); de los servicios llamados OTTs (*Over The Top*), como Netflix; o, el acceso a internet. Además, los embates sobre Uber y la nueva categoría de taxis; propiedad intelectual (marcas – links patrocinados y nombres de dominio – y, patentes); y, los proveedores (responsabilidad civil, hospedaje de servidores).

Lawrence Lessig, eximio investigador y profesor de la Universidad de Harvard, en aquella época, docente de la Universidad de Stanford, elaboró un dictamen, el cual fue anexado a los autos del proceso en que figuraba como parte Napster Inc., listando tres pruebas a ser realizadas por el magistrado que se deparase con un caso que involucrase el uso de una nueva tecnología, siendo:

- Potencial uso lícito de la tecnología;
- Proporcionalidad entre las pretensiones de las partes;
- Eficacia del recurso jurisdiccional.

A pesar de que el caso "Naspter" versase sobre derechos autorales, es interesante notar cómo la referida prueba puede ser aplicada en caso de análisis sobre la viabilidad de nuevos servicios y productos tecnológicos.

Por último, no menos importante, se destaca el debate propuesto en el Libro, que intentó traer las principales discusiones de la actualidad instauradas en la estructura organizacional de gobernanza de internet en el mundo en el ámbito del ISOC, IETF, ICANN, entre otros, así como en Brasil (LACNIC, CGI.Br), teniendo en cuenta que sus resoluciones y

[1]Harvard Gazette. Big data, massive potential. Disponible en: [http://news.harvard.edu/gazette/story/2015/10/big-data-massive-potential/?utm_source=facebook&utm_medium=social&utm_campaign=hu-facebook-general].

dictámenes influyen directamente en la expansión de internet, en términos técnicos, jurídicos y económicos.

El Derecho Digital es uno de los resultados de ese nuevo escenario, al representar la evolución del propio Derecho, introduciendo nuevos institutos y elementos para el pensamiento jurídico, como un eslabón entre innovación y gestión de riesgo.

Pasados casi 15 años del lanzamiento de la obra homónima de la Dra. Patricia Peck Pinheiro, incontables prácticas se extinguieron, otras numerosas surgieron, y en la era post-internet los datos son la moneda de cambio, nuestras identidades se extendieron al ambiente digital y muchos de los riesgos vienen en forma de código binario. Tal fluidez exige más formación en Ética y Seguridad en el mundo cibernético, no solamente para determinados profesionales, sino para todos los ciudadanos digitales que actualmente pasan la mayor parte de las horas conectados.

El objetivo de la Obra y del equipo del PPP Advogados es el de diseminar la cultura del Derecho Digital y el conocimiento. En tal dirección, el bufete PPP Advogados lanza su segundo libro de artículos, todos elaborados por el equipo de investigadores en el campo del Derecho Digital. La obra trae a colación temas que provocaron gran reflexión y repercusión en el área en los últimos tiempos, desde la inserción de las nuevas tecnologías en el ambiente corporativo, pasando por la entrada en vigor del Marco Civil de Internet, hasta casos de relevancia internacional como ciberterrorismo y espionaje digital.

La importancia de este trabajo se origina del hecho de que la sustentabilidad de la Sociedad Digital sólo será garantizada por medio de la educación. En la era del tiempo real, en la cual los contenidos se perpetúan con facilidad y los daños son catastróficos desde el punto de vista social, lo ideal es invertir en la prevención de los incidentes y valorizar la diseminación de contenidos legales, constructivos y auténticos, contribuyendo así a la formación de usuarios conscientes y

ciudadanos preparados para esta coyuntura cada vez más disruptiva, en la cual el conocimiento se mantiene como uno de nuestros activos más valiosos.

Coriolano Aurélio de Almeida Camargo Santos Ph.D.

Abogado. Director Titular Adjunto del Departamento Jurídico de la FIESP. Consejero electo a nivel de estado de la OAB/SP (2013/2018). Presidente de la Comisión de Derecho Digital y *Compliance* de la OAB/SP. Máster en Derecho en la Sociedad de la Información y certificación internacional de "The High Technology Crime Investigation Association (HTCIA)". Doctor en Derecho con certificado internacional en Derecho Digital por el *Caldwell Community College and Technical Institute*. Profesor y Coordinador Nacional del Programa de Postgrado en Derecho Digital y *Compliance* de la Facultad Damásio. Profesor invitado de los cursos de Postgrado de la USP/PECE, Fundación Instituto de Administración, Universidad Mackenzie, Escuela de Hacienda del Gobierno del Estado de Sao Paulo Fazesp, Acadepol-SP, EMAG y otras. Desde 2005 ocupa el cargo de Juez del Egregio Tribunal de Impuestos y Tasas del Estado de Sao Paulo.

CAPÍTULO PRIMERO

NUEVAS TECNOLOGÍAS EN EL AMBIENTE CORPORATIVO

LA SEGURIDAD DE LA INFORMACIÓN EN EL USO DE APLICACIONES DE INTERCAMBIO DE MENSAJES

Caroline Teófilo da Silva

Las aplicaciones que posibilitan el intercambio de mensajes de manera instantánea por medio del uso de internet son la nueva tendencia de la comunicación. Ejemplos como WhatsApp, Snapchat, Chaton, Telegram y Viber impulsan cada vez más el uso de esos softwares en detrimento del otrora célebre SMS.

Definitivamente, *¡la moda gustó!* Y no sin motivos, después de todo, esos softwares permiten, además del envío y recibimiento de mensajes ilimitados por medio del acceso a internet, el intercambio de archivos, fotos y la creación de grupos que facilitan la conversación con los contactos de la agenda que también descargaron la aplicación.

Los beneficios son muchos y van más allá de la economía financiera. Sin embargo, de la misma forma que gran parte de las otras tecnologías que ya surgieron, *las aplicaciones de intercambio de mensajes invadieron el ámbito corporativo*. ¿O no tienes a ningún compañero de trabajo en tu WhatsApp? Y, aun sin querer, asuntos profesionales también *demandarán tu atención* en esos ambientes.

Pero no todo es flores. Las aplicaciones *de moda* pueden ocasionar filtraciones de información, impedir la concentración durante el trabajo o dificultar el *networking* presencial y el trabajo en equipo.

El argot *Lea los Términos de Uso* surge como una alerta en nuestras relaciones digitales-presenciales, o simplemente relaciones.

Los Términos de Servicio y Aviso de Privacidad[2] del propio WhatsApp son claros al alertar que utilizan protecciones físicas, gerenciales y técnicas razonables para preservar la integridad y la seguridad de las informaciones, no obstante, *no pueden garantizar la seguridad de cualquier información transmitida.*

Los mismos documentos afirman también, específicamente para los usuarios internacionales, que WhatsApp está en California (EUA). *Por eso, al utilizar el servicio, el usuario está transfiriendo sus informaciones personales hacia allí y será regido por las leyes del Estado norteamericano.*

Existe además la restricción en cuanto al uso de contenidos protegidos por derechos autorales, por secreto comercial o de propiedad de terceros. Sin embargo, tal limitación es sólo para el contenido publicado en el Estado o de acuerdo con el término *Status Submissions*.

Ante lo expuesto, la preocupación con los términos y políticas de los servicios que utilizamos es primordial, *principalmente con la gran probabilidad de que el uso sea, en algún momento, para finalidad profesional.*

[2] Disponible en: [www.whatsapp.com/legal/?l=pt_br]. Acceso el: 08.04.2014, a las 11 h 59 min.

Para disminuir el riesgo y capacitar a los empleados, *las empresas necesitan tener reglas claras sobre el uso de aplicaciones para intercambio de mensajes.*

Inicialmente, es esencial establecer qué tipos de información pueden ser compartidas, por ejemplo, datos secretos o confidenciales no deben ser transmitidos por aplicaciones de esa naturaleza. Así, no es recomendable utilizar WhatsApp para tratar de proyectos que aún no fueron lanzados al mercado, para expresar opiniones personales sobre clientes o demás colegas de trabajo e incluso para, en el grupo de su área, comentar sobre su gestor.

La regla de oro es: asuntos secretos y comentarios que identifiquen o califiquen proyectos, clientes o prestadores de servicios no deben ser tratados por esas aplicaciones y, al compartir asuntos profesionales, el respeto a la ética y a la legislación vigente en Brasil es esencial.

¿La recomendación para el uso de contraseña? También la vemos aquí. Por tanto, además del bloqueo automático del aparato tecnológico, pueden ser utilizados softwares de protección que permiten el acceso a las aplicaciones solamente con el uso de contraseña y posibilitan el borrado remoto del contenido en caso de pérdida, hurto o robo del dispositivo.

¡Es esencial que el usuario realice periódicamente el backup de los mensajes corporativos enviando las conversaciones a las direcciones electrónicas de la empresa y, enseguida, borre el contenido!

Cuidados con intentos de ingeniería social también son importantes. En ese caso, el usuario debe siempre confirmar la identidad de la otra parte y si existe necesidad de compartir la información.

Es importante que el usuario esté atento a si la persona con quien está hablando es realmente su gestor o colega de trabajo. Después de todo, ¿cuántos casos no vemos de hurto de celular en que el criminal publica hasta foto en el Facebook de la víctima? ¿Por qué motivo no interactuaría por WhatsApp?

A continuación, describimos algunas reglas simples que pueden incorporar las normativas y evitar problemas:

- Respete la moral, la ética y la legislación de Brasil, la privacidad de terceros y los derechos autorales. No comparta mensajes, fotos o videos con contenidos pornográficos, racistas o prejuiciosos ni ofenda o humille a otras personas;

- Tenga cuidado con contenidos publicados en los grupos, estos pueden ser replicados y retransmitidos por los demás usuarios;

- Use softwares de protección, como antivirus y *firewall*, en el dispositivo;

- Evite dar clic en enlaces desconocidos que pueden contener softwares maliciosos o redireccionar al usuario hacia sitios que permitan el acceso a sus informaciones;

- Atención con las conexiones públicas, en general, estas no ofrecen protección para las informaciones facilitadas.

Por último, resaltamos la importancia de que las empresas estén atentas a sus normativas internas, *elaborando una Norma específica para el uso de aplicaciones de comunicación*, de acuerdo con las recomendaciones contenidas en este artículo, actualizando la Política de Seguridad de la

Información y demás documentos, además de capacitar constantemente a sus empleados.

La tecnología está ahí para todos y es inevitable. ¡Es mejor reglamentarla que ni siquiera mencionarla!

CÓMO PROTEGER LA IMAGEN DEL ALTO EJECUTIVO EN LAS REDES SOCIALES

Patricia Peck Pinheiro

Es cada vez más difícil lidiar con los nuevos tipos de crisis de imagen corporativa. Las redes sociales trajeron una nueva forma de exposición de las Marcas que puede generar impactos directos en la reputación y en el valor de las acciones de la empresa en el mercado.

¿Qué se puede hacer para blindar al más alto nivel ejecutivo y evitar que eso afecte no sólo la empresa, sino también la vida personal del líder empresarial?

Ser el CEO de una empresa o pasar a integrar el *board* del más alto nivel ejecutivo es una actividad que somete al individuo a una gran exposición. La identidad del líder muchas veces se confunde con la identidad de la propia corporación que este comanda.

Pero, en la era de las redes sociales, desde el consumidor hasta el empleado, pasando incluso por el entorno familiar, todos pueden de alguna manera afectar la imagen del CEO en la web y generar efectos negativos para los negocios.

Después de un evento empresarial, el vicepresidente de una compañía fue fotografiado en la piscina del hotel por su esposa, que publicó la imagen en Facebook. La repercusión fue tal, debido al hecho de que el

jefazo se estaba divirtiendo, sosteniendo un vaso de caipiriña apoyado en la barriga, que el ejecutivo fue separado del cargo.

Fotos y videos con escenas en momentos de esparcimiento que puedan generar una connotación de que la jefatura está ausente divirtiéndose, o incluso con demostraciones excesivas de la vida íntima, como partes del cuerpo apareciendo o algún tipo de desnudo, son las que más aterrorizan a las compañías y a sus departamentos de Relaciones con Inversionistas (RI) y de Comunicación y Marketing.

Fue lo que sucedió con un médico que estaba en una parrillada de domingo. Fue fotografiado por un pariente que compartió la foto por WhatsApp con otras personas y la imagen terminó circulando por internet.

El problema es que se trataba del jefe responsable del cuerpo de guardia de un gran hospital y la foto probaba que el profesional no estaba donde debería en aquel momento, impactando incluso la imagen de la institución, que sufrió comentarios de pacientes que esperaban en la fila de urgencias para ser atendidos.

Comentarios desastrosos de opinión personal publicados en Twitter o incluso en LinkedIn también generan crisis de imagen digital a las grandes empresas.

Está siendo necesario dar un entrenamiento a la alta dirección sobre cómo redactar mensajes electrónicos corporativos y cómo practicar su libertad de expresión sin afectar a la empresa que él mismo representa.

No es tarea fácil, pues este tipo de *coaching legal* va mucho más allá de las actividades de *media training*, comunes para quien asume un cargo de mayor relevancia en el mundo corporativo.

Existe la necesidad de orientar también a la primera línea de quien convive con el ejecutivo, lo que incluye a personas cercanas, incluso familiares, pues sus comentarios y publicaciones pueden afectar directamente la imagen del gestor.

Hay situaciones de riesgo diversas que deben ser debidamente tratadas y evitadas. Como cuando los hijos publican en las redes sociales fotos de los bienes y de la riqueza de la familia (casa, carros y viajes) o cuando detallan la rutina de los padres, contando a qué hora salen para el trabajo, cuándo llegan, si están ausentes, sus trayectos y hasta cuáles son los proyectos en que están involucrados.

A pesar de parecer inofensivos en un primer momento, comentarios como: "Mi papá está en un proyecto súper confidencial, va a quedarse una semana en la casa matriz en Alemania." pueden tener consecuencias desastrosas.

Ahí no queda la cosa. Es frecuente la filtración de asuntos discutidos en casa e informaciones confidenciales son cada vez más públicas en internet. Es un *big data de ejecutivos*, que alimenta desde secuestradores hasta el espionaje electrónico entre empresas.

En Europa, no sólo ejecutivos, sino científicos e investigadores, han sido orientados respecto a qué compartir o no en sus perfiles personales en las redes sociales. Dependiendo del caso, implica hasta una cuestión de soberanía y seguridad nacional. Pero el europeo, a diferencia del brasileño, posee una cultura de exponerse menos en las redes.

Entonces, ¿cómo prevenir ese tipo de exposición de imagen en los medios digitales y qué hacer cuando ocurre? A continuación, damos algunas orientaciones prácticas.

Primer consejo: capacitar a las personas sobre protección de privacidad en los medios digitales.

La alta dirección debe ser blindada, lo que significa controlar lo que es publicado respecto a ella, incluso por familiares.

Un CEO es una persona pública y debe tener todos los cuidados asociados a su tipo de cargo para evitar impactos negativos. En la actual era de la Sociedad Abierta, transparente y en tiempo real, su vida personal se encuentra mucho más expuesta, y mucho más vigilada por todos, desde el cliente hasta la competencia.

Segundo consejo: se debe tener mucho cuidado en la generación e intercambio de imágenes, sea por medio de WhatsApp o de las redes sociales.

Como es casi imposible suprimir contenido de internet, muchas veces la mejor opción es no crearlo, evitando arrepentimientos en caso de que su compartición se salga de control.

Ante la duda, el ejecutivo debe mantenerse alejado de fotos y grabaciones, aún en eventos corporativos, pues las imágenes amateurs producidas por el propio equipo pueden ser demasiado comprometedoras.

Tercer consejo: monitorear siempre la reputación digital para evitar exceso de exposición en la web.

Debe ser hecho un escaneo periódico en los buscadores sobre lo que está apareciendo respecto a los ejecutivos de primer nivel, incluso en sus perfiles personales y de familiares próximos.

Ya no se trata solamente de buscar lo que está asociado directamente a la marca de la empresa, sino a las identidades de las personas físicas que pueden afectar a la persona jurídica.

Cuarto consejo: planear la publicación de contenidos con textos revisados y atención especial al tono y al tipo de lenguaje.

Esto no sólo se aplica al perfil y a la *fanpage* oficial de la empresa, sino también y sobre todo a los perfiles personales de su alta dirección.

El uso de palabras en diminutivo o incluso de saludos más íntimos como *besos* pueden generar mucho revuelo. Así como algunas manifestaciones acaloradas relacionadas al equipo de fútbol favorito o una opinión personal sobre un aspecto referente a la agenda política.

Aun cuando el ejecutivo manifiesta una opinión sobre otra marca, desde un banco hasta un seguro médico, el comentario estremece las relaciones institucionales entre las empresas.

Quinto consejo: reaccionar rápido a los incidentes de crisis de imagen digital.

Cuanto más rápido pueda ser publicada una información positiva para diluir la negativa, mejor. La respuesta a una foto no autorizada es publicar varias fotos autorizadas, a un rumor falso es distribuir información verdadera de forma rápida y transparente.

Es necesario combatir la información con más información. Demorar en la respuesta o abstenerse de responder pueden agravar el problema. El silencio sólo impulsa la diseminación del contenido y empeora aún más la situación para la reputación corporativa.

Sexto consejo: no personalizar las críticas.

Todo CEO o alto ejecutivo tiene que ser entrenado para no tomar personalmente cualquier comentario por más incisivo, ridiculizante o difamatorio que pueda recibir por motivo de su cargo o función. Forma parte de ser una personalidad pública.

Por eso, nunca debe responder de forma inmediata, sin pensar, sin planear, al calor de la emoción. Su respuesta tiene que ser rápida, pero planeada, pues su respuesta es también la respuesta de la compañía.

La mejor estrategia es preparar una lista de frases legalmente apropiadas para responder a esas situaciones, pues muchas se producen los fines de semana o por la noche, justamente cuando el Presidente no está con su equipo de asesores jurídicos y de comunicación para orientarlo sobre qué hacer.

Como quedarse desconectado no es una opción en la era de las redes sociales, es necesario cautela con lo que es publicado, ya que la ley del Marco Civil de Internet privilegia la libertad de expresión y dificulta la supresión de contenido, exigiendo una orden judicial para prácticamente todo. Definitivamente, los ejecutivos tendrán que controlar cada vez más el entusiasmo. Comentario publicado sin haber sido bien pensado genera perjuicio para la empresa.

Por último, es esencial contar con un especialista en Derecho Digital que sepa qué hacer para eliminar el contenido lo más rápido posible, y así apoyar a la presidencia y el área de comunicación institucional, marketing, relaciones con inversionistas y relaciones públicas y gubernamentales.

En una era de más libertad, en un mundo plano, sin fronteras, pero viviendo en un país aún con poca educación sobre el uso responsable, ético, legal, seguro y saludable de la tecnología, tendremos mucho trabajo por delante para proteger la imagen de los ejecutivos y de las empresas.

¡Es indispensable realizar un trabajo estratégico y preventivo con la alta directiva para evitar que los sinsabores de la web determinen el sube y baja de las acciones en la bolsa de valores! Como están las cosas, no hay corazón ni bolsillo que aguante.

¿EXISTE RIESGO JURÍDICO EN LA MOVILIDAD CORPORATIVA CON EL USO DE RECURSOS PARTICULARES?

Luiz Philippe Moura

El escenario actual de la sociedad está intensamente permeado por el uso de dispositivos electrónicos para la interacción, comunicación e intercambio de informaciones con alta velocidad entre personas de las más diversas clases, etnias, edades, culturas e inclusive filosofías.

Como consecuencia de esa profunda inmersión tecnológica social en el espacio democrático digital, la incorporación de la movilidad para la realización de actividades profesionales se hizo realidad en los más diversos entornos corporativos.

Las características espaciales y temporales del trabajo fueron ampliamente modificadas, incorporando o remodelando la identidad personal, profesional, cultural, social o política de los individuos como consecuencia de la movilidad.

Los profesionales de este milenio tienen la posibilidad de utilizar dispositivos móviles particulares (*Bring Your Own Device – BYOD)* y/o corporativos para ejercer sus actividades laborales, enteramente conectados con la empresa por medios digitales.

El principal desafío de las empresas ante esta conducta corporativa digital es establecer límites que separen lo que es profesional de lo que es personal, de forma que se prevenga al máximo la filtración de informaciones y que se brinde seguridad jurídica para todos los implicados, garantizando la integridad y protección de los datos corporativos.

En una investigación reciente, Symantec con el Ponemon Institute[3] señaló que la suma de los gastos de empresas brasileñas derivados de la filtración de informaciones llegó a casi 10 millones de reales en 2013.

Según el estudio, las amenazas cibernéticas son consecuencia de ataques externos (*outsiders)* o de la negligencia de los propios empleados (*insiders)*. En ambos casos, el resultado es la filtración de contratos, informes, planeamientos, presentaciones y diversos datos confidenciales y estratégicos que son colocados ilegalmente en Internet, comprometiendo las políticas comerciales de la empresa, su imagen y reputación en el mercado y ante la competencia.

Es incuestionable el poder de ataque de *hackers, crackers* y *attackers*, que son implacables y hasta insuperables en la sofisticación de estafas a las organizaciones mundiales, más aún con el surgimiento de la *deep web* y de las diversas formas de enmascaramiento de datos de origen de acceso.

[3] Disponible en: [www.symantec.com/pt/br/security_response/publications/threatreport.jsp]. Acceso en: 02.08.2016, a las 11 h 25 min.

Del otro lado, en la lucha contra el *cyber crime*, existen diversos órganos internacionales y empresas privadas de *cyber security*, como McAfee y Symantec, que trabajan diariamente en el combate a las vulnerabilidades tecnológicas, rastreando amenazas y creando vacunas digitales contra los incontables males cibernéticos.

Sin embargo, una de las grandes vulnerabilidades que puede aumentar el riesgo de filtración de informaciones corporativas se deriva de la diversa gama de dispositivos móviles particulares que actualmente interactúan con el entorno lógico corporativo.

Esa diversidad de aparatos, asociada a un comportamiento negligente en la aplicación de medidas de protección en equipos personales, deja el escenario extremadamente favorable a amenazas. Basta un simple sondeo de concientización de seguridad para identificar que la mayoría de los profesionales, que conocen las reglas de protección de los equipos corporativos, tales como el uso de contraseñas y antivirus, no las aplica cuando el dispositivo es particular, aun conteniendo éste informaciones de la empresa.

En Brasil, al Poder Judicial le tomó más de 10 años que se entendiese que el empleador puede monitorear los recursos e informaciones corporativas que sean de acceso y uso de los empleados, debiendo hacer un aviso previo para ello, a fin de evitar que el empleado exponga su intimidad en esos ambientes por desconocer que existe la vigilancia del patrón.

Y, ¿cuándo el recurso a ser monitoreado no es de propiedad de la empresa, sino del empleado? ¿Cómo implantar la movilidad corporativa en ese escenario híbrido y complejo de modo que se eviten riesgos de seguridad de la información y de violación de privacidad por acceso a datos personales del individuo?

Es válido mencionar, en ese punto, que las relaciones de trabajo son formadas por dos sujetos, el empleador, que tiene el poder de dirigir, organizar y fiscalizar la prestación del servicio, llamado poder directivo, según el art. 2.º, de la CLT, y el empleado que tiene el deber de cumplir con las reglas de trabajo.

No obstante, el poder directivo no es absoluto o ilimitado, después de todo, la Constitución Federal resguarda los derechos de los empleados e igualmente tutela la autonomía directiva del empleador, de forma que se cohíba conductas del empleador nocivas a la libertad y a la dignidad de la persona natural del empleado, que serían consideradas abuso de poder patronal.

Es oportuno subrayar que el empleador posee la facultad de permitir o no el uso de dispositivos personales en el entorno laboral, así como los empleados poseen el derecho de decidir sobre utilizar o no dispositivos móviles particulares para el ejercicio de sus actividades profesionales.

Claro que, si el uso del equipo propio es requisito de la plaza (cargo o función) preestablecido (como cuando se exige un vendedor con carro propio, por ejemplo, por analogía hoy sería con celular propio), esta facultad del empleado deja de existir (lo que ya ocurre en Estados Unidos, donde las reglas de BYOD son requisitos contractuales de trabajo en algunas empresas).

Independientemente del escenario y de la decisión de las partes, es fundamental que la regla esté clara y documentada para evitar riesgos jurídicos en el uso de esos dispositivos personales en el entorno laboral.

Por tanto, es recomendable que siempre haya un término de uso de dispositivos móviles particulares, aplicable inclusive para visitantes, y que

en este estén previstas algunas directrices legales esenciales, principalmente las que incluyen monitoreo e inspección, previendo, por ejemplo, qué ocurre de haber pérdida, daño, hurto, extravío del dispositivo de propiedad del particular.

Por tratarse de una actividad reciente, la inspección de dispositivo particular aún genera cierta incomodidad para los equipos de TI y SI. ¿Cuáles son las mejores prácticas técnicas y jurídicas a seguir para evitar que haya conducta abusiva o desproporcional por parte del empleador? ¿Qué hacer si el empleado se rehúsa a entregar el dispositivo para inspección?

Nuevamente, la primera orientación es que ese procedimiento esté debidamente escrito, para servir como *guideline* de conducta de la propia empresa, que exige estandarización e imposición de algunos límites.

La ejecución de esas actividades de auditoría depende de la previsibilidad de la rutina (acontecimiento periódico para educación y cultura), transparencia en el procedimiento (que esté claro cómo debe ocurrir para no sorprender al empleado), justificaciones plausibles (sean preventivas, que impliquen aleatoriedad, o puntuales, cuando hay una sospecha o incidente con evidencia comprobable) y del cumplimiento de los requisitos de proporcionalidad y razonabilidad (que delimita hasta dónde puede ir la verificación del equipo de forma administrativa, aún no judicial).

En analogía, puede mencionarse los casos de revisión personal, una práctica tolerable y aceptada por la jurisprudencia, siempre que: sea avisada previamente, realizada de forma indiscriminada y aleatoria, siendo preservada la dignidad del trabajador, y si fuera utilizada para el buen funcionamiento de la actividad emprendedora y para la seguridad de las personas. Por ejemplo, las empresas de tecnología que fabrican

componentes y hacen uso de esa actividad en la rutina de salida de los empleados, al final de la jornada laboral.

Como se dijo, para que el empleador no exceda los límites del poder directivo, pudiendo alcanzar dispositivos particulares que accedan al perímetro físico y lógico de la empresa, es necesario *notificar previamente a los empleados*, por medio de cláusulas contractuales y avisos en los ambientes lógicos y físicos, respecto a la seguridad del monitoreo (*todos los ambientes son monitoreados*) y de la realización de inspección física periódica aleatoria.

Como ejemplo de cláusula, que da a conocer previamente al empleado sobre la realización de la inspección física, tenemos el siguiente texto:

> "La Empresa puede solicitar el dispositivo para inspección en caso de que tenga sospecha de riesgo de filtración de informaciones o en defensa de su patrimonio o reputación, respetando los principios de la razonabilidad y de la proporcionalidad."

Con eso, la actividad de inspección y monitoreo es legal y no configura violación de privacidad o interceptación ilegal de datos, de acuerdo con los preceptos legales vigentes en el país constantes en el art. 5.º, incs. IV, X, XII, XXVIII, XIX y XXXV, de la CF, arts. 7 y demás de la Ley 12.965/2014, arts. 21 al 23 del CC y art. 10 de la Ley 9.296/1996.

Para la elaboración del procedimiento de inspección, teniendo en cuenta el escenario complejo e híbrido de los dispositivos, así como las innumerables vulnerabilidades tecnológicas existentes en el mundo cibernético que pueden afectar directamente las actividades económicas, es imprescindible el análisis de riesgos para diagnosticar la situación de

la seguridad de la información en la empresa y recomendar acciones para las vulnerabilidades mapeadas en los dispositivos móviles.

Es necesario realizar una evaluación para clasificar los riesgos y localizar dónde residen todas las informaciones confidenciales de la empresa, cuáles son las *palabras clave* que las identifican (para realización de escaneo por medio de software), revisando los perfiles de acceso remoto de cada usuario y a qué informaciones se está accediendo desde equipos particulares y por medio de qué recursos personales (e-mail, WhatsApp, Dropbox, y otros), permitiendo con este mapeo que la empresa defina claramente cómo ejecutar la actividad de inspección.

Y, ¿cómo prevenir los incidentes? ¿Cómo evitar la filtración de información desde esos dispositivos? Ciertamente, la solución involucra la aplicación de medidas técnico-comportamentales como el uso de la herramienta (DLP, encriptación, y otras) y realización de campañas de concientización.

Corresponde al empleador establecer cuáles son los requisitos de seguridad de las informaciones corporativas en los dispositivos particulares. Para ello, el uso del aparato móvil particular debe ser previamente autorizado por la empresa y el empleado debe cumplir con algunos procedimientos técnicos, tales como utilizar softwares de seguridad, contraseñas de bloqueo automático y habilitar la funcionalidad de borrado remoto en su equipo personal.

Además, los empleados deben estar bien orientados respecto a portar siempre la menor cantidad posible de datos y por el menor tiempo en sus dispositivos móviles, teniendo en cuenta los riesgos, inclusive, de pérdida de estos.

Otro aspecto que exige entrenamiento se refiere a la cuestión de las estafas con uso de aplicaciones gratuitas disponibles en las tiendas oficiales de Apple y de Google, que son trampas de virus con aplicación de metodología de ingeniería social.

La mayoría de las personas aún no usa antivirus en el smartphone, por tanto, este es un riesgo muy alto para la empresa, que puede inclusive estandarizar y brindar ese tipo de recurso de protección para ser instalado por todos sus empleados. O sea, la propia compañía suministra el revestimiento de seguridad de la información a ser instalado obligatoriamente.

De esa forma, queda claro que el entrenamiento de los empleados es fundamental para que las empresas diseminen la cultura de seguridad de la información durante el acceso al ambiente lógico corporativo.

Además de instruir a los empleados de punta, es necesario exigir que gestores y líderes orienten a sus equipos en cuanto al uso ético, seguro y legal de los recursos tecnológicos particulares y que verifiquen si las medidas de seguridad y políticas internas implantadas están siendo debidamente aplicadas por los empleados.

Para las empresas de la era digital es necesario crear y mantener actualizadas las políticas de protección de Seguridad de la Información, siempre involucrando a los sectores de tecnología de la información, jurídico, recursos humanos y gestión de riesgos. El objetivo es que las estrategias de actuación alcancen el equilibrio entre movilidad, protección de derecho del individuo, así como de las informaciones de la empresa.

Y esta tarea no es fácil, exige la ejecución de un revestimiento técnico-jurídico-educativo. Por tanto, una cosa es cierta: las personas van al

trabajo llevando consigo dispositivos particulares con los que pueden acceder a datos de la empresa. El mayor riesgo que se corre es justamente dejar de establecer la regla del juego claramente. Esa es una tarea urgente del empresario brasileño.

CYOD – LA ORGANIZACIÓN DEL BYOD EN SU EMPRESA

Leandro Bissoli

Los dispositivos móviles ya forman parte de nuestras vidas y de nuestras rutinas corporativas, lo que hizo cada vez más compleja la separación entre el uso personal y profesional de esas herramientas. En la sociedad digital, dejamos de *estar conectados* y pasamos a *ser conectados*.

Desde el lanzamiento del iPhone, en 2007, los dispositivos móviles personales conquistan espacio en el ambiente corporativo. Esa onda, llamada por los especialistas BYOD (*Bring Your Own Device*), trajo consigo una revolución y un enorme desafío para las áreas de Tecnología de Información y de Seguridad de la Información de las empresas.

Tenemos como norma de BYOD el siguiente escenario: el empleado conecta su dispositivo móvil personal a los recursos de la empresa. Las políticas y controles corporativos, cuando existen, son aplicados solamente a nivel de servidor y en la autenticación del dispositivo móvil en la red. Seguidamente, el empleado pasa a recibir, almacenar y transmitir informaciones corporativas en todo momento. Independientemente de su jornada laboral, el dispositivo permanece conectado.

El empleado, en ese escenario, es el responsable de la compra, manutención y principalmente de las informaciones almacenadas en el dispositivo móvil. Es él quien permite la instalación o eliminación de

aplicaciones, quien controla las actualizaciones (*patches*) y, como consecuencia, posee acceso remoto al ambiente lógico de la empresa.

Junto a eso, debemos destacar la *libertad* dada al empleado en la definición de qué dispositivo pretende utilizar en el ambiente corporativo. En contrapartida, la Empresa tendrá:

- *Disponibilidad*, con el acceso a las informaciones y aplicaciones en cualquier lugar, y flexibilización del puesto de trabajo;
- *Satisfacción* del usuario en el uso del recurso, pues podrá administrar sus actividades personales y profesionales en un único dispositivo;
- *Usabilidad* garantizada debido al desarrollo de dispositivos y aplicaciones cada vez más intuitivos, reduciendo el plazo de adaptación respecto al uso;
- El aumento de su *productividad*, pues el conjunto de beneficios antes mencionados contribuye a la mejora de la calidad de trabajo, por tanto, habrá más productividad.

Podemos además mencionar otros puntos positivos, como la percepción de la marca y la diferenciación competitiva, ya que la empresa está en línea con las tendencias del mercado, y la reducción de valores y costos de Telecom, pues algunos paquetes personales llegan a ser más baratos que los corporativos.

Muchas compañías están en esa onda del BYOD sin saberlo, pues es común que el colaborador utilice su dispositivo móvil personal en el ambiente corporativo sin avisar a las áreas competentes.

Sin embargo, los impactos positivos de esa fuerza de trabajo en movilidad acarrearon riesgos legales y desafíos vinculados a la Seguridad de la Información. Podemos destacar:

- *Invasión de la privacidad* del colaborador durante las actividades de monitoreo e inspección realizadas por la empresa. El empleado debe tener conocimiento previo de esas acciones antes de ingresar con el dispositivo;
- *Licencias de aplicaciones y softwares* instalados en el dispositivo. El uso de programa irregular es crimen, las indemnizaciones pueden llegar a hasta tres mil veces el valor del software irregular y a penas de prisión de hasta cuatro años. Vale destacar que incluso algunos softwares libres (freeware) pierden su gratuidad en el ambiente corporativo;
- *Laboral*. Con el acceso disponible en tiempo integral a las informaciones de la empresa, el empleado utilizará el dispositivo en horario diverso, no tenga duda. Tendremos muchos casos de jornada excedente de la ordinaria debido al uso del recurso tecnológico, y no simplemente por el porte (consolidado por el Compendio 428 del TST). La justicia trabaja con la verdad real (hecho ocurrido), y no sólo con la verdad formal (la que se establece en los autos, como un documento de control de horas);
- *Daños*. El empleado correrá con los perjuicios derivados de los daños causados, pérdida, hurto o robo del dispositivo en el ejercicio de sus actividades profesionales. Debe quedar claro para el empleado cuál es la responsabilidad de la empresa en esas situaciones;
- *Seguridad lógica*. El empleado debe programar mecanismos de seguridad lógica (contraseña, firewall, antivirus, etc.), actualizar las aplicaciones instaladas, utilizar encriptación (por lo menos en las informaciones corporativas relevantes), realizar acceso remoto de modo seguro, instalar aplicación para borrado remoto, almacenar los archivos en directorio en la red corporativa para garantizar una copia de seguridad, entre otros controles. La empresa asume

riesgos al delegar esas actividades de TI o de SI en el empleado, que muchas veces no posee el conocimiento y principalmente el tiempo necesario para gerenciarlas.

- *Seguridad física*. La empresa debe establecer controles para la entrada, estancia y salida de esos dispositivos de sus instalaciones, creando procedimientos de barrera para la verificación, además de ampliar la vigilancia interna.

Además, el *equipo de soporte* pasa a ser muy demandado por los empleados debido a problemas relacionados con las configuraciones e incompatibilidades dada la diversidad de modelos de dispositivos, operadoras y versiones de sistemas operacionales involucrados.

Ante esta situación, destacamos que las políticas de dispositivos móviles, cuando existen, poco abordan sobre los puntos presentados anteriormente, como: monitoreo e inspección, trasiego de informaciones, costos y gastos con relación al uso, comportamiento seguro del empleado y los niveles de seguridad implantados, sea tanto para almacenar la información como para establecer la conexión a la red.

Por otro lado, *cuando todos los puntos son presentados de forma clara*, sucede que el empleado opta por *no utilizar* más su equipo personal, pues es necesario mucho tiempo para realizar la gestión y manutención de la adecuación de su dispositivo móvil con las normas de la empresa. Además, es importante analizar los riesgos de transitar con su dispositivo diariamente en pro de la empresa y de estar sujeto al monitoreo o inspección corporativa.

Con eso, crece el CYOD (*Choose Your Own Device*), en el que la Empresa le presenta un grupo determinado de dispositivos ya definidos (adquiridos y homologados) al empleado para que seleccione el que más le convenga.

De ese modo, TI y SI *mantienen la gestión y el control de los dispositivos* de modo eficiente y dejan a los empleados satisfechos al atender a sus expectativas de movilidad. Así es mucho más fácil la comprensión del empleado sobre las actividades relacionadas al monitoreo e inspección por la Empresa, pues el dispositivo es de la Empresa. TI y SI establecen e implantan los controles y aplicaciones necesarios para garantizar la seguridad de las informaciones almacenadas o a las que se accedió desde el dispositivo antes de entregarlo para uso del empleado.

Investigaciones como la realizada por Azzurri Communications[4] señalan que la mayoría de las empresas opta por políticas de CYOD. De acuerdo con el estudio citado, tan solo 13% de las compañías creen que el BYOD es el estándar más adecuado para su negocio.

El modelo CYOD deberá asumir el liderazgo en las empresas brasileñas por ser una iniciativa más conservadora respecto a la adopción del BYOD, además de mitigar riesgos legales y de seguridad de la información si la Empresa ya posee por lo menos una Política de Seguridad de la Información vigente.

CYOD es el primer paso para las Empresas que buscan ampliar su madurez en la gestión de los dispositivos móviles y en la definición práctica de un plan de movilidad corporativa realmente eficiente.

[4]Disponible en: [www.azzurricommunications.com/resources/analyst-reports/infographic-byod-vs-cyod.aspx].

INSPECCIÓN EN DISPOSITIVOS MÓVILES: ¿CÓMO REALIZAR ESTE PROCEDIMIENTO SIN EXCEDER LOS LÍMITES DE LA LEY?

Luiz Philippe Moura

Diversos estudios[5] señalan que la movilidad de la fuerza de trabajo genera riesgos legales y desafíos para la seguridad de la información en las empresas, aún más cuando los empleados pueden utilizar dispositivos móviles particulares (BYOD) para el ejercicio de sus actividades profesionales.

La utilización de dispositivo móvil particular es una *facultad* conferida al empleado, siempre que la empresa no haya establecido el uso del dispositivo móvil particular como requisito para su contratación (de cargo o función), dando como indispensable el uso del BYOD por el empleado.

Por tratarse de una *facultad*, el empleado solamente podrá utilizar su equipo personal para ejercer actividades laborales, en caso de que firme y esté de acuerdo con el término de autorización de uso específico, o sea, el empleado estará sujeto a cumplir las condiciones previstas en contrato/término, en caso contrario, deberá atenerse solamente al uso de los dispositivos suministrados por la empresa para almacenamiento o manejo de las informaciones corporativas.

Las reglas deben ser formalmente establecidas de modo claro y por escrito durante toda la relación de trabajo, a fin de *cohibir* el uso de dispositivos particulares para el trasiego de informaciones corporativas *sin la previa y expresa autorización del empleador.*

Antes de adentrarnos específicamente en los procedimientos necesarios para la inspección, es necesario recordar que las relaciones de trabajo son formadas por dos sujetos, el empleador, *que tiene el poder de dirigir, organizar y fiscalizar* la prestación del servicio del empleado, y el

[5] Trend Micro. Bring Your Own Risk. Disponible en: [www.trendmicro.com/us/enterprise/challenges/it-consumerization/infographic/index.html]. Acceso en: 28.04.2015, a las 14 h 58 min.

empleado, subordinado jurídicamente al primero por medio del contrato de trabajo, términos y normativas internas de la propia empresa.

El ejercicio del poder directivo[6] del empleador no es absoluto y está sujeto a los límites establecidos por los derechos fundamentales previstos en la Constitución Federal, aplicados de forma horizontal, asegurados a los empleados en tanto sujetos de la relación de empleo.

Los límites del poder directivo son igualmente delineados en la Constitución por la existencia de principios impositivos, como el principio general de la igualdad de todos ante la ley y de la "inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad" (art. 5.º, *caput*), la regla general de que "nadie será sometido a tratamiento inhumano o degradante" (art. 5.º, inc. III), y, además, el principio general que declara "inviolables la intimidad, la vida privada, la honra y la imagen de las personas, asegurado el derecho a la indemnización por el daño material y moral derivado de su violación" (art. 5.º, inc. X).

La Constitución Federal salvaguarda derechos de los empleados e igualmente tutela la autonomía directiva del empleador. Por eso, hay diversas situaciones de colisión entre esos bienes protegidos constitucionalmente – derecho a la propiedad, a la libre iniciativa del empleador y derechos fundamentales de los empleados.

Nótese que la Constitución Federal tiene fuerza normativa en todo el ordenamiento jurídico, y que el derecho del trabajo forma parte de ese ordenamiento, o sea*, los derechos fundamentales deben ser respetados en el ámbito del contrato de trabajo.*

Vale señalar, a propósito, que los derechos del empleador son igualmente fundamentales, siendo garantizado principalmente el derecho de

[6] NASCIMENTO, Amauri Mascaro. *Curso de Direito do Trabalho*. 19. ed. São Paulo: Saraiva, 2004, p. 620-621.

propiedad y a la libre iniciativa para la creación y gestión de su emprendimiento.

Considerando que el poder directivo y de fiscalización del empleador no es absoluto, sino limitado, el *principio de la razonabilidad*[7] debe ser aplicado para dirimir el conflicto y, concretamente, a fin de determinar cuál de los derechos o bienes protegidos constitucionalmente deberá prevalecer, si los del empleado o los del empleador.

Para verificar la proporción de la incidencia de los derechos fundamentales de las dos partes que integran la relación de trabajo y qué medidas serán aplicadas en cada caso concreto, se debe aplicar el *principio de la proporcionalidad.*

Debido a que la jurisprudencia aún no ha tratado casos relacionados a la inspección de equipos particulares utilizados para finalidad corporativa (BYOD), es posible, ante las definiciones de revisión personal, hacer una analogía entre esta y la inspección de dispositivos personales que manejan informaciones corporativas, ya que ambas poseen la misma finalidad de fiscalizar las actividades y garantizar la seguridad del negocio de la empresa, siendo la última menos intrusiva por producirse en un equipo (dispositivo), y no en un ser humano.

Siendo así, se puede afirmar que las inspecciones y auditorías en dispositivos particulares *son tolerables y deben atender a los principios de proporcionalidad y razonabilidad presentes en la Constitución Federal.*

Pasadas las consideraciones acerca de los principios y límites constitucionales del poder directivo del empleador, veamos el paso a paso

[7] JUNIOR, Nelson Nery. *Código Civil Comentado*. São Paulo: Ed. RT, 2006.

ideal para la realización de inspecciones corporativas en dispositivos móviles.

¿Cuáles son los procedimientos necesarios para la ejecución de las inspecciones y auditorías?

I. *Conocimiento previo, por parte del empleado, de los términos y condiciones impuestos por el empleador;*
II. *Previsibilidad de la rutina: su acontecimiento periódico para educación y cultura (ejemplo: siempre a la salida, cada tres meses);*
III. *Transparencia en el procedimiento: que esté claro cómo debe ocurrir y no ser una sorpresa para el empleado;*
IV. *Justificaciones plausibles*: ya sean preventivas, que implican aleatoriedad, o puntuales, cuando hay una sospecha o incidente con evidencia comprobable o cuando se consigue demostrar la necesidad específica (ej.: siempre en caso de dimisión del empleado);
V. *Cumplimiento de los requisitos de proporcionalidad y razonabilidad:* Que delimitan hasta dónde puede llegar la verificación en el equipo de forma administrativa, aún no judicial (la orden judicial es esencial de haber algún tipo de interceptación de comunicación, pero no para verificar datos en el dispositivo si eso ya fue avisado previamente).

La empresa debe auditar e inspeccionar los equipos tecnológicos particulares que interactúan con sus ambientes físicos y lógicos, en situaciones puntuales que justifican su realización dentro de un procedimiento estándar, como el de dimisión del empleado. O sea, todo empleado sabe que será hecha la inspección, no es una sorpresa.

Excepcionalmente, puede darse el escenario en que el dispositivo debería ser sólo de uso particular, pero el empleador sospecha que el empleado esté portando datos de la empresa en el equipo. Ese es el caso más delicado desde el punto de vista jurídico, y será importante tener indicios que justifiquen una verificación puntual (no aleatoria), de modo que se evite cualquier entendimiento relacionado a la persecución y/o a la discriminación por parte del empleado.

Pasaremos, entonces, a detallar cuáles son los cuidados que deben ser observados en los procedimientos para la ejecución, sin riesgos legales, de la actividad de inspección de equipos particulares en el ambiente de trabajo (que estén en el perímetro físico de la empresa).

Primeramente, es necesario *notificar previamente a los colaboradores*, por medio de cláusulas contractuales, normas internas, términos de conocimiento y avisos en los ambientes internos, respecto a la inspección y auditoría, para que no se caracterice la violación de privacidad o interceptación ilegal de datos, de acuerdo con los preceptos legales vigentes en el país constantes en el art. 5.º, incs. IV, X, XII, XXVIII, XIX y XXXV, de la CF, arts. 7 y demás de la Ley 12.965/2014, arts. 21 al 23 del CC y art. 10 de la Ley 9.296/1996.

En ese sentido, tenemos precedentes jurisprudenciales favorables para ese posicionamiento,[8] así como la vigencia de la norma ABNT NBR ISO/IEC 27002:2013, que en el ítem 7.1.2 trata de los Términos y Condiciones de Contratación y recomienda que los contratos con los empleados declaren las responsabilidades de estos y las de la empresa para con la seguridad de la información, *estando de acuerdo específicamente con los términos y condiciones* estipulados en el contrato.

[8] TST; AIRR - 58941-85.2007.5.01.0052; 1.ª T., rel. Min. Lelio Bentes Corrêa, *DEJT* 02.04.2012 y TRT-9 3058200513905 PR 3058-2005-13-9-0-5, rel. Luiz Celso Napp, 4.ª T., 16.10.2007.

El modo en que se dará el procedimiento debe ser comunicado a todos los empleados, para que sea creada la cultura de la inspección en la empresa, así como para evitar la insubordinación.

Para que sea elaborado el procedimiento de inspección, teniendo en cuenta el escenario complejo e híbrido de tipos de dispositivos distintos, así como las numerosas vulnerabilidades tecnológicas, es imprescindible el análisis de riesgos para diagnosticar la situación de la seguridad de la información en la empresa y recomendar acciones para las vulnerabilidades ya existentes en la empresa con dispositivos móviles particulares.

La inspección es independiente de sospecha o de incidentes específicos de filtración de informaciones, pero debe ocurrir como medida preventiva de seguridad. Se recomienda, incluso, que el procedimiento sea rutinario para que se pueda verificar si las configuraciones de seguridad mínimas se mantienen activas y actualizadas, así como si las autorizaciones de uso se están produciendo de forma ética y segura por parte del empleado.

Entre las medidas técnicas aplicables para la implementación del procedimiento de forma correcta, se le sugiere a la empresa:

- ✓ Realizar una evaluación para clasificar los riesgos y localizar dónde se encuentran todas las informaciones confidenciales corporativas;
- ✓ Definir las *palabras clave* que identifican informaciones críticas (para realización de escaneo por medio de software en el dispositivo);
- ✓ Revisar los perfiles de acceso remoto de cada usuario;

- ✓ Analizar y mapear a qué informaciones se está accediendo por equipos particulares y por medio de aplicaciones de comunicación (e-mail, WhatsApp, Dropbox y otros), permitiendo con este mapeo que la empresa defina claramente cómo ejecutar la actividad de inspección, o sea, identificar dónde estarán dentro del dispositivo, cuál será el lugar predeterminado de almacenamiento, evitando tener que acceder a otras particiones o carpetas. Por eso, cuando el empleador suministra el paquete de seguridad, es más fácil establecer de antemano dónde las informaciones corporativas serán almacenadas en el dispositivo particular y proceder a la inspección sin acceso directo a las informaciones personales (como carpetas de fotos, por ejemplo);

- ✓ Siempre realizar la inspección ante la presencia del empleado, así como que le corresponde a él el desbloqueo de su equipo particular (digitación de la contraseña, si fuera necesario);

- ✓ Establecer requisitos estandarizados de seguridad que deben contener los dispositivos particulares, como, por ejemplo:

    - o softwares de seguridad, antivirus, firewall, entre otros;

    - o contraseñas de bloqueo automático;

    - o funcionalidad de borrado remoto de las informaciones corporativas en el equipo personal.

- ✓ Aplicar medidas técnico-comportamentales, como uso de herramienta (DLP, encriptación y otras) y realización de campañas de concientización.

Con motivo de la inspección rutinaria y/o incidental, los empleados deben ser orientados a llevar consigo siempre la menor cantidad posible de datos por el menor tiempo en sus dispositivos móviles, teniendo en cuenta los riesgos de filtración.

Además de instruir a los empleados de punta, es necesario exigir que gestores y líderes orienten a sus equipos respecto al uso ético, seguro y legal de los recursos tecnológicos particulares y que verifiquen si las medidas de seguridad y políticas internas implementadas están siendo debidamente aplicadas por los empleados.

En la hipótesis de que, durante el procedimiento, aquel que lo realiza acceda a alguna información íntima del empleado, esta debe ser desconsiderada o descartada de modo seguro (proceso de clonación o copia), ya que escapa de la motivación de búsqueda de informaciones corporativas (prevención del riesgo de filtración).

Además, de ser posible, es importante que se instale el paquete de seguridad suministrado por la empresa, dado que este conjunto de softwares permite preestablecer qué y dónde será hecha la búsqueda de informaciones en el dispositivo (como ocurre con la solución IBM de comunicador instantáneo corporativo, cuyos mensajes quedan guardados en el propio almacenamiento local).

Es posible, aún, mencionar la existencia de softwares en el mercado tecnológico que posibilitan la inspección remota de recursos específicos de equipos particulares, soluciones de tecnología MDM (Mobile Device Management), que son ofrecidas inclusive de forma gratuita, como las de McAfee Mobile Security, Microsoft Azure y Symantec Enterprise Mobility. De ese modo, la inspección física, inclusive rutinaria, no necesitaría ser

realizada con frecuencia, debido a la verificación remota, opción práctica y segura para el equipo de Tecnología de la Información.

Sin embargo, en caso de que la empresa no adopte la utilización de softwares de inspección y monitoreo remoto, o incluso que los utilice y eventualmente necesite examinar el dispositivo manualmente, la inspección física debe ser hecha con la mayor cautela posible para que los datos personales del empleado no sean expuestos.

Recomendaciones específicas de conducta ética que deben ser observadas por el equipo que realice el procedimiento de inspección:

- ✓ La inspección física debe ser presenciada por el propio empleado y, de ser posible, ante dos testigos, para asegurar la confiabilidad de la ejecución y preservar la prueba de la realización idónea del procedimiento;
- ✓ La contraseña del dispositivo debe ser tan solo de conocimiento del empleado y en hipótesis alguna podrá ser de conocimiento del inspector, o sea, para verificación del equipo, es necesario que el propio usuario introduzca la contraseña;
- ✓ Las aplicaciones de comunicación social, como WhatsApp, Facebook, Instagram y otros de uso particular del empleado, no pueden ser verificadas en ninguna hipótesis;
- ✓ El contenido de e-mails y mensajes particulares no puede ser verificado, bajo pena de violación de la intimidad y privacidad del empleado;
- ✓ A fotos y archivos personales no podrá acceder el inspector, es necesario tener el máximo cuidado en ese momento, pues existe el riesgo de que el empleado deje una foto íntima a propósito para que el técnico la visualice y se genere un incidente vergonzoso de

autoexposición, ocasionando futura causa laboral contra la empresa;

- ✓ Al final de la inspección, deberá generarse un informe detallado acerca de todos los recursos a los que se accedió y que fueron verificados en el dispositivo particular. El informe deberá ser firmado por el empleado, inspector y testigos que presenciaron la inspección física.

Todos los medios legales, así como los moralmente legítimos, aunque no especificados, son hábiles para probar la verdad de los hechos, en que se funda la acción o la defensa.[9] Además, el Nuevo Código de Proceso Civil trajo consigo disposiciones específicas en los arts. 439 al 441 sobre la admisión de documentos electrónicos en procesos judiciales. Siendo así, cualquier dato en medio digital que pueda colaborar en el sentido de probar que un fraude o irregularidad fue cometido y que pueda establecer vínculo entre el incidente y la víctima y entre la víctima y el agente.

Cuando se evidencie algún incidente por parte del empleado, al inspector le corresponderá recolectar prueba de manera cautelosa, teniendo en cuenta que toda evidencia digital puede ser adulterada, alterada o destruida por manejo o examen inadecuado.

La recolección debe hacerse en el momento de la inspección, debiendo ser realizada la copia de la evidencia digital en el proceso de adquisición. Además, la cadena de custodia de esa evidencia es fundamental para preservación de la prueba.

El registro de la cadena de custodia debe hacerse por medio de un documento, describiendo, en orden cronológico, todo el proceso de

[9] Art. 369 – Código de Proceso Civil

identificación, recolección y adquisición de la evidencia digital, hasta el momento de la ubicación actual, además de los responsables, de acuerdo con la ABNT, en la ISO 27037:2013, en el ítem 6.1, que recomienda expresamente que el responsable describa todas las adquisiciones de datos e informaciones que estén bajo custodia de la empresa.

Además, recomendamos el registro de acta notarial, siempre que corresponda, ya que su fuerza probatoria sustituye eventuales testigos, y da mayor seguridad en la apreciación de la ocurrencia o existencia del hecho narrado.

Como las pruebas digitales son muy volátiles, el acta notarial se hace imprescindible en casos de incidentes digitales. Esa modalidad de prueba aporta la buena fe de un tercero (que en este caso es dotado de fe pública) y es de extrema importancia, dado que el empleador es la parte interesada en la inspección y necesita apartar cualquier acusación de que la prueba pueda haber sido *plantada*. Además, hace que el evento se perpetúe (durabilidad de la prueba) y garantice que el hecho existió, en caso de que desaparezca.

Durante la vigencia del contrato de trabajo, el empleador posee la facultad de aplicar penalidades laborales a los empleados que no cumplan con las obligaciones previstas en el documento. La adopción de medidas punitivas, por tanto, tiene la finalidad de corregir la conducta inadecuada del trabajador, así como de evitar que se repita, haciendo inviable la manutención del propio contrato de trabajo.

Es importante destacar que el *poder de disciplina* que compete al empleador debe ser ejercido con *moderación y compatibilidad* respecto al incidente ocasionado, dentro de los límites de la *proporcionalidad y razonabilidad.*

El exceso de rigor de una pena o advertencia que impida la retractación y la rectificación de la conducta puede ocasionar la recisión indirecta del contrato de trabajo, pues implica falta grave del empleador. Por eso, existe la práctica de documentar advertencias para entonces basar la justa causa (o por la gravedad o por la reiteración de la conducta que demuestra mala fe).

Por tanto, las medidas punitivas deben ser aplicadas de forma gradual, siendo agravadas a medida que haya repetición de la falta, pues tiene como objetivo proporcionar al empleado la oportunidad de corregir su comportamiento.

Es oportuno recomendar que la empresa establezca claramente ante los empleados que la resistencia a la inspección determina la prohibición y/o restricción de uso del dispositivo móvil particular en el ambiente de la empresa (perímetro físico, y no sólo durante el horario de trabajo), o sea, para concesión y continuidad de la autorización de uso, el conocimiento previo y colaboración por parte del empleado, cuando sea necesario, para que se produzca el procedimiento de inspección es condición inherente y de ella no debe abstenerse el empleado bajo hipótesis alguna.

Por último, esclarecemos que, en la legislación laboral vigente, no existe previsión legal que discipline la concesión de advertencia, siendo esta, por tanto, originada del poder de dirección del empleador y utilizada en dos sentidos en el lenguaje jurídico: de aviso y amonestación.

La advertencia en casos de *uso indebido* o de *incidentes de seguridad de la información* debe hacerse por escrito y siempre registrada en la ficha del empleado (expediente del trabajador, sea físico o digital), siendo vedada, no obstante, anotaciones que desacrediten la conducta de este

empleado en su Cédula de Trabajo y Seguridad Social, en los términos del § 4.º del art. 29 de la Consolidación de las Leyes del Trabajo.

En ese escenario, recomendamos que, además de la advertencia, se le suspenda (provisoriamente) o cancele (definitivamente) la autorización de uso del recurso particular del empleado en el ambiente de trabajo, para evitar que se produzcan nuevos incidentes.

En caso de que el empleado se rehúse a firmar la advertencia, es aconsejable que el empleador recoja la firma de dos testigos que presenciaron el hecho y que vieron la recusa del empleado a firmar la advertencia. De esa manera, el empleador se resguarda para comprobar que la advertencia ocurrió, de ser necesario en sede judicial. La validez de la advertencia firmada por testigos es confirmada por el Poder Judicial brasileño.[10]

La reiteración del uso indebido (no conforme a las reglas establecidas), o no autorizado (cuando hubo recusa a la inspección anteriormente) del dispositivo móvil particular, en el ambiente de trabajo relacionado con las informaciones de la empresa, puede acarrear la recisión por justa causa del contrato de trabajo.

Aplicada la advertencia y reiterada la práctica indebida por parte del empleado, podrá ser aplicada la suspensión de las actividades laborales, como medida educativa para el empleado que, de alguna forma, violó las reglas de la empresa o no cumplió con el deber que le es impuesto, incluso con relación a lo que fue pactado en el contrato de trabajo y en el término de autorización de uso.

[10] TST - AGRAVIO DE INSTRUMENTO EN RECURSO DE REVISIÓN AIRR 913000620095030071 91300-06.2009.5.03.0071 (TST)

Siendo así, es lícito que el empleador suspenda al empleado que cometió algún acto inadecuado de mediana gravedad. Sin embargo, tal suspensión no podrá prolongarse por más de 30 días, bajo pena de que el empleador recaiga en una falta grave, posibilitando al empleado el ingreso de una acción laboral pleiteando una recisión indirecta del contrato de trabajo, como preceptúa el art. 483 de la CLT, además de la incidencia de multa administrativa por infligir el art. 474 del mismo Diploma Legal, el cual determina el mencionado plazo de 30 días.

Aplicada la advertencia y suspensión, la dimisión por justa causa será aplicada como punición máxima que se puede imponer al empleado, como dispone el art. 482 de la CLT.

Vale resaltar que la pena de ruptura de la relación de empleo es reservada a las faltas que implican *violación seria e irreparable de las obligaciones contractuales asumidas* (abarca inclusive hipótesis de abuso de confianza), concluyéndose, por tanto, que no es cualquier incumplimiento de contrato el que da derecho al empleador a rescindirlo, sin embargo, al seguir el orden cronológico de aplicación de penalidades en este dictamen sugerido, la dispensa se vuelve legal y motivada.

Robert Siciliano,[11] consultor de McAfee y especialista en robo de identidades, afirmó que la mayoría de los dispositivos móviles permanece con informaciones incluso después del procedimiento de eliminación de archivos por parte del usuario. Además, los informes también señalan que los técnicos en tecnología de la información consiguen realizar el borrado integral de un dispositivo en menos de tres minutos.

Por tanto, es imprescindible que, en el acto de demisión, el equipo de Tecnología de la Información logre borrar las informaciones corporativas por medio de la inspección adecuada, preservando la intimidad y los límites de privacidad de los empleados, ya señalados.

[11] Disponible en: [http://itforum365.com.br/noticias/detalhe/113359/byod-como-manter-a-seguranca-empresarial-]. Acceso en: 02.08.2016, a las 11 h 30 min.

Sin embargo, es prohibida la coacción del empleado, obligándolo forzosamente a proporcionar su dispositivo, incluso con motivo del incumplimiento de la cláusula contractual. O sea, debido a las garantías constitucionales que le son previstas, el empleado puede rehusarse a entregar el dispositivo personal para análisis del inspector.

La empresa puede, entonces, seguir dos caminos:

a) Amigable: documentar la recusa y recoger la firma del empleado (en caso de que se pueda demostrar posteriormente que la recusa a colaborar fue intencional y constatar el daño causado);
b) No amigable: ya exige la necesidad de involucrar a la autoridad (policial y/o judicial con pedido de orden de búsqueda y captura). En síntesis, la aprehensión de bienes, en este caso, se destina a la preservación de los medios de prueba y en el intento de manutención para utilización en la instrucción criminal. Siendo así, durante la permanencia del conjunto aprehendido en el distrito policial, la responsabilidad por la custodia segura, eficiente análisis y pronta destinación de las cosas retenidas es de la policía judicial.

El objetivo de la inspección es tan solo garantizar que el uso de dispositivos móviles particulares debe hacerse de manera ética y segura, para que los empleados sepan sus responsabilidades al portar informaciones corporativas y del deber de protección de estas en el curso de las actividades laborales.

Se pretende, igualmente, evitar el desvío de finalidad de la autorización de uso del dispositivo móvil particular, que debe ser estrictamente profesional, teniendo en cuenta las innumerables vulnerabilidades

tecnológicas existentes en el mundo cibernético que pueden afectar directamente las actividades de la empresa.

Por tanto, la previsión de la inspección en el contrato de trabajo, en Políticas y Normas Internas, protege además al empleador contra situaciones de filtración o sustracción de informaciones, incluso para casos en que el empleado se niegue a ceder información importante o decisiva para el negocio de la empresa, pero que está en poder de su dispositivo móvil particular. Por medio de la comunicación previa de la posibilidad de inspección, el empleado queda sujeto a proporcionar el dispositivo, de haber algún caso excepcional que necesite el debido tratamiento, mitigando o, al menos, minimizando riesgos que pueden impactar a la empresa de forma negativa.

CAPÍTULO SEGUNDO

EL TAN ESPERADO MARCO CIVIL DE INTERNET

AL FIN, EL MARCO CIVIL DE INTERNET

Victor Auilo Haikal

El proyecto de ley más relevante para el uso de internet fue aprobado por la presidenta Dilma Rousseff durante el NETMundial[12] con todos los honores que la ocasión ameritaba. El Marco Civil de Internet (MCI) posee una naturaleza bastante peculiar, especialmente por la forma en que fue ideado, creado y discutido, que contó con una amplia participación de los ciudadanos en foros de discusión en internet y en audiencias públicas promovidas por el Congreso Nacional.

Uno de los temas abordados por la ley que más causa debates es la responsabilidad civil por la divulgación de contenidos en la red, que involucra varios deberes delegados al controlador del sitio, por ejemplo, la necesidad de remoción del contenido en caso de denuncia y si se debe indemnización a aquellos que sufrieron daño por la publicación, además del dilema de la conservación de los registros de actividad en su ambiente digital.

Aunque la redacción inicial del MCI incluyese el procedimiento de retirada inmediata luego de la notificación del interesado (*notice and takedown*), el proyecto fue enviado por el Ministerio de Justicia al Congreso con la responsabilización del hospedero del contenido solamente después de orden judicial, y ahora, contiene la reserva sobre material vinculado a la pornografía, que debe ser removido en cuanto la comunicación sea recibida.

Actualmente, la Jurisprudencia se muestra bastante madura respecto a la responsabilidad, habiendo recientes sentencias del STJ orientando la toma

[12] NETmundial – Encuentro Multisectorial Global Sobre el Futuro de la Gobernanza de Internet, organizado por el Comité Gestor de Internet en Brasil (CGI.br) con la colaboración de /1Net.

de providencias en un máximo de 24h de la denuncia, sea la remoción del contenido o su mantenimiento, lo que configuraría una responsabilización conjunta con el ofensor, independientemente de la naturaleza del material. Si el proyecto es aprobado con esa redacción, la actuación del Poder Judicial será modificada, lo que indica retroceso, pues habrá más acciones judiciales y resultará en lentitud para lo que exige agilidad.

La conservación de los registros (logs de actividad) siempre causa polémica, sobre todo por el riesgo de vigilantismo de los proveedores de servicio en internet, alegado por diversos debatientes con relación a la medida. Sin embargo, en ausencia de cualquier disposición específica de la legislación, esa conservación ya puede ser realizada, por cuestiones de gobernanza interna y protección de los derechos de terceros, atendiendo siempre a la necesidad previa de orden judicial para suministro.

Si hay violación o no de la confidencialidad de esos registros, es imposible afirmarlo, ya que no existe tecnología a prueba de mala fe.

Sin embargo, vale señalar que esos registros son indispensables en la investigación de autoría de actos ilícitos y crímenes en internet, por eso, la conservación previa de esos registros es necesaria para preservar el equilibrio y el derecho de defensa de aquellos que sufren alguna especie de abuso. La falta de obligatoriedad de esos datos genera inseguridad jurídica y un ambiente propicio para quien tiene como objetivo perjudicar la imagen y reputación de otras personas.

Sorprendentemente, el artículo 17 de la redacción aprobada posee un defecto en contraposición al artículo 15, pues exime a los proveedores de aplicación de responsabilización en caso de no conservación de los registros de acceso. Pues bien, ¡si existe una obligación legal de conservarlos por seis meses, no hay la alternativa a no hacerlo! Este

disenso merecería reparación por parte del Senado Federal, donde ni siquiera fue señalado. Queda registrada la primera necesidad de enmienda.

También merece ser destacada la conservación de la neutralidad de la red, que pasa por discusión tanto en Estados Unidos como en Europa. Estamos al día con lo que ocurre en el escenario cibernético mundial. En EUA la cuestión gravita en torno a la banda ancha ofrecida por el gobierno americano gratuitamente, que será controlada para evitar usos entendidos como no pertinentes, por ejemplo, la compartición de contenido no autorizado y acceso a servicios vinculados a actividades criminales o a la *Deep Web*.

En Europa la cuestión involucra también la cantidad de uso de banda por servicios que consumen gran cantidad en tráfico de datos, por ejemplo, los servicios de mensaje instantáneo y *streaming*, más parecido a lo que se debate en el escenario brasileño.

Sim embargo, Chile ya poseía reglas asegurando la neutralidad de la red desde 2010, con la promulgación de la ley nº 20.453 y su decreto reglamentario de diciembre de aquel año, siendo el primer país en editar una norma en ese sentido.

También, es relevante destacar que la regulación de México entró en vigor poco tiempo después de la ley brasileña, a partir de la *Ley Federal de Telecomunicaciones y Radiodifusión* (LFTyR), promulgada el 14 de julio de 2014 que en sus artículos 145 y 146 preveían expresamente la no discriminación de paquetes y el acceso pleno a internet por cualquier proveedor de conexión, cuyo tráfico debería estar libre de cualquier interferencia.

La idea de neutralidad es parte inseparable de internet, porque da acceso sin limitación a la información disponible en la red, salvo por condiciones exigidas por el proveedor de servicio. Ese carácter impulsó la comunicación y el acceso a informaciones en tiempo real en diversas movilizaciones en los últimos años, por ejemplo, las elecciones en Irán en 2009, la primavera árabe en 2010 y las protestas brasileñas de junio de 2013.

El volumen de tráfico debe ser solucionado con mejorías en la infraestructura y no con la obstaculización al acceso a un recurso que es esencial para incontables personas, en las más diversas regiones y grupos etarios.

Para los que trabajan en Derecho, un alivio: ahora existe un procedimiento propio para la requisición de datos para los proveedores de conexión y acceso, siendo dispensable la deformación de ritos para alcanzar tal tutela.

Para los usuarios en general: lectura obligatoria. Conocer la regla del juego es esencial para el buen uso de la red y para la preservación de los derechos del usuario sobre un recurso cada vez más inseparable del día a día de todas las personas.

Finalmente, Ley nº 12.965 de 2014, Marco Civil de Internet.

¿CÓMO EL MARCO CIVIL AFECTA NUESTRA VIDA DIGITAL?

Patricia Peck Pinheiro

Si usted no puede vivir sin conectarse a la *web*, usa aplicaciones sociales y en la nube, le gusta expresar su opinión en las Redes Sociales, tiene

celular con banda ancha y está preocupado con su privacidad, entonces el *Marco Civil de Internet* tiene efectos en su vida.

Entienda qué es el Marco Civil

El Marco Civil es una *ley* que llegó para proteger más la *privacidad* y la *libertad* del *internauta*.

Neutralidad de la red

El Marco Civil se trata de la *neutralidad de la red*, que consiste en la garantía de la *igualdad en el tráfico de datos*, donde todos tienen que tener acceso a las informaciones, sin que haya una selección de qué contenido pasa primero que otro. Imagine que usted prefiere un determinado servicio de videos, como YouTube, y este llega a un acuerdo con la operadora para que los datos pasen antes que los otros servicios de video competidores, haciendo que el suyo sea más rápido que los demás. Eso en la ley brasileña es considerado competencia desleal y hiere el principio de que todos deben ser tratados de igual manera, sin privilegios o cualquier tipo de discriminación.

Pero eso no significa que todos los internautas que se conectan tienen la misma velocidad de navegación. Además, es posible que las operadoras cobren valores diferentes para quien quiere una conexión más rápida, sólo no siendo permitido dar preferencia de transmisión a un tipo de contenido en detrimento del otro. Pero hay una excepción: la posibilidad de que el Presidente de la República permita que pasen más rápido informaciones relacionadas con seguridad o soberanía nacional o de salud pública.

Secreto

El internauta ahora tiene sus *datos* más *protegidos* y puede pedir que estos sean borrados. Aun así, es necesario estar atento a las Políticas de

Privacidad de cada servicio. El Marco Civil exige que sea aplicada la *ley Brasileña* si involucra a un usuario brasileño o por lo menos que una de las partes esté en Brasil, aunque el proveedor del servicio esté en otro país.

Libertad de expresión con responsabilidad

El mayor impacto tiene que ver con el uso responsable de la libertad de expresión. Es más difícil remover rápidamente un *contenido ofensivo*, a no ser que este envuelva desnudos o escena de sexo, o que exponga a menores de edad, pues se aplica el Estatuto del Niño y del Adolescente. En esos casos es posible hacer la denuncia online en la propia plataforma y el contenido tiene que ser retirado del aire inmediatamente. Para otros incidentes, las publicaciones sólo son removidas con el pedido de un Juez, lo que llamamos "orden judicial".

Conservación de Pruebas Digitales

¡En internet todo es rastreable! Los testigos son las máquinas y ellas registran todo que hacemos. Por eso, el tema de la conservación de las evidencias electrónicas llamadas "*logs*", que no son más que los registros de los hechos en el ambiente computacional con asociación a una autoría "*login*", se volvió tan relevante. ¡Sin prueba no hay crimen! Por consiguiente, los proveedores de conexión y los proveedores de aplicaciones (que están en los ambientes de navegación) deben guardar esos registros por el plazo de un año para el primero y de seis meses para el segundo, así como suministrarlos en cumplimiento de orden judicial, y sólo en esa hipótesis.

Para el internauta, resta el consejo de tener cuidado con las actitudes en internet, pues es bastante difícil que nadie se entere o lograr ser totalmente anónimo. *No existe "nadie lo vio" en el mundo digital.*

Por eso, *piense antes de publicar* y analice bien el contenido antes de compartir. En la era de la *transparencia digital* es imposible esconderse. Además de las informaciones propagarse rápidamente, existen muchos medios de rastrearlas y es bastante difícil ser totalmente anónimo en ese ambiente.
El Marco Civil representa un gran paso en la *discusión democrática* de qué valores proteger en la era digital, pero aún hay mucho por hacer.
Sin *educación*, el uso de la *tecnología* puede ocasionar grandes daños a la sociedad.

EL MARCO CIVIL Y LA LIBERTAD DIGITAL

Patricia Peck Pinheiro

El Derecho tiene la misión de establecer los parámetros legales que deben proteger los valores sociales de una comunidad en determinada época. En este caso, hoy, el mayor desafío del Derecho de la Sociedad Digital es justamente trabajar en una arquitectura jurídica que permita el pleno ejercicio de la libertad y de la libre iniciativa.

Pero, ¿cómo hacer eso en un momento de intensa "Economía Creativa", donde las nuevas tecnologías dictan las tendencias de las costumbres y comportamientos de los individuos que ya no conviven en territorios físicos, aprisionados en ordenamientos jurídicos tradicionales, sino en un mundo plano, global y digital, en el que los contratos privados, como los Términos de Uso y las Políticas de Privacidad de los servicios y aplicaciones de internet rigen la vida de las personas y determinan las reglas del juego para poblaciones inmensas, multiculturales y multinacionales?

Ese es el concepto de la "Sociedad Abierta" ("*Open Society*"), que según Don Tapscott, uno de los mayores especialistas en Generación Digital, trae consigo cuatro grandes principios: Colaboración ("*Collaboration*"), a través de redes de inteligencia ("*networked intelligence");* Transparencia ("*Transparency*"); Compartición de Contenido y su Propiedad Intelectual ("*Sharing*"); y Movilización ("*Empowerment*").

Vivimos un momento único de ruptura de paradigma del propio modelo de producción, pues las redes sociales y la cultura de las "*apps*" (aplicaciones) permiten la producción colectiva y colaborativa, a un costo de distribución bajísimo y con la posibilidad de explotación de la "gratuidad" como una forma de atraer usuarios-clientes y después cobrarles el precio del servicio con el uso de una nueva moneda: información.

Por eso, las redes sociales alcanzaron en los últimos años el puesto de primer lugar de búsquedas, donde se puede encontrar a alguien o incluso obtener una información.

Eso genera una profunda transformación en la estructura organizacional tradicional. Además, las empresas son cada vez más fluidas y sin límites físicos, lo que exige una mayor conducta ética, más integridad ejecutiva y más gobernanza corporativa.

Como resultado de la mayor distribución de conocimiento a través de la descentralización de la información, se da más poder al individuo y se garantiza libertad. Es por eso que iniciativas como *WikiLeaks* son tan sólo la punta del iceberg y tienden a aumentar, con revoluciones sociales digitales produciéndose a través de la web, como en el caso de Túnez, en 2010.

Pero no es sólo eso. A pesar de este individuo poseer más conocimiento, no quiere decir que sea más educado y preparado para aceptar toda la diversidad que la cercanía a esta gran aldea digital trajo a su ambiente de convivencia social. Lo que vemos es el aumento de incidentes de abuso de la libertad a través de la práctica de ofensas, discriminación, prejuicio, persecución.

Por tanto, cuando Brasil optó por crear una nueva ley para tratar algunas de estas cuestiones, siguiendo la tendencia europea y en respuesta al espionaje electrónico norteamericano, que fue aprobada por Dilma Rousseff como Marco legal de la Internet Brasileña, y llamado "Marco Civil de Internet" (MCI), eso supuso un hecho histórico para el mundo digital, que nació libre y sin reglas y que, después de casi 50 años de Arpanet, pasa a ser más regulado. Pero ¿cuáles son sus impactos?

La Ley 12.965/2014, o mejor dicho, el Marco Civil de Internet, trae consigo *10 grandes principios* para una internet más inclusiva y justa para los brasileños: neutralidad, acceso a internet como derecho esencial para el ejercicio de la ciudadanía, libertad de expresión y permanencia del contenido y su remoción sólo en casos excepcionales y con orden judicial, privacidad (con veda para monitoreo no acordado de forma previa y expresa con el internauta), protección de los datos personales, transparencia con exigencia de reglas claras de proveedores de conexión y de aplicaciones en la *web*, seguridad de la red, educación en ética digital, uso preferencial de códigos abiertos y responsabilidad de los agentes.

Claro que la nueva ley brasileña viene al encuentro de la tendencia de apertura mundial, que demuestra justamente la presión de los usuarios digitales para compartir y expresarse sin censura, pero trae consigo diversos efectos legales directos e indirectos para los negocios.

¿Estaremos preparados en Brasil para asumir una posición de tanta libertad? ¿O esto puede traer efectos colaterales indeseados? Tales como el aumento de rumores sobre marcas, comentarios ofensivos de consumidores, perfiles falsos que pueden ser usados por criminales para estafar a los internautas, aumento de actos ilícitos debido al favorecimiento del anonimato, entre otros.

Algunos segmentos de mercado son más afectados que otros, especialmente en lo que se refiere a la aplicación de los principios de la neutralidad, de la libertad de expresión y de la privacidad de los datos de los internautas brasileños. Entre ellos tenemos: Telecomunicaciones, Proveedores de Internet, Proveedores de Aplicaciones en general (desde el Internet *Banking* hasta la aplicación de taxi), Portales de Contenido, Redes Sociales, empresas que ofrecen servicios de *cloud computing*, de monitoreo de la navegación del usuario y generación de métricas para marketing digital, y empresas que hacen uso de *Big Data* para realizar enriquecimiento de bases de datos.

O sea, de cierto modo, la nueva ley trajo cierta intervención del Estado en la economía y en la libre iniciativa cuando pasó a reglar, inclusive, situaciones en que la empresa ofrece un servicio vía internet y está en otro país (su servidor está fuera de Brasil), pero capta datos de ciudadanos brasileños o a cuyo servicio se accede por medio de una aplicación en que el usuario interactúe a partir de una conexión de internet desde Brasil.

Cualquiera que se encuadre en la condición prevista por el art. 11, que plantea que en cualquier operación de recolecta, almacenamiento, conservación y tratamiento de registros, de datos personales o de comunicaciones por proveedores de conexión y aplicación de internet en que por lo menos uno de esos actos ocurra en territorio nacional (uno de

los terminales esté en Brasil), está sujeto al Marco Civil de Internet obligatoriamente y demás leyes brasileñas sobre protección de datos personales y secreto de las comunicaciones privadas de los registros.

Siendo así, está sujeto a tener que cumplir la ley brasileña bajo pena de aplicación de las siguientes penalidades del art. 12 en caso de que no atienda a las reglas de privacidad y protección de los datos en cuanto a la conservación, suministro, almacenamiento y tratamiento de los registros y datos personales: (a) advertencia, con indicación del plazo para adopción de medidas correctivas; (b) multa de hasta 10% (diez por ciento) de la facturación del grupo económico en Brasil en su último ejercicio; (c) suspensión temporal de las actividades que involucren operación de recolección, almacenamiento, conservación y tratamiento de registros, de datos personales o de comunicaciones; y (d) prohibición de ejercicio de las actividades que involucren operación de recolección, almacenamiento, conservación y tratamiento de registros, de datos personales o de comunicaciones.

La penalidad que la nueva ley trae es bastante alta si se compara a otras previstas en leyes específicas para segmentos regulados (como ocurre con Bancos, Telecomunicaciones, Energía, Seguros Médicos, Industria Farmacéutica, otros).

El punto que más puede afectar a las marcas involucra la cuestión de la libertad de expresión, pues ahora vale todo, o "casi todo". Flexibilizamos la protección constitucional de la honra, imagen y reputación del individuo. La remoción de contenido de forma directa e inmediata con el proveedor de la página sólo ocurre si este envuelve desnudez, escena de sexo, infracción de derecho de autor o exposición de menor de edad. Fuera de eso, solamente con orden judicial y sin ninguna garantía de remoción completa (de acuerdo con las limitaciones técnicas del servicio).

O sea, le corresponderá a la víctima decir exactamente dónde está el contenido que desea remover y al Juez decidir con la misma claridad y objetividad, de lo contrario, el contenido permanece en el aire. Los altos ejecutivos de las empresas están todavía más expuestos. A no ser que haya una foto del presidente "como Dios lo trajo al mundo", prácticamente todas las informaciones publicadas respecto a él y a la compañía dependerán de orden judicial para ser removidas de la *web*.

Por tanto, nuestro mayor desafío será educacional, ya que habrá mucha más exposición de víctimas de contenidos digitales ofensivos provocados por el exceso de la propia libertad sin responsabilidad, lo que genera no sólo un gran perjuicio social, sino también económico, pues puede afectar el valor de las acciones de empresas abiertas en la bolsa. Sumados a los contenidos que infringen derechos autorales, tenemos ahí un gran impacto en la Economía Digital.

Por lo visto, a la inversa, el Marco Civil acabó por contribuir con un manto de impunidad que puede estimular el crecimiento de los actos ilícitos basados en dos tipos de comportamiento: "sin sentido común" y "de mala fe" debido a la impunidad.

En lo que se refiere a la responsabilidad, la nueva ley disminuye considerablemente el riesgo de que una empresa sea responsabilizada por comentarios de terceros, o sea, por el contenido posteado o compartido en su ambiente (siempre que este tercero no sea empleado, pues recae la regla del art. 932 del Código Civil).

En resumen, lo que todo gestor debería observar sobre la aplicación de la nueva ley del Marco Civil de Internet sobre su negocio, en especial quien actúa en las áreas de comunicación y gestión de la marca, implica especial cuidado con:

- ✓ actualización del Término de uso y la Política de Privacidad de la empresa y publicación de la nueva versión en todos los ambientes digitales de la marca;
- ✓ recolección de datos de usuarios y su uso de acuerdo con la finalidad expresa claramente en una Política de Privacidad, que debe estar públicamente accesible en cualquier ambiente de la marca (*site*, *fanpage*, aplicación);
- ✓ uso de *Big Data*, enriquecimiento de bases de datos y rastreo de navegación *web*, lo que incluye uso de servicios de publicación de publicidad digital destinada a la navegación de usuarios que tienen que demostrar que aviso previo y expreso del monitoreo fue hecho, y conservación de los *logs* de navegación del usuario;
- ✓ contratos de compra de Medios Online y el estado de la Política de Privacidad de los respectivos ambientes donde se insertará;
- ✓ uso de bases de dados de terceros propias de la *web*, como sistemas de análisis de crédito, sistemas de mapeo de perfil de consumidor (Clearsale, Serasa) – actualización de la Política de Privacidad con la nueva Ley;
- ✓ remoción de comentarios de clientes en redes sociales, incluso en los ambientes propios de la marca, debido a que las hipótesis tienen que estar claramente previstas en el Término de Uso para evitar infracción de la ley (cercenamiento de la libertad de expresión), que exige una revisión del procedimiento de la empresa para administración de contenidos publicados en interacciones en los perfiles y *fanpages* en las Redes Sociales;
- ✓ observar la eventual modificación de los Términos de Uso y Política de Privacidad de las propias Redes Sociales (para atender a los requisitos del Foro Brasileño, en idioma portugués, regla para solicitar exclusión de la base de datos, limitación de responsabilidad, entre otros).

Por último, es recomendable que todos los que trabajen con proveedores de Tecnología y Comunicación, nacionales y extranjeros, que interactúen con datos de usuarios brasileños vía web, principalmente en lo referido a proveedores de aplicaciones, inclusive de Redes Sociales y de *Cloud Computing*, les soliciten el envío de una declaración de conformidad respecto a la nueva Ley del Marco Civil de Internet, en especial a los arts. 7.º, III y VIII; 8.º, II, 11,12, y 13. Eso es muy importante para evitar riesgos jurídicos para la empresa y eventual no conformidad señalada en auditoría.

Sea en Brasil o en otros países, especialmente en Europa, el tema iniciado por el Marco Civil de Internet se debe seguir de cerca, pues debe generar repercusiones, eventuales reglamentaciones, y hasta nuevas leyes sobre protección de datos en la *web*. ¡Es bueno no perderlo de vista!

Tabla resumen de los Principales efectos legales del Marco Civil alineados con la tendencia mundial Sociedad Abierta

Efecto	Previsión Legal
Extraterritorialidad	Art. 11, § 1º, § 2º
Deber de Ley y Foro Brasileño	Art. 7º, XIII, art. 8º, párrafo único, II, art. 11, § 3 º, § 4 º, art. 19, § 2º
Garantía de la libertad de expresión y no remoción de contenidos	Arts. 3º, I, 18, 19, 20, 21

Protección Privacidad	Art. 3º, II, III, art. 7 º, I, II, III, VII, VIII, *c*, IX, X, art. 8º, párrafo único, I, art. 10, § 1º, § 2º, § 3º, § 4º, art. 16, II, art. 23
Garantía de la Neutralidad	Art. 3º, IV, art. 9º
Garantía de la Calidad de Conexión	Art. 3º, VII, art. 7 º, VI, XI, XII
Garantía del Derecho de Acceso a internet e inclusión digital	Art. 4º, I, art. 7 º, IV, V, art. 24, art. 25, art. 28
Garantía del Uso de Software Libre (estándares abiertos)	Art. 4º, IV, art. 24, V
Deber de conservación de pruebas electrónicas	Arts. 13, 14, 15, 16, 22
Deber de Protección de Niños y Adolescentes en la Web	Art. 21, art. 29, *caput*
Deber de Educación	Art. 26, art. 27, art. 29, párrafo único

Penalidades por incumplimiento	Art. 11, § 4 º y 12, I, II, III, IV

Autoría: Dra. Patricia Peck Pinheiro, 2014.

Tabla resumen de los Segmentos de Negocios afectados por el Marco Civil y que necesitan hacer ajustes para adecuarse a la propuesta de mayor apertura, libertad, transparencia, colaboración y compartición

Segmento	Previsión legal del Marco Civil de Internet
Telecomunicaciones	Art. 3º, IV Art. 7º, II Art. 9º, § 1º, II, §2 º III y IV, §3 º Art. 10, § 1º, § 2º Art. 12
Proveedores de Conexión *Web*	Art. 7º, II, III, IV, V, VI, VII, VIII (*a*, *c*), IX, X, XI, XII Art. 9º, § 1º, II, § 2º III y IV, § 3º Art. 10, § 1º, § 2º, § 4º Arts. 11, 12, 13, 14 y 18

Proveedores de Aplicaciones *Web*, Portales y *Sites* (contenido), Redes Sociales	Art. 7º, II, III, IV, V, VI, VII, VIII (*a*, *c*), IX, X, XI, XII Art. 8º, II Art. 10, § 1º, § 2º, § 4º Arts. 11, 12, 15, 16, 19, 20 y 21
Empresa de Almacenaje de Datos (*Storage, Cloud*)	Art. 7º, III y VIII Art. 8º, II Arts. 11 y 12 Art. 13, § 1º
Judicial	Art. 8 º, II Art. 10, § 1º, § 2º Art. 13, § 5º Art. 15, § 1º, § 2º, § 3º Art. 19, § 1º Arts. 20, 21, 22, 23
Institución Financiera	Art. 10, § 1º, § 2º

	Art. 13, § 5º Art. 9º, § 3º Art. 10, § 1º, § 2º Arts. 16 y 22
Comercio Electrónico	Art. 7º, VIII, XIII Art. 16
Administración Pública	Art. 3º, VIII Art. 4º, I y IV Art. 9º, II Art. 25, II, III, V
Empresa de TI	Art. 24, V, VII Art. 29
Policía y Ministerio Público	Art. 10, § 3º Art. 13, § 2º, § 3º y § 5º Art. 15, § 2º y § 3º
Empresa de Medios Digitales	Art. 7, VIII (*a*, *c*), IX, X

	Art. 16 Art. 31
Instituciones de Enseñanza Públicas y Privadas	Art. 24, VIII y IX Art. 26 Art. 27 Art. 29, párrafo único
Todas las empresas	Art. 9º, § 3º (enrutamiento) Art. 10, § 4º Art. 19, § 2º Arts. 21 y 22

Autoría: Dra. Patricia Peck Pinheiro, 2014.

CAPÍTULO TERCERO

LOS NUEVOS MODELOS ECONÓMICOS EN LA REALIDAD DIGITAL

LOS DATOS SON LA NUEVA MONEDA DIGITAL

Aristides Tranquillini Neto

En los últimos años, Internet tuvo un aumento significativo de popularidad, especialmente por su accesibilidad. Fueron diversos los motivos responsables de tal expansión, que inclusive es tema de estudios, tesis y teorías abocados a entender el fenómeno. Sin embargo, es posible afirmar que la masificación de dispositivos tecnológicos con capacidad de conexión, la mejoría en las tecnologías de comunicación, el abaratamiento en los precios y la disponibilidad de esas novedades fueron factores decisivos cada vez en más lugares.

Con un público creciente y sin perspectiva de desacelerar el ritmo, Internet sé mostró un óptimo lugar para negocios, atrayendo la atención de personas y empresas interesadas en invertir en ese mercado pionero y emergente.

Enseguida comenzaron a surgir en Internet diversas empresas alcanzando niveles inesperados de éxito, generando millones de dólares de ingresos. Una de las características que esas empresas tenían en común y que dejaban a muchas personas confundidas y perplejas fue el hecho de que

generaban esas ganancias millonarias ofreciendo servicios gratuitos a los usuarios.

A pesar de que actualmente sea de conocimiento del público en general que una de las formas más eficaces de que servicios gratuitos generen lucro es por medio de anuncios dirigidos a sus usuarios, en aquella época tal concepto era extremadamente nuevo, siendo de difícil asimilación por parte de las personas que aún no comprendían la magnitud que Internet llegaría a tomar.

La innovación de los anuncios dirigidos rompió paradigmas. Antes de Internet, cuando una empresa decidía anunciar producto o servicio, no tenía muchos filtros a disposición para delimitar su público objetivo, sino tan sólo espectros amplios e inmutables que estaban genéricamente asociados a este, tales como el medio seleccionado o el horario específico.

A título de ejemplo, en caso de que una empresa quisiese anunciar su nuevo carro deportivo, tendría pocas opciones para garantizar el alcance del público deseado. Las opciones en aquella época permitían intentar delimitarlo a través del medio segmentado, con anuncios en revistas de automóviles, por ejemplo. Lo que es más, la publicidad podría ser ignorada por miles de personas que, a pesar de interesarse por carros, prefieren otros modelos que no son los deportivos.

La alternativa sería el uso de medios más generalizados, pero en un horario específico, anunciando en la televisión cuando la empresa creía que era el momento en que su público objetivo estaría viéndola. Sin embargo, el anuncio también podría ser fácilmente ignorado por miles de personas que no se encajan en el perfil de interés o simplemente no se interesan en carros.

En otras palabras, los anuncios hasta entonces exigían un gran esfuerzo y aporte de capital sin garantía de retorno en la misma proporción, ya que para alcanzar una pequeña parcela era necesario apuntar a un público gigantesco.

Por mucho tiempo fue (y aún es) así que las empresas se comunicaban con su público, siendo inclusive, por causa de esa práctica, que surgió la famosa expresión "horario estelar".[13]

Los anuncios dirigidos, por otro lado, permiten alcanzar al público objetivo con precisión quirúrgica a precios considerablemente menores, ya que, gracias a la interactividad de Internet, pasó a ser posible proporcionar experiencia individualizada, teniendo como base perfiles construidos a partir de la recolección y análisis de datos de cada usuario.

De esa forma, para que las empresas pudiesen ofrecer anuncios dirigidos, pasó a ser necesaria la recolección de datos personales de los usuarios (como los contenidos más visualizados y los hábitos de compra), para entender su comportamiento y conocer sus áreas de interés.

Para alcanzar ese objetivo, las empresas pasaron a desarrollar una extensa gama de servicios gratuitos que, cuando son utilizados por los usuarios, automáticamente colectan informaciones relacionadas. Con ello surgieron herramientas de búsqueda, e-mails, redes sociales, repositorio y visualización multimedia (incluyendo fotos, videos y música), juegos, aplicaciones de comunicación instantánea y muchos otros ítems que hoy son tan comunes en el día a día de cualquier persona.

Con la popularización de los servicios – en gran parte por ser gratuitos – las empresas pudieron construir bases de datos gigantescas y extremadamente detalladas, que permitían la venta de anuncios no sólo con precios bastante reducidos, sino también vinculando el pago al "clic"

[13] Se trata de un bloque de programación exhibido durante las noches y en el horario de comer, cuando la audiencia es mayor. En Brasil, el horario estelar está entre las 18h y 00h, teniendo como "pico" el horario entre las 20h y 23h.

del usuario, garantizando al anunciante que él sólo tendría que pagar por los anuncios que diesen algún retorno.

Buscando enriquecer esas bases de datos con informaciones cada vez más precisas de los usuarios, las empresas pasaron a adoptar actitudes más agresivas para garantizar la recolección de datos, siempre generando polémicas en el proceso, tal como ocurrió con Google,[14] Twitter,[15] Apple[16] y Facebook.[17]

Teniendo en cuenta que la privacidad es considerada derecho fundamental en la gran mayoría de los países – incluyendo Brasil[18] – comenzaron a surgir legislaciones y entendimientos jurisprudenciales sobre lo que podría ser considerado lícito en el acto de recolección y almacenamiento de datos personales.

En Brasil, podemos señalar el Marco Civil de Internet (Ley 12.965/2014) como legislación vigente que trata el tema relacionado a la recolección de datos por Internet, siendo válido destacar también el Anteproyecto de la Ley de Protección de Datos, que fue habilitado para consulta en

[14] Con el lanzamiento del servicio de e-mail "Gmail", hubo una gran polémica relacionada al hecho de que Google supuestamente analiza el contenido de los e-mails de los usuarios para poder ofrecer publicidad. Tal polémica solo disminuyó con una actualización de los términos de servicio y el esclarecimiento de que ese análisis era hecho automáticamente por *bots*, sin involucrar a seres humanos.

[15] Twitter fue cuestionado al declarar que su aplicación para dispositivos móviles colectaría informaciones relacionadas a qué aplicaciones el usuario había instalado en su dispositivo.

[16] En 2011, Apple se envolvió en una polémica con sus iPhones, los que estarían guardando el historial de todos los lugares donde el usuario estuvo. A través de una actualización en el sistema operativo, la empresa corrigió la cuestión.

[17] Desde 2013, Facebook pasó a señalar que haría revisiones en la forma cómo las empresas utilizan su herramienta "Insights" para monitorear marcas en la red social. Las modificaciones fueron reglamentadas y pasaron a valer a partir de mayo de 2015, por medio de las cuales un cambio en la API de la red social impidió el monitoreo de los muros o actualizaciones públicas de los usuarios, o sea, ninguna herramienta de monitoreo de redes sociales podría capturar las declaraciones de los usuarios de Facebook.

[18] Vale observación sobre lo dispuesto en la Constitución Federal:

"Art. 5.º Todos son iguales ante la ley, sin distinción de cualquier naturaleza, garantizando a los brasileños y a los extranjeros residentes en el País la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los términos siguientes:

(...)

X – son inviolables la intimidad, la vida privada, la honra y la imagen de las personas, asegurado el derecho a la indemnización por el daño material o moral derivado de su violación;"

plataforma propia el día 28.1.2015[19] y trata el tema de forma más amplia, abarcando la recolección de datos por cualquier medio y no solo a través de Internet, y el Código de Defensa del Consumidor (Ley 8.078/1990), que determina la necesidad de que el consumidor autorice previamente la creación de un banco de datos respecto a él, al cual se podrá acceder en cualquier momento[20].

El surgimiento de legislaciones o proyectos de leyes es resultado de la creciente atención que la recolección y almacenamiento de datos pasó a tener en los últimos años, siendo consecuencia no sólo del éxito obtenido por empresas que ejercen esa práctica, sino también por los escándalos relacionados al espionaje practicado por la *National Security Agency* – NSA (Agencia de Seguridad Nacional) del gobierno estadounidense, la cual tuvo acceso a bancos de datos de diversas empresas de tecnología, tales como Google y Yahoo!, alertando a las personas respecto a cuánto podrían revelar informaciones consideradas simples y aisladas cuando son analizadas en conjunto.

Por ese motivo, varias empresas comenzaron a creer que la creación y manutención de bancos de datos conteniendo las informaciones recolectadas de sus clientes y/o usuarios sería el próximo negocio del futuro y, por tanto, en caso de que recibiese inversión ahora, tendrían un buen chance de enseguida comenzar a generar ingresos.

El gran desafío por superar, cuando se adopta esa línea de pensamiento, es que muchas veces la empresa puede verse compelida a iniciar una recolección desenfrenada de todos los datos de clientes/usuarios a los que

[19] Plataforma a la que se accedió a través del sitio [http://participacao.mj.gov.br/dadospessoais/].

[20] "Art. 43. El consumidor, sin prejuicio de lo dispuesto en el art. 86, tendrá acceso a las informaciones existentes en inscripciones, fichas, registros y datos personales y de consumo archivados sobre él, así como sobre sus respectivas fuentes.
(...)
§ 2.° La apertura de inscripción, ficha, registro y datos personales y de consumo deberá ser comunicada por escrito al consumidor, cuando no es solicitada por él."

pueda tener acceso,[21] sin poseer propósito u objetivo específicos, hasta decidir cómo podrá obtener retorno financiero de aquella actividad.

Tal actitud no es correcta y debe ser completamente evitada, ya que trae consecuencias tanto jurídicas como financieras. Para comprender mejor la razón por la cual empresas no deben adoptar esa política agresiva en la recolección de datos – realizando primero la recolección para después decidir qué hacer con los datos en vez de tener un plan trazado y colectar las informaciones para atender a esa propuesta – analizaremos brevemente a continuación las consecuencias jurídicas y financieras de tal actitud.

En el aspecto financiero, es importante resaltar que realizar la recolección, almacenamiento y curaduría de los datos no es tarea sencilla ni barata, ya que depende de inversiones considerables en infraestructura, softwares y personas capacitadas para trabajar en el ramo. En caso de que la empresa no tenga una finalidad específica cuando realiza la recolección o un plan claro para la utilización de los datos – como Google y Facebook, cuyos servicios orbitan en torno a la obtención y uso de datos –, acabará resultando en la realización de grandes inversiones con bajo o ningún retorno financiero.

El segundo aspecto que observar es el jurídico. A pesar de ser bastante reciente, y aún no tan abordado en profundidad en ciertos aspectos, ya existen leyes que tratan sobre las medidas a adoptar por empresas que prestan servicios en Internet y realizan la recolección de datos, siendo la más relevante, en este momento, la ley que instituyó el Marco Civil de Internet.

[21] En ese sentido, vale citar el concepto de dos términos importantes cuando se habla de recolección y tratamiento de datos: "big data" y "junk data". *Big data* supone gran almacenamiento de datos y mayor velocidad, centrándose en cinco aspectos: velocidad, volumen, variedad, veracidad y valor. *Junk data*, por su parte, son los datos imprecisos o inútiles, siendo así considerados aquellos que, cuando compilados con un gran número de datos, no atienden a los parámetros necesarios, siendo generalmente descartados para mantener la integridad de los demás dados.

El Marco Civil de Internet establece directrices generales a seguir, entre las cuales vale destacar algunas disposiciones respecto a la recolección y almacenamiento de datos:

(i) La empresa no puede suministrar los datos recolectados a terceros, salvo si hubiera consentimiento expreso del usuario;[22]

(ii) La empresa debe suministrar informaciones claras y completas sobre cómo los datos recolectados serán utilizados, almacenados o tratados, siendo necesario que justifiquen el motivo de su recolección;[23]

(iii) Es necesario que las informaciones sobre la recolección y uso de los datos aparezcan en forma destacada de las demás cláusulas contractuales, garantizando así el consentimiento del usuario;[24] y

(iv) La eliminación definitiva de los datos a pedido del usuario.[25]

---

[22] "Art. 7.º El acceso a internet es esencial para el ejercicio de la ciudadanía, y al usuario les son asegurados los siguientes derechos:
(...)
VII – no suministro a terceros de sus datos personales, inclusive registros de conexión, y de acceso a aplicaciones de internet, salvo mediante consentimiento libre, expreso e informado o en las hipótesis previstas en ley;".

[23] "Art. 7.º. (...)
(...)
VIII – informaciones claras y completas sobre recolección, uso, almacenamiento, tratamiento y protección de sus datos personales, que solamente podrán ser utilizados para finalidades que:
a) justifiquen su recolección;
b) no sean vedadas por la legislación; y
c) estén especificadas en los contratos de prestación de servicios o en los términos de uso de aplicaciones de internet;"

[24] "Art. 7º. (...)
(...)
IX - consentimiento expreso sobre recolección, uso, almacenamiento y tratamiento de datos personales, que deberá ocurrir de forma destacada de las demás cláusulas contractuales;"

[25] "Art. 7.º. (...)
(...)
X – eliminación definitiva de los datos personales que hubiera proporcionado a determinada aplicación de internet, a pedido suyo, al término de la relación entre las partes, exceptuando las hipótesis de conservación obligatoria de registros previstas en esta Ley;"

Como se nota, la legislación vincula la recolección de datos a la existencia de algún propósito, el cual debe ser informado al usuario de forma clara, previa y completa, junto con qué datos serán recolectados y para qué finalidades serán utilizados, no siendo permitido transferirlos a terceros sin su consentimiento previo y expreso.

De esa forma, no tiene sentido iniciar la recolección de informaciones para construir base de datos sin que haya finalidad o propósito específicos, ya que la empresa no podrá utilizarlos o cederlos si, en el momento de la recolección, no informó las intenciones al usuario, haciendo su utilidad ser cuestionada. Es importante resaltar que actuar de otra forma – cediendo los datos o utilizándolos de forma diferente a lo informado a los clientes – es considerado acto ilícito y podrá generar consecuencias jurídicas para la compañía.

A pesar de que la legislación parezca demasiado restrictiva, uno de sus propósitos es exactamente el de proteger la privacidad de los usuarios,[26] lo que es hecho al garantizar transparencia en la recolección, uso y tratamiento de los datos, que muchas veces poseen naturaleza sensible.

Ante lo expuesto, es de extrema importancia que las empresas no se dejen llevar por el frenesí causado por la popularidad de los bancos de datos de informaciones personales, siendo recomendado que no los recolecten de manera desenfrenada sólo para participar del mercado, así como que estén atentas a la tramitación del Anteproyecto de la Ley de Protección de Datos, cuya redacción podrá impactar directamente a varios modelos de negocios.

Como fue demostrado, no se aconseja recolectar primero los datos para después decidir qué hacer o cómo obtener retorno financiero, siendo necesario primeramente trazar su plan de negocio, verificando si datos personales son necesarios para los productos o servicios y, en base a eso, delinear la mejor estrategia para su recolección, dejando muy claro qué

[26] Art. 3.º La disciplina del uso de internet en Brasil tiene los siguientes principios:
(...)
II – protección de la privacidad;"

informaciones serán recolectadas y cómo serán utilizadas, revisando sus políticas de privacidad para insertar esas y otras cuestiones, tales como la conservación de los datos en servidor en Brasil o fuera del país, uso de servicios subcontratados de *cloud computing*, procedimientos de enriquecimiento y tratamiento de datos, así como la compartición con empresas del mismo grupo.

LAS OPORTUNIDADES DE PARTICIPACIÓN DE LAS MARCAS EN LOS DEBATES PÚBLICOS DIGITALES Y EL MARKETING 3.0

Victor Varcelly Medeiros Farias

Desde finales de la década de los noventa, oponiéndose al Proyecto de Ley Azeredo (PL nº 84/1999), la sociedad brasileña, principalmente el área jurídica y la sociedad civil organizada, defensora de los derechos de los consumidores y ciudadanos[27], se ha movilizado en torno a la producción de normas jurídicas específicas para Internet. A raíz de esta movilización fue elaborada la ley del Marco Civil de Internet (Ley nº12.965/2014) y se produjo su posterior reglamentación por el Decreto nº 8.771/2016. Estas normas jurídicas poseyeron una peculiaridad en su creación, pues además de la fuerte divulgación que recibieron de los medios, las minutas de sus textos fueron previamente puestas a disposición en Internet por el Ministerio de Justicia, permitiendo la contribución directa de los interesados. Al historial de las contribuciones y de los debates públicos digitales se puede acceder en el sitio Pensando el Derecho (*PoD*)[28] del Ministerio de Justicia.

[27] Proteste (Asociación Brasileña de Defensa del Derecho del Consumidor), Intervoces (Colectivo Brasil de comunicación social), Internet Lab y la FGV Derecho son algunos ejemplos de instituciones implicadas en el debate por la garantía de derechos en Internet.

[28] A todo el historial on-line de los debates citados, así como de otros puestos a disposición por el Ministerio de Justicia, se puede acceder a través de la dirección electrónica: http://pensando.mj.gov.br

PoD se constituyó en una de las iniciativas de democracia y transparencia digital del Gobierno brasileño abocadas a la participación ciudadana en las decisiones del Poder Ejecutivo[29]. Un contexto similar de incentivo a la participación popular por Internet existe en otros países de América Latina, por ejemplo, México, Argentina y Paraguay[30], que también habilitan consultas públicas digitales. Según el Ministerio de Justicia, la iniciativa busca lograr una mayor aproximación entre gobernantes, estudiosos y legisladores, aspirando así a instrumentalizar la proposición de normas jurídicas más relevantes y adecuadas a la realidad brasileña.

El hecho de que el debate no esté limitado al territorio brasileño, pudiendo tener acceso y ser complementado por cualquier usuario de Internet, hace el potencial del proceso aún más relevante en lo referido a la pluralidad de visiones, pues los usuarios de otros países pueden participar previendo riesgos y beneficios aún no existentes en Brasil y aportando sus experiencias personales para ampliar el debate. De esa forma, la habilitación digital de los debates sobre la regulación de Internet en el país se probó un formato innovador en lo referido a la ampliación de la oportunidad de participación del público, en especial de los usuarios de Internet.

Cualquier persona, conectada a internet, puede registrarse en *PoD*, informando nombre completo y dirección de e-mail, y participar en los debates habilitados enviando comentarios y respuestas o haciendo clic en las opciones estoy de acuerdo y no estoy de acuerdo[31] disponibles en el sitio. En algunos debates, *PoD* permitió la creación libre de pautas[32]

[29] Otras iniciativas ciber-democráticas del Gobierno brasileño a destacar son e-Cidadania (https://www12.senado.leg.br/ecidadania/) y e-Democracia (https://edemocracia.camara.leg.br/home)

[30] Mayores informaciones sobre las consultas pueden ser obtenidas en los enlaces siguientes, a los que se accedió el 2 de julio de 2017: www.gob.mx/participa/consultas; consultapublica.argentina.gob.ar/participacion y www.conatel.gov.py/index.php/consulta-publica.

[31] Las funciones de estoy de acuerdo y no estoy de acuerdo son semejantes al me gusta presente en diversos sitios de redes sociales digitales como *Facebook*, *YouTube* e *Instagram*.

[32] Las pautas funcionan de manera similar a las herramientas de foros on-line, pero poseyendo temáticas previamente definidas por el Ministerio de Justicia. En el caso de la reglamentación del MCI, el Ministerio de Justicia habilitó 4 ejes temáticos (neutralidad, privacidad en la red, conservación de registros y otros temas y consideraciones) en los cuales los usuarios podían crear textos y proposiciones propias.

dentro de ejes temáticos predefinidos que influenciarían la redacción de la primera minuta del texto propuesto por el Ministerio de la Justicia.

En base a los requisitos de registro de *PoD* es posible verificar que los debates públicos propuestos en este sitio no se encuadran en ninguno de los modelos de consulta pública previstos en el artículo 14 de la Constitución de la República Federativa de Brasil de 1988[33]. Las herramientas previstas en el artículo 14 de la Constitución están abocadas exclusivamente a la participación del ciudadano brasileño, o sea, el individuo detentor de derechos políticos, comprobados estos en el ordenamiento jurídico brasileño por la obtención del título de elector, documento no obligatorio para el registro o acceso del usuario a *PoD*. De esa forma, los debates del *PoD* no son exclusivamente dirigidos a personas físicas o a ciudadanos brasileños, ya que están disponibles en internet sin la exigencia de comprobación de nacionalidad por el participante o la configuración de cualquier impedimento a la creación de perfil institucional. Teniendo en cuenta la no previsión legal de su formato o efectos, es posible afirmar que *PoD* no funciona como una herramienta capaz de vincular al Ministerio de Justicia con las contribuciones presentadas por sus usuarios. Las contribuciones sólo enriquecen e instrumentalizan la decisión del Ministerio de Justicia con relación a la temática puesta en debate. A pesar del carácter no vinculante, *PoD* ofrece una gran oportunidad a las personas jurídicas al hacer público el historial digital de los debates, conteniendo la expresión autónoma del posicionamiento de la marca sobre la temática puesta en discusión.

Los debates fueron además divulgados por los medios de comunicación de masa y canales de creadores autónomos y especializados de contenido de la propia Internet, como participantes de sitios de redes sociales digitales, listas de e-mails, foros de debates y otros, brindando mayor visibilidad a los temas, como la protección a la privacidad y a la libertad de expresión, y a las marcas participantes. Es en este punto entre

[33] CF, Art. 14. La soberanía popular será ejercida por el sufragio universal y por el voto directo y secreto, con valor igual para todos, y, en los términos de la ley, mediante: I - plebiscito; II - referendo; III - iniciativa popular.

producción de contenido y divulgación de marcas que el Marketing 3.0[34] (Kotler 2010) y los debates en *PoD* se cruzan.

La implicación en los debates hace viable la creación de nuevas misiones y posicionamientos de la marca pautados en el respeto y la transparencia, además de fortalecer e incentivar prácticas gubernamentales que favorecen el empoderamiento del consumidor ciudadano, principalmente en lo referido a la defensa de los derechos de los usuarios en Internet y de los valores abocados a la transformación positiva del mundo y de la sociedad en los moldes del llamado Marketing 3.0 (Kotler 2010).

La presentación y defensa de derechos como la privacidad del usuario y la neutralidad de la red previstos en el MCI traducen valores claros de defensa por un mundo mejor con énfasis en la conciencia sobre el uso de las herramientas de Internet y en sus consecuencias para el usuario común, siendo una clara posibilidad de actuación de la institución en la esfera del Marketing 3.0, demostrando además implicación en el debate jurídico, social y tecnológico, además de empoderar la participación del consumidor, transformándolo en un verdadero colaborador y defensor de la marca (KOTLER,2010).

Por último, es indispensable que la defensa y la implicación de la institución en la protección del usuario de Internet sean posturas coherentes con la actuación de la marca, fortaleciendo la transmisión de estos valores hasta el consumidor final. Acciones interactivas que incentiven el empoderamiento del consumidor, la creación de informes temáticos didácticos, la rápida implementación de los derechos digitales

[34] Kotler (2010) presenta tres modalidades de marketing que surgieron con el paso de los años, debido a los cambios comunicacionales y mercadológicos de las últimas décadas. El marketing 1.0 es abocado al producto, en el cual la industria crea un nuevo producto y construye el mercado después. O sea, las acciones de comunicación buscan crear la necesidad de aquel nuevo producto en la vida de los consumidores. El Marketing 2.0 posee una vertiente un poco diferente, con el énfasis de la producción de la industria en las ganas y deseos del consumidor en aquel momento. Como modalidad más reciente del Marketing, Kotler presenta el Marketing 3.0, que además de las vertientes industriales y de producción de productos, posee un posicionamiento diferenciado transcendiendo la industria y abocándose a la creación de un mundo mejor. Acciones pautadas en el Marketing 3.0 incluyen la defensa y la divulgación de valores admirados, esperados por la sociedad y, es claro, coherentes con los valores de la institución.

aportados por el MCI en la Política de Privacidad de aplicaciones y sitios, el abordaje más innovador y menos amigable de los documentos gigantescos de Términos de Uso o incluso piezas publicitarias basadas en una historia sólida y coherente con la misión de la marca son instrumentos interesantes para la efectiva participación de las instituciones en este momento de gran oportunidad en Brasil y en América Latina que une tecnología, valores, derecho y publicidad.

Referencias

BRASIL. Constituição (1988). Constituição, de 05 de outubro de 1988. **Constituição Federal**. Disponible en: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acceso en: 03 mayo 2016.

BRASIL. MINISTÉRIO DA JUSTIÇA. **Pensando o Direito**. Disponible en: <http://pensando.mj.gov.br/>. Acceso en: 10 jun. 2016.

Comitê gestor da internet. **TIC Domicílios**. Disponible en: <http://cetic.br/pesquisa/domicilios/>. Acceso en: 7 mayo 2016

KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. Bem-vindo ao Marketing 3.0. In: KOTLER, Philip; KARTAJAYA, Hermawan. **Marketing 3.0**. Río de Janeiro: Campus, 2010. Cap. 1. p. 3-28.

KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. O marketing da missão junto aos consumidores. In: KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. **Marketing 3.0**. Río de Janeiro: Campus, 2010. Cap. 3. p. 57-78.

LA REGLAMENTACIÓN DE LOS ACUERDOS DE PAGO

Aristides Tranquillini Neto

En esta era en que Internet está más presente que nunca en nuestras vidas, siendo incluso clasificada como derecho fundamental e indispensable, no es poco común la compra de productos *online*. Aunque usted sea la excepción y nunca lo haya hecho, seguramente conoce personas que lo hicieron o hacen con frecuencia.

Al menos en Brasil, la compra *online* tardó en alcanzar todo su potencial por diversos motivos, siendo uno de ellos la falta de confianza en los métodos de pago habilitados por los sitios – que, a pesar de ofrecer medios más tradicionales como talones bancarios, pueden exigir la inserción directa de los datos de tarjeta de crédito del comprador.

Con el crecimiento del universo *online*, surgieron plataformas que permiten a cualquier usuario poner a disposición productos y servicios en la red, tales como eBay y MercadoLibre. Para algunas personas, esa innovación representó una complicación y un impedimento aún mayor a la hora de la adquisición, ya que la negociación es hecha directamente con el comprador, sin toda la estructura característica de las grandes redes de comercio minorista.

Para atender ese mercado emergente, comenzaron a surgir los servicios de pago, entre los que podemos destacar Paypal, PagSeguro y Google Wallet, cuya función inicial buscaba intermediar ese tipo de relación, cuidando de la transacción entre las partes y garantizando que ninguna sepa informaciones confidenciales de la otra, tales como datos bancarios.

El modelo tuvo tanto éxito que se expandió y comenzó a abarcar más y más finalidades, siendo uno de los mayores casos de éxito de esa expansión el M-Pesa, lanzado en Kenia por la Safaricom en marzo de

2007. El M-Pesa, que viene de la junción de las palabras *Mobile* ("móvil" en inglés) y *Pesa* ("dinero" en Suajili), es un servicio financiero que permite transferir y sacar dinero, pagar servicios y comprar créditos a través del celular, sin necesidad de cuenta bancaria. El servicio respondió perfectamente a la demanda de los mercados emergentes, ofreciendo todas las funciones de una cuenta bancaria, sin la obligatoriedad de tener una. Además, la burocracia, los requisitos y las tasas de manutención de la cuenta de pago del M-Pesa son considerablemente menores y permiten una movilidad inalcanzable con los servicios bancarios, ya que todas las transacciones pueden ser hechas por celulares más simples, los algunas veces llamados *dumbphones*, a través de mensaje de texto SMS, sin necesidad de aplicaciones específicas.

Servicios de pago también pasaron a ganar más notoriedad gracias a las noticias y valoración recibida por el *Bitcoin*, moneda digital creada en 2009 por una persona anónima que se autodenominó Satoshi Nakamoto. El *Bitcoin* permite la propiedad y transferencia anónima de valores, utilizando un programa de código abierto para generación, uso y transferencia de la moneda, en que la red es de punto a punto (*peer-to-peer*), o sea, directamente entre las computadoras, sin necesidad de entidades centralizando y administrando la moneda.

Con el crecimiento de los servicios de pago y de empresas ofreciendo cada vez más medios alternativos de pago y recibimientos, tuvieron inicio discusiones respecto a la necesidad de una reglamentación específica que abarcase esas nuevas formas de circulación monetaria y las instituciones financieras por ella responsables.

De esa forma surgió la Ley 12.865 de 09.10.2013, que dispone, entre otras cosas, sobre los acuerdos de pago y las instituciones de pago que podrían integrar el Sistema de Pagos Brasileño (SPB).

Como complemento de la Ley 12.865, el Banco Central de Brasil editó las Res. 4.282/2013 y 4.283/2013 y las Circulares 3.680/2013, 3.681/2013, 3.682/2013, 3.683/2013 y 3.705/2014, responsables de la parte técnica, cuentas de pago, requisitos para funcionamiento y necesidad de registro de las instituciones financieras en el SPB.

Y, ¿qué significa eso para el usuario final, aquel que realiza una compra en un sitio y opta por pagar utilizando Paypal, PagSeguro o, quién sabe, *Bitcoins*? En principio, nada. Los usuarios finales podrán continuar usufructuando de todas las facilidades que los servicios de pago ofrecen sin preocuparse por realizar nuevos registros, obtener e-CPF (Registro de Persona Física electrónico), o abrir nuevas cuentas, pues la legislación se enfoca en medidas a ser tomadas por las instituciones financieras, y que tiene como objetivo, entre otras cosas, regularizar la manera cómo los servicios son prestados, aumentar las medidas de seguridad, evitar fraudes – tanto por parte de los usuarios como de las instituciones –, vigilar si las instituciones financieras están cumpliendo con las determinaciones, así como garantizar la interoperabilidad entre los servicios de pago, para que no haya restricciones entre acuerdos de pago, viabilizando el flujo de recursos entre ellos.

Se espera, por tanto, que a largo plazo los servicios de pago se vuelvan más seguros y viables, y que más opciones para su utilización sean difundidas, con el uso de tarjetas de pago, tanto pre como postpago, o incluso de tarjetas de débito, como fue anunciado por la empresa china Xapo, que puso a disposición de sus clientes la posibilidad de utilizar una tarjeta magnética para pagos en Bitcoin, pudiendo ser usada en cualquier tienda que acepte tarjetas Visa o MasterCard.

A pesar de que el Banco Central de Brasil aún tenga que regular ciertos aspectos de los servicios de pago, especialmente en lo que se refiere a

las transacciones con valores más elevados, en diferentes territorios e incluyendo dispositivos diversos, se nota una preocupación de las instituciones financieras, especialmente las especializadas en servicios de pago, por buscar su regularización ante el Banco Central cuanto antes, teniendo en cuenta el recelo de que sus actividades sean paralizadas frente al no cumplimiento de algún requisito.

Por otro lado, el Banco Central está buscando esclarecer y justificar las medidas tomadas, demostrando que la adecuación a la nueva legislación no exigirá grandes restructuraciones por parte de las instituciones financieras y que la obtención de autorización para funcionamiento, cuando sea necesaria, podrá ocurrir sin burocracia excesiva y a través de procedimientos considerados rápidos.

Por ese motivo los usuarios finales no deben experimentar ninguna traba, lentitud o cualquier modificación sensible con la entrada en vigor de la legislación y de las Ordenanzas y Circulares del Banco Central de Brasil, pudiendo, a largo plazo, sentir una mejora en el flujo de los servicios, su aceptación en más lugares, así como estar más seguros de que sus informaciones están más protegidas.

QUIEN ESTÁ EN CONTRA DE UBER ESTÁ EN CONTRA DEL FUTURO

Patricia Peck Pinheiro

¿Cómo mejorar el transporte en los centros urbanos? Esta es una cuestión actual y extremadamente importante. ¿Cómo reinventar la movilidad de las personas en las grandes ciudades?
Ciertamente, es posible usar la tecnología para resolver ese problema, por ejemplo, a través de aplicaciones que ofrecen servicios de transporte basados en la autoorganización, movilización, transparencia, mejora de la calidad, generación de empleo y aumento de la competencia.

Vivimos un momento de ruptura de paradigmas, en el cual debemos jubilar lo que es viejo y obsoleto para dar lugar a nuevas fórmulas. Y eso es urgente cuando se trata de transporte de pasajeros.

De ese modo, cualquier dificultad en la gestión adecuada de ese modelo implica la pérdida de competitividad (con otras ciudades de otros países), aumento del costo de vida, pérdida de empleos (pues tienden a migrar hacia lugares más propicios), además de efectos colaterales en la caída de productividad de las empresas resultantes directamente de los atrasos y del estrés causado a la salud debido a los largos tiempos de desplazamiento de los trabajadores.

Por principio, cualquier reglamentación debe tener el compromiso de seguir la evolución de la sociedad, en sus relaciones sociales y económicas.

Desde la Constitución Federal de 1988, el centro de atención pasó a ser el estímulo a la libre iniciativa para la mejoría de la calidad de vida de los ciudadanos y no la aplicación de un "Estado Proteccionista", burocrático y pesado, que acaba generando como efecto colateral la corrupción.

Siendo así, cualquier ley que represente intervención directa del Estado en la libertad de los individuos, sean personas físicas o jurídicas, debe ser cuidadosamente medida, para que no exceda el límite legítimo de la protección del mercado, de los consumidores, de los minoritarios.

Lo que debe prevalecer es la ley de la oferta y la demanda. Si, por un lado, existe la necesidad de más oferta de servicio de transporte, y si, por otro, es viable que eso ocurra a través de inversión privada, sin uso de recursos públicos, la discusión debe pasar a ser entonces tan sólo sobre cómo implantarlo de modo que cumpla requisitos de seguridad y protección de los usuarios-clientes.

Por eso, estará fuera de lugar cualquier acción en el sentido de proteger un pequeño grupo favorecido por el monopolio previamente establecido,

siendo inadmisible cercenar la competencia que sólo tiende a generar beneficios para los usuarios.

Según Saskia Sassen, socióloga holandesa, las Ciudades Digitales deben reinventarse, pues, para servir a sus ciudadanos, necesitan de una gran inversión en energía, telecomunicaciones, tecnología, transporte, vivienda, educación y salud.

En los últimos años, todas estas tareas migraron desde lo público hacia lo privado. Por tanto, ya no tiene sentido este Estado centralizador y recaudador. ¿Cómo podría continuar cobrando altos impuestos por lo que ya no está entregando, después de las privatizaciones?

Los segmentos regulados surgieron sólo como una fórmula para cohibir abusos, excesos que pudiesen ser perjudiciales al ciudadano o al consumidor. Los mercados libres necesitan tan sólo transparencia y reglas claras para desarrollarse.

Claro que para un servicio como Uber es necesario que haya un registro para control de conductores, y tener algunos requisitos en lo referido a la seguridad del vehículo (que sea un carro en buen estado, por ejemplo). Todo eso la propia aplicación ya lo exige a sus participantes.

También es muy natural que deba recoger impuestos, como cualquier servicio, pero en ese sentido hay una tendencia internacional en migrar a un impuesto único, sobre consumo (sea de producto o servicio), disminuyendo la carga tributaria y nuevamente aumentando la capacidad de crecimiento de la propia economía.

Esa coyuntura se está dando también en otros segmentos. Salimos de la producibilidad, donde todo se volvía un producto, para la *service society*, donde todo se transforma en servicio, pago en la forma de una mensualidad continua. Del software con SAAS (Software as a Service) a Netflix.

Ese cambio viene aportando más acceso al contenido de forma legalizada, lo que ayuda a combatir el mercado paralelo de la piratería.

Además, impacta sobremanera en el costo final para el consumidor, pues se migra de la carga tributaria absurda de casi 40% a algo cercano al 11%.
El Brasil de la Era Digital sólo va a retomar el crecimiento si dejamos en el pasado los modelos viejos y obsoletos. Que surjan muchas más iniciativas como Uber, para que reinventemos el país. Quien está en contra de iniciativas como la de Uber está en contra del futuro.

CAPÍTULO CUARTO
NUEVOS RIESGOS EN LA SOCIEDAD INFORMATIZADA

ACOSO DIGITAL
Patricia Peck Pinheiro

¿Qué hacer si un prestador de servicios o un encargado de Servicio de Atención al Cliente que tuvo acceso a sus datos comienza a perseguirle en Internet, en las Redes Sociales y hasta en el WhatsApp?

Ha crecido el número de casos en que clientes son acosados por empleados de grandes marcas después de haber recibido algún tipo de atención por estos.

En general, el *modus operandi* es siempre el mismo: con el término de la prestación de servicio, comienza a haber envío de mensajes en un tono más íntimo y, dependiendo de la reacción del cliente, ocurren hasta casos de amenaza e intimidación.

¿Qué hace pensar a un empleado que atiende a un cliente de la empresa en la cual trabaja que tiene el derecho de aprovecharse del contacto para conseguir algo más?

¿Cómo las propias empresas pueden identificar mejor este tipo de perfil y prevenir esos incidentes? ¿Qué ha pasado con quien se pasa del límite en la relación de atención con el consumidor o abusa del uso de los datos personales de un cliente?

Una adolescente de 14 años fue víctima de un incidente así. Días después de llevar el celular para arreglar la pantalla en la asistencia técnica, comenzó a recibir en su WhatsApp videos y fotos del empleado que la atendió en escenas de desnudez y de sexo explícito.

En otro caso, la consumidora necesitó llamar a un técnico de la prestadora de servicio de TV por cable. Terminada la visita, el empleado comenzó a abordarla vía mensajes extremadamente indecentes y hasta amenazadores, con insinuaciones como "qué linda eres", "quieres salir conmigo" y hasta "yo sé dónde tú vives".

Ciertamente, toda falla del personal de atención es siempre una falla de los líderes. La empresa responde civilmente por dos tipos de culpa, que involucra la selección del empleado (*culpa in elegendo*) y por la vigilancia y supervisión del trabajo (*culpa in vigilando*).

En la ley brasileña hay previsión de responsabilización del empleador por mala conducta del empleado, art. 932 del Código Civil Brasileño, y hasta del gestor (jefe) por no haber supervisado a su equipo adecuadamente, art. 1016 de la misma legislación.

Sin embargo, no basta solamente con dimitir al empleado. Independientemente de cuánto la empresa invierta en el entrenamiento de sus equipos o de la penalidad que imponga al trabajador que incumpla las reglas de conducta, es necesario que haya indemnización por daño moral y material causados, pues la víctima tiene que ser resarcida de algún modo del trauma que sufrió.

Pero ¿por qué será que aumentó tanto ese tipo de incidencia? ¿Estamos seleccionando mal? ¿Entrenando poco? ¿Faltando con el deber de supervisión laboral? En un país en crisis, de recortes de costos, con toda seguridad, esos casos pueden ser reflejo de la disminución de inversión en el sector de personal.

¿O es la facilidad de las nuevas tecnologías la que está provocando la cultura del exceso de acceso, que es un efecto colateral de la propia súper exposición en que vivimos?

Para que ese comportamiento deje de producirse, todos nosotros, consumidores y clientes de grandes marcas, debemos estar más vigilantes con el uso de nuestros datos personales, verificando la política de privacidad de la empresa antes incluso de la compra o de la contratación del servicio, y cuestionando cuál es el nivel de seguridad de mi información dentro de aquella empresa.

Además, la víctima debe denunciar. La actitud de "déjalo pasar" acaba estimulando aún más la mala conducta, debido a la sensación de impunidad del infractor.

Muchos clientes acosados digitalmente por dependientes, vendedores y técnicos tienen miedo de hablar sobre lo que está ocurriendo y de sufrir

algún tipo de represalia, principalmente si el desenlace genera la dimisión del empleado, que en el futuro puede querer vengarse.

La mejor protección aún es la información. Cuantas más personas sepan lo que pasó, mejor. Cuanto más documentado esté el hecho, más segura está la víctima, pues el agresor tiende a retroceder cuando percibe que ella no se intimidó.

¿Qué puede hacerse para intentar evitar situaciones como esa? La primera gran recomendación es nunca recibir un prestador de servicio estando solo en casa. Es bueno siempre llamar a alguien más, sea un vecino o el conserje, para no estar solo el cliente y el empleado. La presencia de un testigo ayuda a minimizar el abordaje indebido.

Otra recomendación es siempre pedir el nombre al empleado y su función. Lamentablemente, debido al abuso de algunos, es preferible ser más seco en el trato. El mero gesto de una sonrisa, u ofrecer agua o un café, ya puede ocasionar un abordaje más personal.

Además, mantener la puerta de la casa abierta mientras el prestador esté haciendo la visita también puede ayudar.

Evite dejar a la persona sola, hablar por teléfono o hacer otra cosa que pueda desviar la atención, pues eso puede facilitar una situación de riesgo de hurto o, peor aún, de abordaje sexual forzado, como violación.

Independientemente de la acción de las víctimas, que deben, sí, buscar sus derechos y la justicia, existe el deber de actuar del propio Ministerio Público para castigar esos abusos, dado el enorme número de incidencias en los últimos tiempos; de actuar en defensa de los consumidores

brasileños, exigiendo incluso término de ajuste de conducta de las empresas en los lugares donde es alto el índice de esos incidentes.

La falta de respeto con clientes puede encuadrarse, dependiendo de las evidencias, en los crímenes de coerción ilegal, amenaza, acoso sexual y daño. Es fundamental registrar la denuncia y echar a andar la investigación policial, incluso para que el infractor pierda la condición de no tener antecedentes penales, lo que ayuda a evitar que se repita el abuso con otra persona.

Un cliente no puede sentirse inseguro de esa manera. ¡Decir que el caso será investigado no basta! Tiene que haber una punición ejemplar, bajo pena de falta de respeto y de educación en los ambientes de trabajo, en especial para los que tratan con consumidores finales. Es necesario transformar a Brasil en una gran selva urbana y digital.

POR DETRÁS DE LAS BARRAS: ¿CÓMO FUNCIONAN Y CÓMO DEFENDERSE DE LOS FRAUDES DE PAGO POR CÓDIGO Y TRANSFERENCIAS ELECTRÓNICAS?

Márcio Mello Chaves

Quien paga mal, paga dos veces [1]. Este proverbio antiguo y popular en el medio jurídico que se encuentra estampado en el Código Civil [2] debe tenerse siempre en mente al efectuar pagos por medios electrónicos, debido a los cada vez más complejos y osados fraudes digitales.

Además de las ya populares estafas con talones bancarios falsos, los fraudes involucrando diferentes tipos de cuenta e incluso transferencias bancarias internacionales han traído perjuicios de billones de reales [3]. A pesar de poseer diferentes *modus operandis*, los incidentes suelen tener dos detalles en común: los malhechores se aprovechan de la falta de

atención por parte de las víctimas, que difícilmente logran que se repare sus perjuicios.

El motivo del gran éxito de esos nuevos tipos de fraude involucrando el pago por medios electrónicos es simple: los usuarios se olvidan de que los estafadores también se valen de la facilidad aportada por los dispositivos tecnológicos, pero para la práctica de delitos. Independientemente de la forma, esas estafas suelen perjudicar a las dos partes involucradas en la transacción financiera. El comprador, que, por no conseguir efectuar el pago, se ve obligado a repetir la operación; y el vendedor, por tener su nombre implicado en un esquema fraudulento, aunque sin su participación o cualquier responsabilidad comprometida.

Inicialmente apodado de "estafa del talón bancario", el fraude ganó realce en el ambiente empresarial por aprovecharse del descuido de los sectores de cuentas a pagar y por frecuentemente envolver pequeños valores. Así, digitando los códigos de barra adulterados y no revisando la cuenta del destinatario, los pagos son efectuados y el fraude sólo es descubierto cuando la cuantía en abierto es cobrada nuevamente por el acreedor.

Al inicio de esas estafas el falso acreedor estampado en el documento solía hacerse pasar por órganos oficiales en la recogida de impuestos. En el caso de los fraudes actuales, se ha utilizado empresas comunes, especialmente operadoras de tarjetas de crédito e instituciones financieras, además de prestadores de servicio en general, proveedores y compradores en el caso de las negociaciones hechas por *e-mail*.

Los medios utilizados para aplicación de la estafa son los más variados y están en constante evolución. En el medio físico, los estafadores envían los talones adulterados a las direcciones de las víctimas, directamente o por medio de la participación de cómplices en empresas de transporte de

correspondencias. En el caso del ambiente digital [4], el sitio generador del talón es falso o está infectado por virus que adulteran los códigos de digitación, o el propio equipo de la víctima tiene virus que modifican tales números entre su generación en el equipo y su visualización en la pantalla, dificultando su identificación inmediata. Y el fraude no se resume sólo a las transacciones nacionales tradicionales: negociaciones realizadas por *e-mail* con proveedores y compradores extranjeros pueden ser monitoreadas por *hackers* que utilizan códigos maliciosos para interceptar las comunicaciones y adulterar datos bancarios de la cuenta destino del pago. Independientemente del medio utilizado, una vez ocurrido el fraude, ¿de quién es la responsabilidad por el perjuicio sufrido?

Indiscutiblemente, está la responsabilidad del ejecutor del fraude o estafador, esté él implicado directa o indirectamente en la estafa. Sin embargo, cuando es identificado, difícilmente es encontrado para responder por los crímenes practicados (estelionato [5], falsificación de documento particular [6], acceso indebido a dispositivo informático protegido [7]) y tampoco repara los daños materiales causados. Aquí vale recordar que la identificación del responsable de la infección del equipo o la adulteración del documento físico raramente ocurre debido a la utilización de técnicas para ocultar la conexión de acceso (el *IP* del equipo utilizado para conectarse a internet), principalmente cuando los ejecutores del fraude están situados en otros países, dependiendo de morosas y muchas veces ineficientes cooperaciones internacionales entre autoridades policiales, inclusive envolviendo dos o más países.

Así, con la dificultad en la identificación del ejecutor del fraude responsable de la adulteración y la casi imposibilidad de recuperar el valor desviado, el cuestionamiento jurídico relevante pasa a ser sobre la responsabilidad del acreedor "aparente" en el documento fraudulento, o

incluso de la institución financiera destinataria de los valores desviados en virtud de las obligaciones derivadas de la práctica de sus actividades.

En las relaciones de consumo [8], el Código de Defesa del Consumidor [9] determina que *el proveedor de servicios responde, independientemente de la existencia de culpa, por la reparación de los daños causados a los consumidores por defectos relativos a la prestación de los servicios, así como por informaciones insuficientes o inadecuadas sobre su uso y riesgos.*

Es la figura de la responsabilidad objetiva, inherente al propio riesgo del ejercicio de la actividad en pro del consumidor, teniendo en cuenta el defecto en el servicio prestado que es independiente de la voluntad (dolo) del proveedor. Y esta misma ley describe como defectuoso el servicio que *no brinda la seguridad que el consumidor de él puede esperar, teniéndose en consideración el modo de su suministro y el resultado y los riesgos que razonablemente de él se esperan.* Además, en el caso de las instituciones financieras, pesa el posicionamiento del Tribunal Superior de Justicia [10], de que ellas *responden objetivamente por los daños generados por fortuito interno relativo a fraudes y delitos practicados por terceros en el ámbito de operaciones bancarias*. Por tanto, en los fraudes iniciados u ocurridos internamente o con involucramiento del proveedor, como es el caso del sitio infectado, de la cuenta abierta indebidamente a nombre de falso titular para el sacado del valor pagado indebidamente, de las correspondencias intercambiadas por documentos fraudulentos en el trámite de la entrega, los proveedores serán, de hecho, responsables de la reparación de los daños causados.

No obstante, no podemos generalizar y decir que los aparentes acreedores, estampados en los documentos fraudulentos son siempre responsables de los perjuicios causados. O, aún, que la institución

financiera adonde se destina la cuenta del fraude deba ser responsabilizada simplemente por poder identificar el destino del valor desviado. Esto ocurre porque el mismo Código de Defensa del Consumidor determina que *el proveedor de servicios sólo no será responsabilizado cuando pruebe que, habiendo prestado el servicio, el defecto es inexiste o habiendo culpa exclusiva del consumidor o de tercero* [11]. Así, en caso de que el equipo utilizado por el consumidor esté infectado por su negligencia en no actuar de acuerdo con las recomendaciones de seguridad (culpa exclusiva del consumidor), o aún, que el documento fraudulento haya sido enviado directamente por el ejecutor del fraude sin cualquier tipo de involucramiento del proveedor (culpa exclusiva de tercero), estaría alejada la responsabilidad del proveedor.

En esos casos, la víctima debe estar atenta para no acceder a *links* de *e-mails* sospechosos o a cualquier sitio resultante de una búsqueda en Google, mantener su equipo (computadoras, *tablets, smartphones*, *weareables* y ruteadores) siempre actualizado con antivirus y *firewalls,* no conectarse a redes no seguras (como es el caso de los *wi-fi* gratuitos y de terceros) o acceder a cuentas personales, especialmente de instituciones financieras, en computadoras públicas, además de siempre chequear si los datos del destino del pago coinciden con los datos del acreedor. En ese último aspecto, algunos artificios pueden ser útiles, tales como poner la cuenta en débito automático para impedir la realización de los fraudes envolviendo la digitación de códigos de barra adulterados y la simple verificación del código del banco en los primeros dígitos del código, para garantizar que la institución financiera de destino es la misma identificada en el resto del documento.

En el caso de las negociaciones hechas por e-mail, el uso de certificados digitales en la firma de cada comunicación y documento enviado busca garantizar la integridad de su contenido; en casos de gran volumen de

transacciones, pueden ser consideradas soluciones que centralicen los registros y las comunicaciones, como portales de compra y venta, siempre debidamente investidos de las mejores técnicas y herramientas tecnológicas (como la autenticación en dos niveles) para garantizar su protección. En caso de duda, es fundamental buscar al proprio proveedor/comprador, sea por teléfono o incluso *in situ* en las agencias y tiendas, y solicitar la confirmación de informaciones.

Pero ¿cómo actuar después que el fraude ocurrió? Primeramente, se debe buscar a todos los involucrados, en especial la institución financiera de destino (identificada en los primeros dígitos del código de barras) para ser instaurado el procedimiento de control de fraude y bloqueo de las cuentas destinatarias y de los valores desviados. Debe buscarse también al propio proveedor que aparece en el documento fraudulento, inclusive para fines de una potencial mitigación, aunque remota, de la obligación de honrar la deuda para con el verdadero acreedor. Comunicar a la autoridad policial por medio de Denuncia Policial, procedimiento muchas veces realizado por la propia página de la policía en internet, puede ser útil principalmente para fines de registro y reenvío del documento a los involucrados. Y para que la situación no se repita, además de adoptar todas las mejores prácticas de seguridad aquí informadas, es indicado analizar todos los equipos electrónicos utilizados para retirar cualquier código malicioso que esté implantado (nuevamente: computadoras, *tablets, smartphones*, *weareables*, ruteadores), así como alterar las contraseñas de acceso a las cuentas personales, usando contraseñas fuertes [12] para que los ejecutores del fraude no puedan tener acceso indebido nuevamente. Puede ser trabajoso y agotador (e incluso parecer paranoia), pero no es sólo porque tenemos toda la facilidad aportada por la tecnología que podemos bajar la guardia contra

la acción de criminales, bajo el riesgo de, a fin de cuentas, tener que pagar dos veces.

[1] Del proverbio francés *qui paie mal, paie deux fois.*

[2] Art. 308 del Código Civil: *El pago debe ser hecho al acreedor, o a quien de derecho lo represente, bajo pena de sólo valer después de ser por él ratificado, tanto cuanto se revierta en su provecho.*

[3] Datos de la RSA, división de seguridad de la compañía EMC señalan que la conocida "pandilla del talón bancario" en 19 variantes del *bolware* puede haber infectado 193 mil computadores para, a través de la falsificación de talones bancarios, desviar de empresas y personas físicas brasileñas sólo de 2012 a 2014, R$ 8,2 billones de reales en 495 mil transacciones.

[4] El uso de códigos maliciosos para alterar el contenido de talones recibió el nombre de *bolware*, una mezcla de las palabras "boleto" (talón bancario) con *malware*, que es un código (*software*) malicioso desarrollado con el objetivo de damnificar o desactivar computadoras y sistemas.

[5] Art. 171 del Código Penal: *Obtener, para sí o para otro, ventaja ilícita, en perjuicio ajeno, induciendo o manteniendo a alguien en el error, mediante artificio, ardid, o cualquier otro medio fraudulento: Pena – reclusión, de uno a cinco años, y multa.*

[6] Art. 298 del Código Penal: *Falsificar, total o parcialmente, documento particular o alterar documento particular verdadero: Pena – reclusión, de uno a cinco años, y multa.*

[7] Art. 154-A del Código Penal (Incluido por la Ley 12.737/12 – Ley de Crímenes Informáticos también conocida como "Ley Carolina

Dieckmann"): *Invadir dispositivo informático ajeno, conectado o no a la red de computadoras, mediante violación indebida de mecanismo de seguridad y con el fin de obtener, adulterar o destruir datos o informaciones sin autorización expresa o tácita del titular del dispositivo o instalar vulnerabilidades para obtener ventaja ilícita: Pena – detención, de 3 (tres) meses a 1 (un) año, y multa.*

[8] Las relaciones de consumo o *Business to Consumer o B2C* están definidas en el Código de Defensa del Consumidor en los arts. 2.º y 17.

[9] Art. 14 del Código de Defensa del Consumidor.

[10] Compendio 479 del Tribunal Superior de Justicia.

[11] Como determina el § 3.°, I y II del CDC.

[12] Evitar usar palabras cortas, reales y comunes (en palabras del ex-agente de la CIA Edward Snowden, "*think about passphrases instead of passwords*"), combinar letras mayúsculas, minúsculas, números y caracteres no alfanuméricos, no usar la misma contraseña o aprovechar contraseñas parecidas para acceso a diferentes cuentas, no compartir contraseñas, y siempre que solicite nueva contraseña, acceder y modificarla inmediatamente.

ATAQUES POR *RANSOMWARE*: ENTENDER Y PROTEGER

Caroline Teófilo da Silva

Anualmente la empresa *McAfee Labs* divulga un informe [1] conteniendo las previsiones sobre las principales amenazas cibernéticas que están por venir. El estudio divulgado a final de 2015 señaló una vez más el *ransomware* como "tendencia" del año siguiente.

Son ataques que buscan dinero rápido y fácil. Como ya decía el antiguo refrán: todo lo que cae en la red es pescado.

Este tipo de *malware* puede ser instalado en las computadoras cuando el usuario recibe un e-mail y hace clic en *links* redireccionados a sitios maliciosos, anexos infectados, y hasta downloads o actualizaciones de softwares. La *ingeniería social* nuevamente surge como un vector para la explotación de las vulnerabilidades tecnológicas.

Por medio de encriptación, el *ransomware* y sus variaciones (ex. *CryptoLocker, CryptoDefense* y *CryptoWall*) impiden el acceso del usuario a los archivos almacenados en sus propios recursos tecnológicos y servidores. Así, para liberar el acceso, el ejecutor del fraude exige un pago a cambio de la "promesa" de desbloqueo de los datos.

La acción se produce de la siguiente manera: en la pantalla de la computadora aparece un mensaje (aviso de rescate) informando que sus datos están encriptados y solamente mediante pago el ejecutor del fraude entregará la clave privada para desbloqueo, si no los datos serán eliminados en aproximadamente 72 horas. Estén tranquilos, en esta misma pantalla constan orientaciones sobre cómo acceder a los servicios de decodificación.

Detalle: ¡el pago debe ser en Bitcoin*, la moneda virtual, y gira en torno de US$200 y US$500 dólares!* Es un modelo de éxito: dinero rápido y de diversas fuentes.

No podemos olvidar que este tipo de ataque ya está tipificado como crimen en nuestra legislación y previsto en el Art. 154-A, § 1.º del Código Penal Brasileño:

"Art. 154-A. Invadir dispositivo informático ajeno, conectado o no a la red de computadoras, mediante violación indebida de mecanismo de

seguridad y con el fin de obtener, adulterar o destruir datos o informaciones sin autorización expresa o tácita del titular del dispositivo o instalar vulnerabilidades para obtener ventaja ilícita:

- *1.º En la misma pena incurre* quien produce, ofrece, distribuye, vende o difunde dispositivo o programa de computadora con el objetivo de permitir la práctica de la conducta definida en el *caput". (subrayado nuestro)*

Como el ataque está siempre vinculado al pedido de "rescate", no podemos olvidarnos del crimen de extorsión previsto en el art. 158 del mismo diploma legal:

"Art. 158 – Coaccionar a alguien, mediante violencia o grave amenaza, y con el propósito de obtener para sí o para otro, ventaja económica indebida, a hacer, tolerar que se haga o dejar de hacer alguna cosa:"

Ahora que sabemos qué es ransomware *y cuál es la tipificación penal, la duda es: ¿pagar o no pagar?*

El FBI *(Federal Bureau of Investigation)* [2] cree que la mejor opción sea pagar la cuantía solicitada y orienta a los que tuvieron sus datos bloqueados a realizar el pago.

Pero aun pagando los valores, podemos o no obtener los datos de vuelta, eso no es garantía. *¡El pago del rescate debe ser siempre la última opción!* Pues, recuérdense, las vulnerabilidades en la infraestructura tecnológica continúan, las sofisticaciones de los ataques aumentan y contribuimos a la manutención del crimen.

Nada cambia, perdemos dinero y corremos el riesgo de exponer nuestros datos en vez de aumentar la inversión en seguridad de la información.

No podemos olvidar además que es obligación tanto de las *empresas privadas como de la administración pública* la protección de datos personales y secretos que están bajo su responsabilidad, como prevé la Constitución Federal de 1988 en su art. 5.º, XII:

"Art. 5.º, XII – es inviolable el secreto de la correspondencia y de las comunicaciones telegráficas, de datos *y de las comunicaciones telefónicas, salvo, en el último caso, por orden judicial, en las hipótesis y en la forma que la ley establezca para fines de investigación criminal o instrucción procesal penal" (subrayado nuestro).*

También en diversos otros dispositivos legales existe la protección a los datos de acuerdo con su ámbito de aplicabilidad, *como el Código Civil, el Código de Defensa del Consumidor y el Marco Civil de Internet*.

Específicamente para la administración pública, corresponde a los órganos y entidades del poder público proteger las informaciones secretas y personales que están bajo su responsabilidad, de acuerdo con la *Ley de Acceso a la Información 12.527 de 18.11.2011, Art. 6.º, III:*

"Art. 6.º Corresponde a los órganos y entidades del poder público, observadas las normas y procedimientos específicos aplicables, asegurar la: (…)

III – protección de la información secreta y de la información personal, observada su disponibilidad, autenticidad, integridad y eventual restricción de acceso*." (subrayado nuestro)*

Corresponde a todos la obligación de proteger los datos que están bajo su responsabilidad, y la mejor defensa aún sigue siendo la prevención, después de todo este tipo de ataque no cuenta con muchas novedades: *malwares* explotando vulnerabilidades; sitios maliciosos; anexos infectados; ingeniería social; ejecutores de fraude anónimos.

Así como no son originales los ataques, tampoco lo son las recomendaciones de seguridad para protección de los datos:

- Realizar *backup* periódico de los datos, para que sea posible recuperarlos en caso de bloqueo;
- Instalar y mantener actualizados *softwares* de protección, como antivirus y *firewall*, que posibilitan el bloqueo inicial de esas amenazas y de sitios maliciosos;
- No hacer clic en *links* o abrir mensajes desconocidos y no acceder a sitios que no sean seguros;
- Al percibir el ataque, desconecte el equipo de la red, inclusive del *wi-fi* y quite el cable de energía, para disminuir el riesgo de que otros archivos sean encriptados.

Por último, ¡no podemos olvidarnos de los controles preventivos! *Establecer programas anuales de concientización sobre seguridad de la información es esencial para disminuir los riesgos de ingeniería social***.**

¡Estén atentos y protejan nuestro mayor activo: los datos!

[1] [www.mcafee.com/br/resources/reports/rp-threats-predictions-2016.pdf]. Acceso en: 02.12.2015, a las 17h20.

[2] [http://gizmodo.com/the-fbi-thinks-ransomware-victims-should-just-pay-up-1738846246?utm_referrer=https%3A%2F%2Fwww.google.com.br&utm_expid=66866090-68.hhyw_lmCRuCTCg0I2RHHtw.0]. Acceso en: 02.12.2015, a las 18h12.

GUERRA DIGITAL Y CIBERTERRORISMO

Patricia Peck Pinheiro

Los atentados ocurridos en París en el año 2015 trajeron a colación el debate sobre la importancia de combatir el terrorismo en su más nueva base digital, donde algunos ambientes de internet sirven de carnada para atraer a jóvenes de todo el mundo hacia una propuesta de radicalismo extremo.

Lamentablemente, aún estamos apenas reaccionando a los eventos cuando estos ocurren. Tenemos que invertir en prevención y detección, ya que estas acciones, en general, son planeadas con mucha antelación e involucran a personas que se conectan e interactúan constantemente por las vías digitales.

Siendo así, se puede afirmar que la verdadera batalla contra el terrorismo está siendo librada en una nueva frontera, que es el territorio de la *deep web*.

Incontables prácticas ilícitas son diseminadas y están concentradas en la *deep web*, como la pedofilia, canibalismo, tráfico de drogas, de armas y de otros materiales controlados, además del terrorismo. Existe incluso una moneda propia, los *bitcoins*, que contribuyen al lavado de dinero digital, ya que dificulta el rastreo del origen y destino de los recursos.

Por tanto, el perímetro del terror ya no es físico ni tiene un lugar específico, pues ya alcanza una dimensión planetaria, donde sus

integrantes consiguen recibir todo tipo de entrenamiento remoto, con uso de los más variados recursos tecnológicos que tenemos a disposición, que van desde una clase a distancia (EAD) hasta una reunión vía grupo de WhatsApp o Skype.

La tecnología no tiene un mal intrínseco, todo depende de la forma en que es utilizada. Ciertamente, es necesario construir un Plan Estratégico de Seguridad Pública y Defensa Digital que permita realizar campañas para el ciudadano, que constituye la primera línea del combate al terror, así como la mayor víctima de los ataques.

Pero ¿de qué modo los operadores de Internet podrían contribuir a combatir efectivamente el Ciberterrorismo? ¿Cómo las autoridades pueden derrumbar de forma más eficiente los sitios que promueven la intolerancia y el terror?

Ciberterrorismo es toda actividad practicada por medio de internet o de dispositivos digitales que busca causar pánico o sensación de inseguridad, yendo desde la propagación de un rumor con la creación de evidencias falsas hasta ataques masivos de denegación de servicio o alteraciones en sistemas críticos, por ejemplo, la distribución de energía, saneamiento básico y control de flujos de agua, etc.

Por consiguiente, hay un límite muy tenue que separa el derecho a la manifestación pacífica de opinión que puede ser practicada por el hacktivismo bueno versus aquel que ocurre con propósitos terroristas.

Muchas veces los ataques son dirigidos hacia empresas, a Marcas que sean iconos de una determinada cultura, o como en el caso de enero de

2015 en París, a personas cuyo oficio suponga criticar, inclusive de forma satírica o jocosa, el fanatismo religioso que nos asola.

Después de los ataques sufridos en la redacción de la revista Charlie Hebdo, el grupo Anonymous publicó un vídeo desencadenando la #OpCharlieHebdo, en que esfuerzos serían dirigidos a combatir el terrorismo islámico y los responsables del episodio en la capital francesa.

Siendo así, ¿en qué momento entonces podemos decir que entramos en una 3ra Guerra Mundial, que es la Guerra Digital? En verdad, ésta ya está aconteciendo, aunque todavía en una escala reducida y de forma silenciosa, en los bastidores de internet.

Vale recordar que en noviembre de 2014 la empresa Sony (división de entretenimiento) sufrió ataques cibernéticos, cuya autoría había sido adjudicada a Corea del Norte y que ocasionó respuesta supuestamente de Estados Unidos de América, que habría dejado al país asiático prácticamente fuera del aire, sin conexión a internet, por más de un día (22.12.2014).

Y no fue la primera vez. Al menos 25 sitios de Corea del Sur fueron atacados en 2009, el *malware* conocido como Careta (The Mask) promovió ataques en más de diez países desde 2007, además del caso involucrando a Rusia contra Estonia, en 2007, cuando sus instituciones financieras, sistemas de telecomunicaciones y sitios de noticias fueron bombardeados por ataques de denegación de servicio.

Todavía somos muy vulnerables y la mayor parte de los líderes públicos y empresariales no aborda el tema de la Seguridad Digital como prioridad de la agenda estratégica. No podemos continuar actuando como

amateurs, pues del otro lado hay todo un grupo armado, profesional, cada vez más organizado.

Por eso, debería haber una agenda común, con el compromiso de acción conjunta entre iniciativa privada y pública, abarcando varios países a fin de garantizar disponibilidad de recursos y servicios esenciales para combatir el Ciberterrorismo y preparar a la población para un escenario más bélico de Guerra Digital.

EL INFIERNO ASTRAL DE LAS APLICACIONES

Patricia Peck Pinheiro

¿Quién no ha pasado un aprieto por estar con el celular todo el tiempo bloqueándose? Así es, en la era de las aplicaciones, el usuario debe hacer mantenimientos constantes en el equipo para liberar espacio de memoria y no sufrir los bugs de la movilidad.

Ese escenario puede agravarse aún más cuando también incluimos los relojes de última generación, dotados de más y más aplicaciones, que además interactúan con el celular. ¡En este momento entramos en la era en que nuestras cosas pasan a saberlo todo sobre nosotros y pueden estar contándoselo a otros!

Por tanto, si usted es de esos que descarga cualquier aplicación gratuita de las tiendecitas de Google y Apple, y ya tiene centenas de aplicaciones instaladas, cuidado. En el último año surgieron diversos virus para celulares, además de hacerse frecuente la estafa de la aplicación falsa, nueva modalidad de ingeniería social que viene generando diversas víctimas diariamente.

Una de las aplicaciones falsas más descargadas es una herramienta que promete acelerar el dispositivo, ¡y de gratis! En verdad, se trata de un archivo malicioso para capturar datos del celular, como números de contactos, fotos e informaciones de contraseñas, que además consigue grabar lo que se está hablando y enviarlo como un archivo MP3 para la pandilla.

Lamentablemente, el usuario brasileño ha sido un blanco fácil para ese tipo de ataque, justamente por no desconfiar de las ofertas gratuitas. Existe la impresión, por parte del consumidor, de que las tiendas de aplicaciones son las que harían la verificación para garantizar la seguridad de lo que es descargado de ellas, pero no es así.

El Término de Uso de estas tiendas, en general, afirma que corresponde al cliente tener softwares de seguridad instalados, así como el cuidado con lo que está descargando en su celular. Desde el punto de vista jurídico, esa es una cuestión que merece ser mejor analizada por el Ministerio Público Federal y por el Programa de Protección y Defensa del Consumidor (Procon), en la defensa del consumidor brasileño digital.

Lo ideal es que el usuario tenga siempre mucha cautela y se certifique sobre la idoneidad de la herramienta y la credibilidad de la tienda virtual antes de hacer la compra, aun cuando sea gratuita o de poco valor. Es necesario estar muy atento, pues lo barato puede salir caro.

Para concluir, dejamos algunos consejos para quien hoy ya no sabe vivir sin celular, y lógicamente, tampoco sin aplicaciones: poner una contraseña de bloqueo en el dispositivo, habilitar el bloqueo automático por inactividad, instalar antivirus y mantenerlo actualizado, evitar descargar cualquier aplicación sólo porque es gratis, hacer backup, utilizar

herramientas para limpieza de archivos y optimización del aparato, habilitar el borrado remoto para que pueda ser accionado en caso de pérdida y/o hurto del equipo.

En la era de las "cosas conectadas", nuestros objetos pueden saber mucho respecto a nosotros. La protección de los datos y la práctica de seguridad digital son esenciales para prevenir riesgos y evitar un gran perjuicio.

CAPÍTULO QUINTO
EDUCACIÓN Y USO RESPONSABLE DE LAS TECNOLOGÍAS

EDUCACIÓN DIGITAL EN ÉTICA Y SEGURIDAD

Patricia Peck Pinheiro

En los últimos 15 años, la Institución de Enseñanza viene pasando por una profunda transformación, no sólo dentro del salón de clases, sino en todas las relaciones con la comunidad escolar.

Se puede afirmar que Internet y las nuevas herramientas de enseñanza y aprendizaje son responsables de parte de ese cambio. Pero hay una parcela relevante de esa revolución de la enseñanza que está ocurriendo dentro de las casas, en el ambiente familiar.

En lugar de limitarse a suministrar tecnología a los hijos, los jóvenes alumnos de la generación digital, la familia debe tener un papel mucho más activo en ese proceso educacional. A pesar de la falta de tiempo, sólo es posible construir un modelo de éxito con la participación y el

compromiso de los responsables legales. Después de todo, el ejemplo comienza en casa.

Siendo así, una gran cuestión involucra justamente la redefinición de los papeles, dado que la Institución de Enseñanza ya no es detentora del control del acceso al conocimiento. Además, la experiencia presencial está siendo, poco a poco, sustituida por la educación a distancia.

Independientemente de cómo el alumno de hoy interactúa con el profesor, que con su experiencia orienta al estudiante para alcanzar un nivel aún mayor de perfeccionamiento y desarrollo, una cosa es cierta: el respeto mutuo y el uso de la libertad con responsabilidad deberían ser principios guías de esta relación, no importa la época ni cuál sea la tecnología.

Siendo así, o la tecnología es utilizada para servir al propósito de la enseñanza-aprendizaje, o puede dificultar e inclusive perjudicar ese resultado.

No sólo la Institución de Enseñanza, sino principalmente la familia, tiene el deber de educar al joven en el uso más saludable, seguro, sustentable, ético y legal de las nuevas herramientas tecnológicas, dentro y fuera del salón de clases. Así como deben dar el ejemplo en el uso de estas.

Pero ¿cómo formar individuos digitalmente correctos, que sepan cuáles son los límites morales y éticos del uso de la tecnología?

Lo primero supone, ciertamente, dejar las reglas más claras. Pero ¿cuáles son los principios que deben ser incorporados en la formación de este nuevo individuo de la era digital?

A continuación, se encuentra una lista de las orientaciones primordiales que deben ser urgentemente incorporadas en el día a día de todos, sean Educadores, Alumnos, Responsables Legales o Comunidad Educacional.

Además, muchas de estas reglas vienen siendo incluidas en la documentación escolar, como Contrato de Matrícula, Regimiento, Manual de Conducta de Docentes y Estudiantes, para atender a dos propósitos: educativo y jurídico.

La solución para disminuir los incidentes que vienen ocurriendo en los ambientes educacionales depende directamente de utilizar la propia información como elemento preventivo, para conducir las conductas hacia un nuevo tipo de sentido común colectivo, abocado a las cuestiones digitales.

En este momento de transición, en que las leyes no se adecuan a los nuevos tipos de casos que vienen surgiendo, ha correspondido al Poder Judicial el papel de legislar cuando las situaciones acaban convirtiéndose en acciones judiciales. Por ello, es fundamental que la Institución de Enseñanza lidere campañas de concientización sobre el uso legal de esos nuevos recursos.

Aun cuando el tema parece no tener relación directa con la prestación del servicio de enseñanza, como cuando ocurren incidentes involucrando WhatsApp o Redes Sociales, aun así, corresponde a la Institución demostrar que no está callada ni es cómplice de malas conductas, independientemente de quien las promueva, y que afectan, aunque indirectamente, al ambiente educacional.

Si aún con esas orientaciones alguien incumple lo pactado, se debe aplicar una medida socioeducativa, pudiendo incluso ser necesario la aplicación de otras medidas administrativas y hasta judiciales, dado que la omisión o la negligencia pueden atraer la responsabilidad solidaria de la Institución de Enseñanza en la eventualidad de daño causado a otro que pueda ser vinculado a las relaciones de esta y con los diversos integrantes de la comunidad escolar.

Principios de Ética y Seguridad Digital para el ambiente Educacional
1. La regla debe estar clara, principalmente sobre el uso de los recursos educacionales tecnológicos. 2. Niño navegando solo en internet sin supervisión de un adulto es menor abandonado digital. 3. Es muy importante que la Escuela limite hasta dónde llega la puerta del salón de clases, evitando riesgos en las interacciones digitales entre alumnos y profesores, como el exceso de intimidad. 4. Seguridad de la información debe ser practicada diariamente. 5. Las informaciones escolares de alumnos son protegidas por secreto profesional y no deben ser compartidas con ninguna persona ni por ningún canal. 6. Dime con quién navegas y te diré quién eres. 7. La foto tiene que ser legal, se debe evitar publicar imagen de menores de edad en situación de exposición del cuerpo o que pueda ser vergonzosa o que lo ridiculice. 8. Quien calla consiente digitalmente. Mucho cuidado con grupos de WhatsApp polémicos o difamatorios. 9. La tecnología debe contribuir con la enseñanza-aprendizaje y no dificultarla. Celular en el salón de clases puede ayudar a la dispersión si no está previamente autorizado por el profesor solamente para uso asociado a una actividad educativa planificada. 10. Se debe siempre leer los Términos de Uso antes de dar OK.

11. Todos deben respetar la edad mínima recomendada para el uso de los recursos digitales.
12. Sea original y respete los derechos de autor al utilizar contenidos, siempre citando fuente y autoría.
13. El chiste tiene que ser cómico para ambos lados, la broma no puede volverse *bullying*.
14. No enviar foto o video íntimo como prueba de amor, pues el amor acaba y el contenido queda, se perpetúa y se propaga en la web.
15. En caso de tener algún problema, ¡denuncie! No se debe hacer justicia con el propio mouse.
16. Proteja su Identidad Digital. Contraseña es cosa seria, además de determinar la autoría, ella es la llave de la puerta en el ambiente digital.
17. Nuestras máquinas saben mucho de nosotros. Active el bloqueo automático, ¡máquina callada no filtra información!
18. Recuérdese de siempre cerrar la puerta digital.

Fuente: Dra. Patricia Peck Pinheiro

Por último, toda documentación escolar debe estar en correspondencia con las nuevas leyes en vigor en Brasil, especialmente la ley de la guardia compartida (Ley 13.058/2014), el Marco Civil de Internet (Ley 12.965/2014) y la ley contra el *bullying* (Ley 13.185/2015).

Vivimos en una sociedad digital, donde ya no hay muros ni puertas, y por eso es necesario enseñar el equilibrio entre transparencia y exposición, para que no sean practicados excesos catastróficos.

Una Sociedad más ética y segura para todos es el resultado de la acción individual de cada integrante de la comunidad escolar, no sólo de la institución de enseñanza**.**

ABANDONO DIGITAL

Patricia Peck Pinheiro

¿Usted dejaría a su hijo solo el día entero, sentado en la acera, sin saber con quién tendría contacto o por quién sería abordado? Entonces ¿por qué será que hoy hay tantos jóvenes así, abandonados en la acera digital de internet?

Si hace 50 años la televisión entró en los hogares y se volvió una especie de "niñera multimedia", ciertamente la interactividad de la web, que permite intercambios entre los más variados usuarios, genera un nuevo tipo de "niñera digital", ¡pero mucho más peligrosa!

Los padres tienen la responsabilidad civil de vigilar a los hijos. ¡Esto quiere decir que necesitan saber con quién están, cómo están y dónde están! No es posible contentarse con la respuesta "está en internet", como si fuese un lugar cercano, protegido y seguro. ¡Internet es la calle de la Sociedad actual!

Lamentablemente, cuanto más acceso a las nuevas tecnologías, mayor es la necesidad de educación. La cuestión de la seguridad debería estar presente en el día a día de las familias.

No puede ser normal que un joven participe en las redes sociales teniendo menos edad de la mínima permitida. Tampoco podemos aceptar que este mismo joven publique el número de su celular de forma abierta en

Facebook o en Twitter, posibilitando que cualquier persona lo llame, desde un colega de la escuela hasta un pedófilo.

En los últimos años, las legislaciones de diversos países, incluso de Brasil, son más rigurosas en lo referido a la pornografía infantil, algo que ha crecido bastante en el mundo digital. Es fácil para las pandillas obtener fotos de jóvenes a través de las webcams de sus casas y después diseminarlas por los sitios y comunidades de pedofilia.

La autoexposición y la falta de sentido de privacidad y de protección de la intimidad hicieron a toda esta generación de niños y adolescentes conectados mucho más susceptibles a ser víctimas de explotación sexual. Y eso ocurre incluso entre amigos, en los pasillos escolares, dentro de las familias.

Lo que comienza como una foto inofensiva puede convertirse en un encuentro en la puerta de la escuela o en un aventón con el "amigo virtual". Son situaciones de riesgo, que pueden tener desenlaces trágicos, como violación y hasta homicidio.

¿Y dónde están los padres? Delante de todo tipo de pantalla e interfaz gráfica, vemos perplejos, diariamente, a niños y niñas sufrir traumas psicológicos causados por la distribución ilimitada y perpetua de su contenido más íntimo en la web. Los jóvenes que más sufren acoso y exposición de desnudos en la web tienen entre 10 y 14 años.

Es importante destacar que comete crimen aquel que suministra el recurso y que permite almacenamiento del contenido de pornografía infantil, así como quien accede o distribuye ese contenido. En Brasil, esa práctica pasó a configurar crimen atroz desde 2014 (PL 7220/14).

Por ley, es considerado crimen atroz quien someta, induzca o atraiga a la prostitución u otra forma de explotación sexual a alguien menor de 18 años o vulnerable. El condenado por explotación sexual infantil queda impedido de obtener amnistía, gracia o indulto. La pena es de 4 a 10 años de reclusión, que también es aplicable a quien facilite esta práctica, o impida o dificulte su abandono por la víctima. Además, quien es condenado por crimen atroz tiene asimismo que cumplir un período mayor en el régimen cerrado (Ley 8.072/1990).

De igual forma, puede encuadrarse en ese crimen el propietario, o gerente o el responsable del local en que ocurre la prostitución. Y la prostitución digital puede responsabilizar también al dueño del equipo que almacena fotos o videos de desnudo infantil, así como hasta al cibercafé utilizado en el esquema.

Nuestros jóvenes están sufriendo violencia a través de clics, que van desde el *cyberbullying* a la pedofilia. Internet no es un lugar seguro para que un niño se quede solo.

La foto, el precio, la programación del encuentro, todo ocurre con máquinas-testigos, en el ambiente digital, con publicaciones en internet o por medio de mensajes en el celular. Sin embargo, los daños causados son muy reales.

¿Cómo un niño de 9 años recibe un celular con cámara y acceso a internet, y no es supervisado firmemente por los padres?

¿Qué le impide a ese niño, aun sin malicia, convertirse en la próxima víctima de un crimen relacionado a la exposición sexual de menor? ¿Cómo evitar que alguien le pida una foto en pijama, en ropa interior, y después desnudo?

La negligencia parental está cerca del complot por omisión, ya que son los padres quienes proporcionan los recursos usados para herir al menor. Es un deber de los padres prestar asistencia y monitorear. Sólo deberían darles los equipos tecnológicos a los niños después de la instalación de softwares de control parental. Información es esencial para proteger a esos jóvenes que son los nuevos "menores abandonados digitales".

CÓMO EDUCAR A LOS JÓVENES EN LA ERA DIGITAL

Patricia Peck Pinheiro

La Sociedad Digital transformó la forma en que las personas se relacionan para siempre. Cualquier individuo tiene el poder de expresarse en tiempo real para el mundo, generando contenidos que se perpetúan en Internet. No obstante, lo que sería algo positivo, sin educación puede generar muchas cosas negativas, desde ofensas digitales a la práctica de plagio, además de otros crímenes digitales.

Esta nueva generación de jóvenes nacidos y criados con mimos tecnológicos, que, impulsados por la inseguridad del mundo real, comenzaron a llevar una vida más virtual, basada en internet, con amigos e interacciones fundamentadas en las redes sociales, también necesita de cuidados. No sólo para que no se conviertan en víctimas, sino principalmente para que no sean infractores. Por eso, los profesores deben estar más presentes y ser más interactivos, conectándose con sus alumnos y usando el nuevo lenguaje de la web, con la misión de mostrar principios, reglas, límites y el uso saludable y seguro de la tecnología.

Internet acabó trayendo la calle para adentro de la casa de las familias brasileñas. Pero muchos de los padres que pasan el día en la computadora trabajando, al llegar a casa quieren distancia de la tecnología. Así, acaban

no enterándose de la rutina de la vida digital de sus hijos, delegando la orientación al "gran oráculo Google" o a la "Wikipedia". Es importante reflexionar al respecto, pues los principales riesgos digitales son muy parecidos a los del mundo real, sea hablar con un desconocido, sufrir un acoso, tener acceso a un contenido inapropiado para la edad, pasar por una situación de exposición de intimidad o incluso ser víctima de una ofensa. Un padre que le da un celular con cámara a un hijo tiene que explicarle que él no puede tirarles fotos a los otros sin autorización y publicarlas en internet.

El joven debe ser orientado en el uso de tecnología, y a medida en que vaya ganando en confianza y responsabilidad, ganará también más autonomía. ¡Y esta orientación es papel de la Escuela! Debido al uso excesivo, ha aumentado la cantidad de incidentes involucrando a jóvenes en Internet, inclusive en el ambiente educacional, relacionados principalmente a una "mala educación digital". Muchos usuarios usan el conocimiento de tecnología para hacer el mal a otras personas, sean colegas de escuelas, profesores o hasta desconocidos.

Escuelas y Profesores deben orientar a sus alumnos sobre la buena conducta digital. Y eso comienza enseñándole a usar los dispositivos. El profesor debe, sí, acceder a los Términos de Uso de las principales Redes Sociales como Facebook, Twitter, Tumblr y leerlos de conjunto con los estudiantes. ¡Sin eso, estamos permitiendo madurar toda una juventud que da "Clic-OK" sin leer! Que miente sobre su edad para estar en un ambiente cuya edad mínima es de 13 años. ¡Imagine cuál será la ética de ese individuo cuando crezca!

La escuela no debe sólo invertir en infraestructura tecnológica, con Portales, EAD, Wireless, Tablets, Pizarra Virtual, y otras tecnologías que

apoyan la Educación, pues es muy peligroso proporcionar las herramientas sin las orientaciones adecuadas. Más que usar tecnología en el salón de clases, es necesario enseñar sobre las reglas del juego, sobre las leyes vigentes y sobre ética en un mundo cada vez más digital.

La libertad de expresión exige responsabilidad. Véase el caso de la estudiante de derecho que en 2010 publicó mensajes prejuiciosos contra habitantes del nordeste de Brasil en Twitter. Dos años después, la usuaria fue condenada a pena convertida en prestación de servicios comunitarios y pago de multa.

El Poder Judicial Brasileño ha castigado severamente los casos que paran en la Justicia,[35] condenándolos a indemnizar con valores de alrededor de R$ 15 mil reales, además de aplicar medida socioeducativa en base al Estatuto del Niño y del Adolescente. ¡Pero la secuela permanece en la vida de la víctima! Ningún dinero va a limpiar su nombre y su honra en Internet, además de los daños psicológicos de quien sufre con *cyberbullying*, por ejemplo. Ese tema debe ser objeto de actividades en salón de clases, como redacciones o seminarios, lo que sea necesario para generar mayor comprensión sobre la gravedad del asunto.

¿Qué configura *Cyberbullying*?

[35] Profesor ofendido a través de Orkut obtiene indemnización de padres. La Justicia de Rondonia condeno a 19 padres de estudiantes a pagar indemnizaciones a un profesor de matemática de Cacoal (500 km de Porto Velho) que, sumadas, resultan en R$ 15 mil. El profesor fue objeto de las ofensas de los alumnos en Orkut. Estos crearon, en 2006, la comunidad virtual "Vamos a Comprarle un Pantalón al Lechón", ilustrada con la foto y el nombre del profesor Juliomar Reis Penna, 33. En la comunidad, diez alumnos de octavo grado, con edades de 12 a 13 años, escribieron ofensas, chistes, cuestionaron notas y amenazaron al profesor. "Yo ayudo a pinchar los neumáticos de su Vectra [...] Vamos a romperle los cristales, echar azúcar dentro del tanque de gasolina", fueron algunos de los mensajes dejados por los alumnos. [...] Denunciados por el profesor en el Juzgado de la Infancia y de la Juventud, los alumnos reconocieron la creación de la página y la autoría de los mensajes. Como medida socioeducativa, ocho estudiantes tuvieron que dar charlas a adolescentes sobre el uso responsable de internet.

Fuente: [www1.folha.uol.com.br/folha/informatica/ult124u446656.shtml].

- Uso de imagen no autorizada de colega (foto o video) en la web, asociado a contenido ofensivo o vergonzoso, que exponga parte del cuerpo del mismo con el objetivo de ridiculizar (ej.: nariz y decirle narizón, oreja y decirle orejón, otros);
- Asociación del nombre de persona (colega, profesor, tercero) con animales (por uso de imagen, sonido, otros efectos) con el objetivo de exponer a la persona públicamente a humillación;
- Redacción de contenido dirigido a alguien (sea un colega, un profesor, un tercero) en tono agresivo, de odio, de amenaza, discriminación, persecución, hablar mal o denigrar a la familia de la persona y de su contexto social;
- Incitación a la práctica de violencia de una o más personas contra una persona específicamente (basta la mención de detalles que puedan generar la identificación de esta, aunque no se cite su nombre).

Autoría: Dra. Patricia Peck Pinheiro

Por todo ello, la asignatura "Ciudadanía y Ética Digital", que puede ser impartida de forma independiente o en el contexto de otras asignaturas (con temas discutidos en clases de historia, geografía, biología, computación, inglés, otras), tiene la finalidad de aportar el fundamento comportamental necesario para que un individuo ejerza al máximo su libertad y ciudadanía en la era digital, de forma ética, segura y legal. O sea, busca permitir el máximo uso de la tecnología con el menor riesgo social posible. No podemos dejar que el ambiente digital se transforme en una "tierra sin ley", o entonces vamos a retroceder al "estado de

naturaleza", donde prevalece la ley del más fuerte. Tecnología no puede estar disociada de ética y de leyes, bajo pena de que saboteemos la próxima generación.
Según una investigación realizada en 2015 por el Instituto iStart en diferentes instituciones de enseñanza ([www.istart.org.br]), han aumentado los incidentes involucrando jóvenes y uso de tecnologías en los últimos años:

- ✓ 100% de las escuelas investigadas ya tuvieron algún incidente de uso indebido de celular en el salón de clases;
- ✓ 75% registraron incidentes de *cyberbullying* (ofensas digitales);
- ✓ 56,25% relataron distracción, dispersión e interferencia en el desarrollo de la clase debido al manejo del celular;
- ✓ 31,25% tuvieron casos de demasiada exposición de intimidad con la compartición de imágenes íntimas de menores de edad.

Necesitamos formar una generación digital centrados en la construcción de lo positivo y no en el uso de la tecnología para fines ilícitos o de mala fe. Internet tiene el poder de perpetuar el contenido. Los jóvenes que experimentan esta realidad ya sienten los reflejos directos en su vida digital.

Por eso, el diálogo es fundamental. Enseñar al joven a tener una visión crítica, a percibir que la "moda pasa y el contenido permanece en internet". Que las actitudes de hoy en la web repercuten en el futuro del individuo. El trabajo conjunto de apoyar el inicio (asistencia), usar software de control parental (monitorear) y enseñar el uso correcto (discernimiento) permiten reducir gran parte de los incidentes.

¡Tenemos que actuar! Pasamos a tener una reputación online por la que velar. Lo que antes era limitado en tiempo y espacio ahora ocurre sin fronteras y se propaga rápidamente por el mundo. Por eso, los profesores deben enseñar la práctica de la prevención, deben hablar sobre seguridad digital en el salón de clases, o sea, apoyar mucho más la formación del joven que la información, pues para esto último, internet ya cumple un buen papel.

Consejos para los padres combatir la Delincuencia Digital

- Dar asistencia en el uso de las herramientas tecnológicas (enseñar sobre las reglas del juego, ética y leyes en vigor);
- Usar un software de control parental;
- Crear perfiles en la computadora cuando es usada por más de un integrante de la familia para saber quién está haciendo qué (eso da mayor libertad a quien tiene más edad y madurez);
- Hacer búsqueda periódica en Internet con el nombre de los hijos (inclusive por imágenes);
- Frecuentar la vida digital de los hijos (hablar con ellos por aplicaciones de intercambio de mensajes, visitarlos en el Blog y en las Comunidades en que participan);
- Orientar sobre exceso de exposición (especialmente que eviten publicar fotos más íntimas y de situaciones de la familia que puedan generar riesgos hasta de seguridad, atrayendo asaltos o secuestros);
- Enseñar viejos consejos que se aplican al mundo digital: "dime con quién navegas y te diré quién eres", no hables con extraños en la web, no pidas un aventón en cualquier comunidad, no codicies o copies el contenido del prójimo, no les hagas a los otros lo que no te gustaría que hiciesen a ti, usa sólo fotos autorizadas por la persona fotografiada.

Corresponde a la Escuela también, en última instancia, institucionalizar estas nuevas reglas de convivencia y comportamiento digitales entre profesores y alumnos. Después de todo, ¿puede un Profesor aceptar a un alumno como amigo en su red social, que, en principio, es personal? ¿Estaremos confundiendo demasiado la relación? El exceso de intimidad también puede perjudicar el proceso pedagógico, es necesario que haya una separación de los papeles.

Si la Escuela ya hubiera definido una directriz al respecto, es más fácil para el Profesor responder que el canal de comunicación debe ser el ambiente escolar. ¿Pero será que así el profesor puede perder una oportunidad de conocer mejor a su alumno, como persona? Esa cuestión debe ser debatida en las reuniones de profesores y no existe decisión correcta o incorrecta. Lo importante es tener una conducta estandarizada, sin que haya diferencias en la manera de actuar entre los profesores, pues eso puede llegar a configurar, jurídicamente, un riesgo de discriminación o de persecución.

Los padres son responsables de culpa *in vigillando*, y tienen el deber de saber lo que le sucede al hijo, aunque no entiendan mucho de tecnología. Es preferible tener una postura participativa que simplemente prohibir o negar que algo está ocurriendo. Dos de cada tres jóvenes ya fueron víctimas de algún incidente digital, en la gran mayoría de los casos *cyberbullying* o uso no autorizado de su imagen, inclusive por otros amigos.

El grupo etario que más sufre riesgos en internet es el de 10 a 14 años. Esto se debe al uso precoz de dispositivos con acceso a internet, como celulares y tablets, sin control o supervisión de los padres. En la primera fase, el mayor riesgo es el de exposición a contenido inapropiado, pues los niños suelen buscar videos en YouTube o juegos online, y pueden fácilmente tener contacto con sitios de pornografía o hasta de pedofilia.

Más tarde, los incidentes más comunes involucran acoso y exposición de la vida íntima (publicación de fotos, informaciones de rutina y datos de la familia que pueden hasta atraer criminales y generar riesgo de secuestro).

Ya cuando el usuario entra en la adolescencia, los problemas más comunes varían entre *cyberbullying*, abusos de la libertad de expresión y práctica de ofensas digitales. En esta época también son frecuentes incidentes de perfiles falsos (alguien crea un perfil en nombre del joven y finge ser él) y exposición a la piratería.

Por último, están además incidentes relacionados con los usos de contraseñas y de tarjeta de crédito (compras en sitios que pueden ser estafas y generar contaminación por virus).

Ante este escenario, recomendamos que los padres:

- Estén más presentes en la vida digital de sus hijos.
- Cuando lleguen a casa del trabajo, muestre que se interesa sobre quiénes son los amigos virtuales del hijo, pregúntele cómo fue el día en la calle digital, con quién interactuó, cuáles son sus sitios favoritos.
- Sea amigo de su hijo a través de estos canales, no sólo desde el celular, sino también vía web.

- No deje a su hijo acceder a esos canales en un ambiente aislado, o sea, coloque la computadora en un lugar visible, para que usted consiga visualizar lo que él está haciendo.
- Oriente a sus hijos a no divulgar informaciones de rutinas, horarios, trayectos, datos financieros de la familia en las redes sociales.
- Lea y esté informado de los términos de uso de los servicios digitales que sus hijos utilizan. Facebook, por ejemplo, es sólo para mayores de 13 años.

Actualmente vivimos en red, todos conectados, y para que esa relación sea saludable, es esencial asumir un pensamiento comunitario (opuesto a los últimos años de individualismo exacerbado), centrado en el cuidado del otro, del medio ambiente y de la propia postura en las Redes Sociales, lo que debe formar parte de la práctica diaria de ciudadanía. ¡Manos a la obra, o, mejor dicho, manos en la máquina!

REFERENCIAS BIBLIOGRÁFICAS

[1] PINHEIRO, Patricia Peck. *Direito Digital*. 4. ed. Ver., atual. y ampl. São Paulo: Saraiva, 2011.

[2] BUCHANAN, Mark. *O Átomo Social*. Traducción del original "*The Social Atom*". São Paulo: Leopardo Editora, 2010.

[3] BAÚ, Alvaro Luiz; GRISARD, Luiz Antonio. *Gestão Escolar Integrada*. Curitiba: Editora Positivo, 2010.

[4] PONDE, Luiz Felipe. *Contra um Mundo Melhor, ensaios de afeto*. São Paulo: Leya del Grupo Texto Editores, 2010.

[5] PINHEIRO, Patricia Peck; SLEIMAN, Cristina. *Tudo o que você precisa ouvir sobre Direito Digit@l no dia-a-dia*. São Paulo: Saraiva, 2009.

[6] PAPERT, Seymour. *A Máquina das Crianças, repensando a escola na era da informática*. Edición Revisada. Porto Alegre: Artmed, 2008.

CELULAR NO ES JUGUETE

Patricia Peck Pinheiro

Ya pasó el tiempo en que el respeto al profesor era algo en que bastaba una mirada para hacer que un alumno se quedara quieto en el salón de clases.

La cuestión de la disciplina y de la atención siempre fue esencial para un buen desarrollo escolar. Sin embargo, actualmente, con los jóvenes brasileños recibiendo un celular alrededor de los ocho años, es mucho más difícil para el profesor conseguir la atención de los alumnos.

Vivimos un problema generalizado de indisciplina, donde el profesor, en vez de tener el papel principal en la educación, se volvió secundario.

Muchos padres que les regalan un celular a sus hijos de hecho no reflexionaron sobre el efecto nocivo de esta herramienta dentro del ambiente estudiantil.

Y están además los que les envían mensajes a sus hijos durante el horario de clases. ¿Cómo lidiar con este problema que es de educación?

Primero, ¿debería haber una edad mínima para que alguien reciba un celular? En definitiva, un celular no es un juguete. Es un equipo que genera responsabilidad en el uso tanto como un automóvil.

La industria de telecomunicaciones está siendo extremadamente descuidada al no informarles a los padres los riesgos del uso de un celular de verdad por un niño.

Los peligros van desde los efectos de las ondas electromagnéticas al cerebro, la emisión de luz azul a la vista, hasta los que tienen que ver con el hecho de que tener un celular con acceso a internet, significa que el niño está en la calle digital, sujeto a ser abordada por extraños, pudiendo ser un pedófilo o secuestrador.

Sin embargo, hoy el celular es vendido y usado por un menor de edad como si fuese una práctica totalmente inofensiva. ¿De quién es la culpa? De los padres.

Corresponde al responsable legal buscar orientación sobre lo que debe ser enseñado a un joven que va a tener un celular por primera vez. Y son consejos sobre la protección del hijo y no del equipo.

La mayoría de los padres suele decirles a los hijos solamente tres cosas: no gastes todos los créditos, no rompas la pantalla y no pierdas el celular.

Bien, ¿qué fue lo que los padres dijeron para proteger al hijo? ¡Nada! Eso da vergüenza.

La generación actual, debido a su sentimiento de culpa por trabajar demasiado y dejar a los hijos con otras personas, desde niñeras hasta en escuelas integrales, no están cumpliendo con su deber legal de vigilancia.

Y lo peor es que esta omisión en la educación y en el uso ético de la tecnología ya está alcanzando a la universidad. Ha sido bastante difícil para los profesores poner límites a los jóvenes adultos, mayores de 18 años, que se pasan la clase entera tecleando boberías en el celular. Qué desperdicio de tiempo y de vidas.

Hasta los 12 años, el joven en Brasil es totalmente incapaz ante el Código Civil. Tanto es así que, para tener una cuenta de celular, es necesario que el contrato sea a nombre de uno de los padres, asociado al CPF del responsable.

¿Podrá alguien con menos de 12 años, de hecho, usar un celular con el cuidado necesario para no exponerse, no transmitir informaciones inadecuadas a otros, evitar acosos y cuidar el equipo?

Además, ¿por qué alguien de menos de 12 años, que está siempre en un lugar con un adulto (de lo contrario ya configuraría abandono de incapaz), necesita realmente un celular con tantas funcionalidades? Si fuese sólo para juegos, hay otros dispositivos más seguros.

¿Le daría usted un Ferrari que corre a más de 300 km por hora a su hijo como primer carro en cuanto él obtuviese la licencia de conducción y aún estuviese aprendiendo a manejar? Entonces ¿es recomendable darles de inmediato el último modelo de smartphone a los hijos, con recursos que ni los padres saben usar?

Necesitamos rescatar la disciplina en el salón de clases y el celular está siendo el gran villano de los últimos años. Una persona que usa demasiado el celular desde la infancia está sujeta a desarrollar adicción tecnológica.

Por tanto, celular es un asunto serio. No es una bicicleta. Tiene reglas de uso y puede generar daños. Las autoridades deberían exigirles una campaña de concientización sobre el uso seguro del celular a todas las empresas que explotan este mercado.

En Brasil todavía vale la idea de que, si todos lo hacen, no hay problema. Vamos a reflexionar sobre lo que provocamos en este joven al darle una tecnología tan poderosa sin enseñarle la forma correcta de usarla.

Por último, los padres tienen el deber de dar una ojeada al celular de los hijos, de saber la contraseña, de saber lo que está ocurriendo en su vida digital.

¿Qué fotos está tirando y compartiendo? ¿Quiénes son los amigos con los que conversa en el celular y vía aplicaciones como WhatsApp?

Y, por encima de todo, si está o no usando indebidamente el celular en el salón de clases. ¿Cómo darle una buena educación a quien no presta atención? Los padres de hoy son responsables de la generación brasileña de mal educados digitales que estamos creando.

CAPÍTULO SEXTO

MUNDO CONECTADO: RELACIONES Y COMPORTAMIENTOS EN RED

LOS SITIOS DE REDES SOCIALES Y LA PLURALIZACIÓN DE LA COMUNICACIÓN

Dr. Victor Varcelly Medeiros Farias

Brasil posee una cultura rica, influenciada y resignificada a partir de las contribuciones de los más diversos pueblos y culturas. Esta diversidad, sin embargo, aún está sólo parcialmente expresada en los medios nacionales tradicionales, levantando cuestiones relacionadas con la representación de las minorías discursivas y fortaleciendo el debate sobre la necesidad de la democratización de la comunicación[36]. Este panorama restricto, sin embargo, está siendo poco a poco modificado por una corriente paralela creada por la ampliación del acceso a Internet, a los sitios de las redes digitales como *YouTube* y *Facebook* y al fortalecimiento de los productores autónomos de contenido.

YouTube y *Facebook* son sitios de red social digital que permiten la divulgación de contenido por los propios usuarios. La estructura estándar de *YouTube*, por ejemplo, permite, sin la necesidad de contrapartida financiera directa, que el usuario cree su propio canal de contacto con el público y divulgue sus videos. Además, todos los usuarios registrados en el servicio pueden comentar, darle "me gusta" y compartir los contenidos públicamente presentados e inscribirse en los canales. Funciones similares se pueden encontrar en las *Fanpages* de *Facebook*, que posibilitan interacciones directas entre figuras públicas, empresas, instituciones y usuarios en general. Estas nuevas formas de interacción

[36] La pauta de la democratización de la comunicación no es solo brasileña, teniendo debates y regulaciones en diversos países de América Latina, como la Ley de Medios, (Ley nº26.522/09) argentina que es referencia mundial.

por Internet poseen un potencial significativo de pluralización de la comunicación, pues permiten que grupos y temáticas detentores de reducido espacio autónomo en los medios tradicionales brasileños, como temas relacionados a la sexualidad y a la identidad de género, ganen mayor realce y repercusión en la sociedad.

Los medios de comunicación de masa en Brasil están en su mayoría relacionados a grandes empresas, que los controlan de manera directa o indirecta y filtran su contenido según sus respectivas líneas editoriales. Este filtro, aliado a la forma unidireccional de creación y divulgación de contenido típica de los medios de masas, no favorece la ampliación de la pluralidad de los de discursos[37], pues centraliza la producción de contenidos en las manos de pocos. El avance de la Web 2.0 (O´Reilly 2005) en Internet por medio de los sitios de redes sociales digitales, sin embargo, subvierte un poco esa dinámica, permitiendo la mayor diseminación de la producción y divulgación autónoma de contenidos. Este cambio que trajeron las herramientas del ciberespacio consiste en lo que Lemos (2003) nombró segunda ley de la cibercultura, que

> […] sería la Liberación del polo de emisión. Las diversas manifestaciones socioculturales contemporáneas muestran que lo que está en juego como el exceso de información no es nada más que la emergencia de voces y discursos anteriormente reprimidos por la edición de información de los *mass media*. La liberación del polo de la emisión está presente en las nuevas formas de relación social, de habilitación de la información y en la opinión y movimiento social de la red

Por tanto, hoy es posible que una minoría discursiva se autorrepresente en Internet, por ejemplo, en YouTube, y, consecuentemente, confronte o enriquezca la interpretación sobre su día a día y sus intereses que son

[37] Esta temática, discutida también en el corto Cordel da Regulamentação da Comunicação, divulgado en 2012 por el Centro de Cultura Luiz Freire está disponible en: https://www.youtube.com/watch?v=NWs1B8goHL8. Acceso en 10 de mayo 2016

presentados a la sociedad. De esta forma, crece el número de productores de contenido como Viva Rocinha, que presenta la comunidad de Rocinha desde la perspectiva de sus propios habitantes, oyendo las reclamaciones, sugerencias y reportando noticias internas. Viva Rocinha posee perfiles en los principales sitios de redes sociales digitales, teniendo aproximadamente veinte mil fans en *Facebook,* y además una aplicación propia para la divulgación de las noticias. Esta legitimación del discurso de las minorías, basada en la reconquista de la propia representación de los grupos y del individuo, no solo ha ocurrido con las comunidades carentes, inicialmente marginalizadas en su divulgación en los medios de comunicación de masa, sino también que alcanza a otros grupos los cuales generalmente poseen reducido espacio o representación estereotipada en los medios tradicionales de comunicación como es el caso de los homosexuales.

Recientemente, canales de *YouTube* como "Põe na Roda"[38], que presenta la temática homosexual de manera humorística y dirigida a la concientización, han ganado notoriedad, llegando a establecer colaboración con órganos internacionales defensores de la causa, como la Organización de las Naciones Unidas (ONU). En el video "Lua de mel gay", los actores escenifican la planificación de un viaje de nupcias a diversos países, mientras presentan las respectivas políticas penales de cada uno de ellos contra la homosexualidad, divulgando al final del video la campaña "Livres e Iguais" de la ONU[39] que combate el prejuicio contra la diversidad LGBTT (lesbianas, gays, bisexuales, travestis y transexuales). El respectivo video tiene actualmente más de ciento sesenta mil visualizaciones en *YouTube.* El canal "Põe na Roda" nació en enero de 2014 y actualmente acumula más de cuatrocientos mil inscritos y cuarenta millones de visualizaciones de sus videos, destacándose como uno de los principales canales de comunicación de la causa LGBTT en Brasil dentro de *YouTube*. En un proyecto de colaboración semejante, la

[38] Video disponible en: https://www.youtube.com/watch?v=_opjl2GQyfY. Acceso en 10 mayo 2016.

[39] Más informaciones sobre la campaña **Livres e iguais da ONU:** http://nacoesunidas.org/campanha/livreseiguais. Acceso en: 10 mayo 2016.

ONU actúo también, junto al canal "Porta dos Fundos" para divulgar los Objetivos del Desarrollo Sostenible[40], abordando temáticas como la igualdad de género y la reducción de las desigualdades, presentados en los respectivos videos "juíza" y "amiguinho" ambos[41] publicados en octubre de 2015.

Iniciativas como estas demuestran el poder de pluralización de los discursos en la web 2.0 que permiten la transformación del individuo de espectador en productor de contenidos. Juntos los videos de "Porta dos Fundos" y de "Põe na Roda" alcanzaron más de ocho millones de visualizaciones y con sus guiones diferenciados presentaron una reflexión necesaria a la sociedad sobre las respectivas temáticas. Lo mismo puede decirse de "Viva Rocinha", que permitió a la comunidad gerenciar su propia narrativa, no dejándola a la elección de los medios tradicionales.

Así, después de este breve análisis sobre estas tres iniciativas, escogidas entre otras incontables de relevancia como la cultura nerd en el canal Jovem Nerd[42] y el feminismo en Jout Jout[43], es posible percibir que los sitios de redes sociales digitales pueden, sí, tener un gran papel en la democratización de la comunicación y en el ejercicio de la libertad de expresión presentada en nuestra Constitución Federal, por tanto, son una potencial forma de garantizar derechos a la sociedad y sus actores deben ser protegidos y estimulados. Finalmente, recuérdese, no todos los contenidos son de calidad, busque buenas referencias, denuncie contenidos vinculados al discurso de odio y aproveche para crear y tener nuevas visiones y recibir contenidos de calidad.

[40] Más informaciones sobre los Objetivos del Desarrollo Sostenible: http://www.pnud.org.br/ods.aspx
[41] A los videos "juíza" y "amiguinho" se puede acceder respectivamente en: https://www.youtube.com/watch?v=nHcQOY-Rews y https://www.youtube.com/watch?v=NxzUU-cZD1o. Acceso en: 10 mayo 2016.
[42] Más informaciones disponibles en: [https://www.youtube.com/user/JovemNerd]. Acceso en: 10 mayo 2016.
[43] Más informaciones disponibles en: https://www.youtube.com/user/joutjoutprazer. Acceso en: 10 mayo 2016

REFERENCIAS

CETIC.br. TIC Domicílios. Disponible en: <http://data.cetic.br/cetic/explore?idPesquisa=TIC_DOM>. Acceso en: 10 mayo 2016

MARTINS, Leonardo; DIMOULIS, Dimitri. **Teoria Geral Dos Direitos Fundamentais:** Revista, Atualizada e Ampliada. 5. ed. São Paulo: Atlas, 2014.

ONU. **Livres e iguais.** Disponible en: <http://nacoesunidas.org/campanha/livreseiguais/>. Acceso en: 8 set. 2015.

O'REILLY, Tim. **What Is Web 2.0**: Design Patterns and Business Models for the Next Generation of Software. Disponible en: <http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1>. Acceso en: 7 mayo 2016.

CIUDADANÍA PARTICIPATIVA

Patricia Peck Pinheiro

En los últimos años han aumentado las acciones para la participación directa de los ciudadanos en la agenda política de su país, e Internet ha sido el canal para viabilizar esta relación directa entre el Pueblo y el Estado.

Es lo que observamos con iniciativas como el presupuesto participativo en Brasil (https://opdigital.pbh.gov.br/orcamento-participativo), a través del cual la comunidad puede votar por el proyecto que le gustaría que

fuese realizado en su municipio entre las propuestas presentadas por el Gestor Público.

Podemos citar, también, el plebiscito de independencia de Crimea, en 2014, que inspiró a regiones del mundo con pretensiones separatistas, por ejemplo, Venecia y otras ciudades de la provincia de Véneto, que promovieron un Plebiscito Online para votar por la posible separación de Italia. Solo con internet fue posible saber la opinión en tiempo real de 2,3 millones de electores, de los cuales 89% votó a favor de la separación y sólo 257 mil votaron en contra.

O sea, ¡un embrollo político que ocurre desde 1797 y que puede ser resuelto por un *clic*! Venecia ya fue de Francia, cuando Napoleón ganó la primera campaña en Italia, después fue de Austria, formando el Reino Lombardo-Véneto, hasta ser de Italia en 1866, con la unificación que sobrevino con el Risorgimento.

Pero ¿estará la Autoridad Pública preparada para esta interacción directa, esta transparencia total? Si quien elegimos debería responder a la voluntad de quien votó por él, ¿por qué después de ver el resultado de la voluntad popular, el gobierno italiano reaccionó alegando ilegalidad pues el plebiscito online no tendría poder constitucional inmediato?

Este miedo del poder a la ciudadanía digital afectó también al plebiscito en Reino Unido, sobre la separación de Escocia, realizado en septiembre de 2014. El Gobierno británico llegó a exigir que la consulta fuese limitada a sólo una pregunta y que se efectuase rápidamente. Según el primer ministro británico David Cameron, que está en contra de la separación, la demora genera incertidumbre y perjudica la inversión en la economía escocesa.

Ciertamente, a través de las nuevas tecnologías se amplía sobremanera la propia democracia. La facilidad de acceso a internet estimula una mayor adhesión a las iniciativas de ciudadanía participativa, que permite que cada individuo pueda influir y afectar directamente una decisión política en su ciudad, estado o País. Si pudiésemos siempre votar por la web o incluso por una aplicación descargada en el celular, tendríamos mucha más implicación de la población en las cuestiones que definen la vida en sociedad.

Hasta en la vida personal, es más fácil separarse por Internet (www.divorcioonline.com.br), ¡y hay quien defiende la tesis de la separación hasta por WhatsApp! ¿Adónde vamos a parar? ¿Estará Brasil preparado para adoptar cada vez más este tipo de consulta directa a través del plebiscito online?

¿Cuál sería el resultado si hoy preguntásemos a la población de Rio Grande del Sur si ellos se quieren separar? ¿Habrá cambiado la opinión desde la Guerra de los Farrapos con Garibaldi? ¿Tendremos el valor de preguntar? Y, dependiendo del resultado, ¿de implementarla? ¡Cuándo la tecnología está asociada a la educación el resultado final es la maduración de una nación!

CREDIBILIDAD EN INTERNET: LOS DILEMAS DE LAS NUEVAS FUENTES DE INFORMACIÓN

Milena Mendes Grado

¿Usted ya se deparó con una noticia en Internet y se quedó con dudas sobre si el contenido era verídico? Las personas siempre cuestionan la credibilidad de las informaciones transmitidas por los medios sensacionalistas tradicionales, pero con la popularización de Internet, dudar de la credibilidad de las noticias se volvió más común. Mucho se

debe al embate entre rapidez y calidad de la información. Con el ansia de ser portadora de la primicia del reportaje, para llevar la noticia con más rapidez a los lectores y espectadores, algunos medios dejan de confirmar y chequear adecuadamente la fuente y la veracidad de las noticias que publican. Encontrar un punto de equilibrio entre esos dos puntos no es fácil, sin embargo, conocer los riesgos jurídicos de la situación y saber evaluarlos puede ser la solución.

La falta de credibilidad de las fuentes puede ser fácilmente identificada a diario. Por ejemplo, en los actos de terrorismo del Maratón de Boston, en abril de 2013, cuando los ciudadanos americanos y de todo el mundo recibieron una avalancha de informaciones que no coincidían con la realidad de los acontecimientos[44]. Muchas informaciones leídas en Twitter se volvieron fuente para cabezales y reportajes sin ningún chequeo efectivo. En Brasil, por ejemplo, después del Examen Nacional de Enseñanza Media (ENEM), en octubre de 2013, fue noticiado que la red de sándwiches McDonald's posteó en su perfil en Twitter un mensaje invitando a los alumnos que no salieron bien en la prueba a trabajar en la red[45]. Posteriormente, la red informó que no había publicado ese mensaje en su perfil y que este era un contenido falso[46]. La divulgación de este mensaje falso, relacionado a un gran acontecimiento nacional, con seguridad provocó perjuicios a la marca de la red.

Errores como los señalados pueden tener consecuencias jurídicas extenuantes y costosas. La publicidad de la noticia ocurre a causa de la prensa y no de la fuente, siendo la publicidad el factor que fundamenta la ilicitud en muchas conductas o agrava la penalización de estas. Así, los medios serán responsabilizados en casos, por ejemplo, de difamación, calumnia, injuria, ofensas a la imagen, así como por la violación al derecho de marca, entre otras. La libertad de prensa y la veda de la

[44] Fuente: http://www.publico.pt/mundo/noticia/as-historias-falsas-de-boston-martin-nao-abracou-o-pai-antes-de-morrer-1591639 acceso en 02/02/2014 a las 14:13h..

[45] Fuente: http://www.oprimeiroencontro.com.br/mcdonalds-manda-mensagem-pra-quem-foi-mal-no-enem/ acceso en 02.02.2014 a las 14:14h.

[46] Fuente: http://oglobo.globo.com/educacao/tweet-falso-convida-candidatos-que-foram-mal-no-enem-2013-trabalhar-na-rede-mcdonalds-10593002 acceso en 02.02.2014 a las 14:16h.

censura no justifican la irresponsabilidad de la falta de confirmación de la veracidad de las informaciones.

La fuente no es considerada propietaria del contenido, sino el medio. Por esta razón hay una responsabilización directa del medio que publicó el contenido ofensivo o ilegal y no sólo el deber de remoción como otros proveedores de internet. Es un deber del medio, como mínimo, valerse de todos las vías disponibles e idóneas para certificar la veracidad y autenticidad de la información.

En este sentido, la jurisprudencia brasileña claramente entiende:

> *"ACCIÓN DE INDEMNIZACIÓN - PRENSA - PUBLICACIÓN DE NOTICIA EQUIVOCADA - NEGLIGENCIA - DAÑO MORAL - OFENSA A LA HONRA - QUANTUM INDEMNIZATORIO - MANUTENCIÓN. Es responsable del daño moral causado al ciudadano ofendido, el Periódico que publica noticia equivocada, implicando persona inocente, por motivo de evidente negligencia en la recolección de las informaciones para publicación. La indemnización debe proporcionar a la víctima satisfacción en la justa medida del trastorno sufrido, sin enriquecimiento sin causa, produciendo, en el causante del mal, impacto suficiente para disuadirlo de igual y semejante atentado.*
>
> *(TJ-MG 101450522035540011 MG 1.0145.05.220355-4/001(1), Relator: ALVIMAR DE ÁVILA, Fecha del Juicio: 25/10/2006, Fecha de Publicación: 18/11/2006)."*

La única forma de suprimir la responsabilidad del medio por el contenido falso o equivocado que cause daño a tercero ocurre cuando la fuente posee presumiblemente fe pública, por ejemplo, en el caso de un proceso judicial. Aun así, el medio debe tener la cautela de no distorsionar los hechos presentados.

Además, estas cautelas pueden evitar la propagación de rumores y mentiras entre la población. En 2012, el diputado brasileño Roberto Freire publicó un *tweet* indignado con la presidenta Dilma quien supuestamente modificaría los billetes de un real para que constase en ellos la frase "Lula sea alabado". El post generó diversos comentarios, pero el diputado no puso atención a que la fuente de información era un sitio de humor. Otro caso, bastante relevante trata del portal brasileño UOL que publicó una noticia de un sitio de humor venezolano como si la información hubiese sido divulgada por el gobierno, la noticia decía que la falta de pasta de diente en el país sería motivada por el hecho de que los ciudadanos se cepillaban los dientes tres veces al día.

Por otro lado, además de verificar las informaciones aportadas por estas nuevas fuentes, es necesario respetarlas. Los amateurs tienen los mismos derechos que los periodistas profesionales, principalmente, en lo que se refiere a la protección autoral, dependiendo de autorización previa y expresa para reproducción, edición, inclusión en producción audiovisual, utilización en radiodifusión sonora o televisiva contenidos. En noviembre de 2013, un fotógrafo haitiano fue indemnizado con US$ 1,2 millones, pues sus fotos del terremoto que devastó a Haití publicadas en su perfil en Twitter fueron indebidamente utilizadas y reproducidas por varias agencias de noticias. Algunas de esas fotos fueron, inclusive, portada de periódicos[47].

Hay una diferencia crucial entre lo que es público y lo que está en dominio público en internet. Una foto o un texto colocados en internet pueden ser públicos, pero no son de dominio público. Publicar significa sólo romper

[47] Fuente: http://g1.globo.com/mundo/noticia/2013/11/fotografo-processa-agencias-por-foto-de-terremoto-e-ganha-us-12-milhao.html acceso en 02.02.2014 a las 14:11h.

con lo inédito. Ser de dominio público, por otro lado, presupone que el plazo de protección de los derechos patrimoniales de la referida obra se ha agotado, de acuerdo con los presupuestos legales dispuestos en las Leyes de Derechos Autorales de cada país y también en Convenciones Internacionales. Una obra autoral, sea una fotografía, un video o un texto, solo puede ser utilizada sin autorización por terceros cuando sea de dominio público o cuando tenga la licencia del autor para tal uso – en *Creative Commons,* por ejemplo. Además, aun siendo de dominio público, los autores aun así poseen derechos morales sobre las obras, lo que indica que los medios deben siempre dar el crédito, independientemente del decurso de cualquier plazo, eso ocurre especialmente en los países que su legislación autoral se deriva del Derecho de Autor francés.

Por la ley brasileña en vigor, por ejemplo, no hay violación cuando hay reproducción en la prensa diaria y periódica de noticias o artículos informativos publicados en periódicos o diarios, siempre que sean mencionados el nombre del autor, cuándo aquellos fueron firmados, y el nombre de la publicación de dónde fueron transcritos[48]. La ley estableció la limitación buscando el libre curso de la información, por lo que exceder ese fin significa abusar del derecho en discusión.

De esta manera, como en internet el concepto de diario y periódico es oscuro y hasta subjetivo, es esencial analizar el contenido de la publicación. Por ejemplo, en el caso del fotógrafo haitiano, las agencias de noticias no necesitaban de aquella foto específica para divulgar el reportaje. Además, en ese sentido, un blog puede reproducir una noticia indicando el autor y la fuente, pero no puede reproducir integralmente todas las noticias de un periódico o dedicarse exclusivamente a

[48] Artículo 46, inciso I, apartado *a* de la Ley nº 9.610 de 1998.

reproducciones, bajo pena de estar cometiendo no sólo una violación de los derechos autorales, sino también prácticas de competencia desleal.

Así, la prensa debe ser cautelosa con sus fuentes en todos los sentidos. Prudencia para certificar la veracidad del contenido y atención para no publicar contenidos que violen derechos de tercero. Además de minimizar riesgos jurídicos, lo que proporciona credibilidad al medio y atrae lectores efectivamente interesados en la noticia de calidad.

LA RELACIÓN MÉDICO VS. REDES SOCIALES

Sandra Paula Tomazi Weber

El paciente ya está en Internet y en las Redes Sociales. Por consiguiente, el médico puede utilizar esa herramienta como vía informativa, o sea, para dar informaciones correctas, asegurando la divulgación de un contenido científicamente comprobado y contribuyendo a esclarecimientos y a la educación de la sociedad. Incluso, para apoyar en la movilización de determinadas campañas, como, por ejemplo, de prevención del cáncer y de enfermedades cardiovasculares.

Las desventajas de este uso, por su parte, tienen que ver con la filtración de informaciones confidenciales de pacientes, en caso de que el médico no esté atento al compromiso de confidencialidad que posee como consecuencia del Código de Ética Médica, y con el acoso de pacientes en las redes sociales. Por eso, recomendamos al médico usar canales apropiados para abordar discusiones científicas o temas informativos de su área del conocimiento y no mezclar en el mismo perfil temas que tienen que ver con su vida personal

Además de las redes sociales destinadas a público en general, como Facebook, LinkedIn y Twitter, ha habido un considerable desarrollo de las redes sociales destinadas específicamente a la clase médica, tales como Ology (www.ology.com.br/), iMeds (www.imeds.com.br) y Sermo (www.sermo.com).

En Brasil, el Código de Ética Médica veda al médico hacer referencia a casos clínicos identificables, exhibir pacientes o sus fotos en anuncios profesionales o en la divulgación de temas médicos en medios de comunicación en general, incluso con autorización del paciente. (Art. 75).

Se prohíbe, además, al médico en Brasil divulgar, fuera del medio científico, el proceso de tratamiento o descubrimiento cuyo valor no esté expresamente reconocido científicamente por el órgano competente (Art. 113), así como consultar, diagnosticar o prescribir por cualquier medio de comunicación de masa, lo que incluye Internet (Art. 114). Así, su participación debe ser pautada por el carácter exclusivamente de esclarecimiento y educativo en relación con temas médicos (Art. 111).

Con relación a la creación de páginas, debe observarse los dispositivos legales aquí ya mencionadas, además de la Resolución nº 1.974/2011 del Consejo Federal de Medicina, modificada por la Resolución CFM nº 2.126/2015, que establece los criterios orientadores de la publicidad en Medicina, conceptuando los anuncios, la divulgación de temas médicos, el sensacionalismo, la autopromoción y las prohibiciones referentes a la materia, incluyendo sitios de temas médicos y postura en redes sociales.

La Resolución trae consigo modelos con las principales informaciones que deben constar en las piezas publicitarias, además de presentar un abordaje específico para la publicidad en redes sociales, donde veda al médico de divulgar dirección y teléfono del consultorio, clínica o servicio,

comunicar públicamente informaciones que causen desasosiego a la sociedad, garantizar, prometer o insinuar buenos resultados de tratamiento sin comprobación científica, exponer la figura del paciente como vía de divulgar técnicas, métodos, o resultados del tratamiento, incluyendo la divulgación del antes y el después, publicar en redes sociales autorretrato (selfie), imágenes y/o audios que constituyan sensacionalismo, autopromoción o competencia desleal, entre otros.

La referida Resolución, en su artículo 13, establece, además, que las redes sociales de los médicos y de los establecimientos asistenciales en Medicina deberán obedecer, además de las Leyes y las resoluciones específicas, también al Manual de la Comisión de Divulgación de Asuntos Médicos (Codame).

La intención es favorecer el acceso a las informaciones correctas por parte del paciente, que cada vez más recurre a internet para salir de dudas, y al mismo tiempo evitar la autopromoción del médico y la eliminación del contacto presencial con el paciente, que es tan importante durante el tratamiento.

Es posible, además, resaltar que de hecho es difícil separar en las redes sociales lo que es personal de lo que es profesional, pues existe cierta confusión de la imagen corporativa con la imagen del individuo. ¡No obstante, esa separación se hace necesaria!

Por ejemplo, si el médico tiene un blog, y desea que el contenido sea solo personal, no debe bajo ninguna de las hipótesis comentar temas de trabajo en esta plataforma. Al hacer esto, crea una situación de confusión y de conflicto, en la cual ya no es posible distinguir si lo que fue dicho es de carácter personal o profesional. **Es necesario dejar muy claro el propósito del medio de información utilizado, y el posicionamiento**

del médico tienen que estar alineado con ello. La mayor parte de los errores ocurre debido a la confusión de estos elementos de propósito y posicionamiento.

Se recomienda, además, que, si el médico opta por una red social personal, no agregue a sus contactos pacientes ni curiosos en atenciones online y que active las configuraciones de privacidad ofrecidas por las redes, con el fin de preservar el contenido allí publicado.

Como ya ha sido apuntado en este artículo, el Código de Ética Médica en Brasil prevé reglas para el comportamiento de los profesionales de medicina en los medios de comunicación de masa, como internet, tales como la veda a la divulgación de informaciones sobre temas médicos de forma sensacionalista, promocional o de contenido no verídico, o de consultar, diagnosticar o prescribir a través de cualquier medio de comunicación de masa.

Si el médico comete cualquier falta grave, como el irrespeto a las vedas presentadas anteriormente, su ejercicio profesional podrá ser suspendido mediante un procedimiento administrativo específico.

En Chile, también existe una preocupación con la privacidad del paciente y la relación del médico con las redes sociales. No hay veda sobre el uso, pero el profesional del área médica debe actuar en estos canales observando siempre los límites éticos y de preservación de la privacidad del paciente.

Lamentablemente, en junio de 2017, el país presenció un incidente en las redes sociales que generó revueltas entre la población. Un video mostraba a un equipo médico dentro de un centro quirúrgico mirando un partido de fútbol, mientras el paciente estaba en la mesa esperando para ser operado. [49]

[49]Fuente: http://esporte.ig.com.br/futebol/2017-06-29/equipe-medica-chile-revolta.html Acceso en: 05/07/2017.

En la era de la tecnología, tenemos que tener mucho cuidado con nuestras actitudes. Y esa preocupación se extiende al área médica.

A pesar del incidente, vale decir que la Organización Médica Colegial chilena, de conjunto con el Consejo General de las Facultades Oficiales de Medicina, elaboraron el "Manual de Estilo para médicos y estudiantes de Medicina sobre el uso adecuado de las redes sociales"50. La publicación, de carácter orientador, fue dividida en los siguientes capítulo: (i) Confidencialidad y secreto médico; (ii) Consejo médico a pacientes virtuales; (iii) Cuidados con la actitud e imagen del médico como usuario de las redes sociales; (iv) Uso de las nuevas tecnologías y la imagen del médico en la consulta directa con el paciente; (v) Responsabilidad sobre la información médica difundida en las redes sociales; (vi) Las relaciones entre colegas profesionales en las redes sociales y (viii) Publicidad, marketing y branding médico.

El objetivo del Manual es reforzar el compromiso de la profesión con la Sociedad y un ejercicio de autorregulación con la finalidad de mantener la confianza social.

DIGA NO A LA DISCRIMINACIÓN EN INTERNET

Patricia Peck Pinheiro

¿Estará la tecnología ayudando a volvernos más tolerantes o sería lo contrario? En los últimos años, ha aumentado la cantidad de casos involucrando prácticas racistas y discriminatorias en internet. ¿Por qué será que eso está ocurriendo?

Primeramente, debemos considerar que el avance de las herramientas de comunicación a distancia permitió no solo una mayor conexión entre todos, sino que también generó un efecto paradójico al aproximar a quien está lejos y alejar a quien está cerca.

[50] Fuente: https://www.cgcom.es/sites/default/files/u183/Manual%20Redes%20Sociales%20OMC.pdf Acceso en: 05/07/2017.

Curiosamente, la interfaz gráfica tiene el poder de volvernos más indiferentes a lo que está sucediendo a nuestro alrededor, así como también confiere más valor para que haya manifestaciones de opinión y pensamiento que no ocurrirían cara a cara.

¿Querrá eso decir que el mundo digital, con su promesa de "pseudo-anonimato", está volviéndonos más crueles?

Desde el punto de vista jurídico, las palabras escritas tienen un efecto mucho más devastador que lo que es verbalizado. Cuando nos relacionamos, el contexto, las expresiones faciales, la voz, todo forma parte del acto de comunicarse e integra el lenguaje.

Sin embargo, el ambiente de internet, con sus espacios de pensamientos instantáneos e impulsivos, simplificó demasiado la comunicación al punto de provocar más ruidos.

Sumado al espíritu juguetón y jocoso del brasileño, tenemos todos los ingredientes para impulsar el crecimiento de la discriminación en internet.

Terminamos siendo mucho más críticos con los contenidos ajenos cuando estamos protegidos por detrás de nuestras pantallas, ya sea del celular, del *tablet* o de la computadora.

Y lo peor de todo eso es que no hay arrepentimiento digital. Después que un usuario comparte un contenido que pueda ser interpretado como racista o discriminatorio, no hay vuelta atrás. Y hoy, se corre el riesgo de entenderse de ese modo. ¿Estaremos también más sensibles a las opiniones?

En nuestras burbujas digitales, una de las cosas que ciertamente internet no nos trajo fue más tolerancia y aceptación hacia las diferencias del otro. Interactuar se volvió una disculpa para entrometerse en la vida del prójimo.

Así, los testimonios de las máquinas podrán un día relatar si a través de ellas nos volvimos mejores o peores. Hasta entonces, el mejor consejo es leer dos veces antes de publicar. Como dice Twitter: "piense y publique". Pues todo lo que hacemos tiene consecuencias.

EL POST DE LA ESTRELLA

Victor Auilo Haikal

Cada vez me impresiono más con el comportamiento de los seres humanos, en especial por lo impactos que resultan de la alta capacidad de acceso a la información y del alcance obtenido por contenidos compartidos. En cuestión de segundos un mensaje puede ser reenviado múltiples veces y llegar a ser de conocimiento global, generando la sensación de que el mundo entero lo escucha.
Gritos silenciosos de las más diversas naturalezas pueden ser observados constantemente en las redes sociales. Pero, llaman la atención los chillidos dejados por dos adolescentes que fueron víctimas de la divulgación de contenido sexual, en contra de su voluntad, por los medios de información y comunicación, terminando en impactantes suicidios.

1:

"Yo te amo, discúlpame por no ser la hija perfecta, pero lo intenté…disculpa disculpa yo te amo mucho mamita.. ¡disculpa, disculpa…! Recuerda este día 10.11.13"

"Dentro de poco todo acaba. Tengo miedo pero creo que es un adiós para siempre.[51]*"*

2:

"Hoy por la tarde resuelvo eso. No seré más un estorbo para nadie.[52]*"*

Aunque espantado por la secuencia de los hechos ocurridos en tan breve lapso de tiempo, el primero el día 10 de noviembre de 2013 y el segundo el día 14 del mismo mes, fue inevitable la conexión de ambos incidentes con el ejemplo de Micronesia señalado por Malcolm Gladwell en su obra "El punto clave", destacando el alto índice de suicidios de aquel país, el rango de edad de las víctimas y los motivos que las llevaron a tales prácticas.

Debido al grado de desarrollo tecnológico, entre las décadas de 1960 y 1980, en vez de posts en redes sociales, fueron dejadas notas de papel. La transcripción de una de ellas merece realce por la carga de dolor que contiene y el motivo que provocó el incidente. Sima, de 17 años, fue expulsado de casa por su padre (severo y exigente) después de no hallar un cuchillo de bambú para cortar un fruto del pan, lo que comprometió la alimentación de la familia.

"Mi vida llega a su fin ahora. Hoy es un día triste y también de sufrimiento para mí. Pero es un día de conmemoración para Papá. Hoy papá me echó de casa. Gracias por amarme tan poco. Sima.

Dígale a mamá que le dejo mi adiós. Mamá, su hijo no le traerá más preocupación ni frustraciones. Mucho amor, de Sima[53]*."*

[51] http://oglobo.globo.com/pais/adolescente-se-mata-apos-ter-video-de-sexo-com-um-casal-divulgado-na-internet-10782350. Acceso en: 9.12.2013 a las 9h (UTC -2:00)

[52] http://noticias.terra.com.br/brasil/policia/rs-jovem-confirma-que-fez-e-postou-foto-intima-de-adolescente-que-se-matou,ef6a73c3df672410VgnVCM3000009af154d0RCRD.html. Acceso en 9.12.2013 a las 9h05 (UTC -2:00)

[53] Gladwell, M. (2000). O ponto da virada. Río de Janeiro: 2009, Editora Sextante. pp. 209-210.

Otros adolescentes de ese país se suicidaron por motivos que amargan la vida diaria, por ejemplo, la negativa de mesada por parte de los padres, la recusa de compra del traje de la graduación, discutir con el hermano mayor por ruido excesivo y por traición amorosa, pasando a ser algo sintomático de esa sociedad, considerado incluso como algo común y corriente.

Situaciones como las ocurridas en Micronesia son preocupantes, principalmente, porque la mayoría de los involucrados están en el final de la adolescencia, momento de constantes conflictos y formación de las bases de la personalidad, y por promover ejemplos a las personas que pasan por situación de dolor similar y tienden a encontrar en el suicidio la solución para acabar con el sufrimiento, aunque involuntariamente, sirviendo como patente evidencia del último soplo de protesta contra los malos tratos, evidenciando el orgullo herido y la auto-conmiseración.

Es común encontrar plataformas digitales sociales alimentadas constantemente por sus usuarios con el envío de fotos, videos y descripciones de hechos que llegan a crear vínculos relevantes entre los lectores, especialmente con desahogos personales o indignados, que son rápidamente respondidos con solidaridad internáutica, comparticiones masivas o condolencias de apoyo y consuelo.

Algunas veces el número de comparticiones y el grado de exposición personal adoptados por la generación de los nativos digitales (nacidos después de 1995) espantan, siendo automática la asociación, pero, con el añadido del componente de interacción y replicación de los contenidos.

Mientras que los individuos buscan retratarse en los medios digitales ansiando la perfección y admiración por los más diversos motivos (popularidad, aceptación, aprobación y reconocimiento), un simple

comentario negativo o crítica puede volverse una amenaza de mácula en sus páginas de presentación, imponiendo medidas inmediatas. Siendo así, ¿qué decir sobre la divulgación de material íntimo, que podrá perdurar por tiempo indeterminado?

Esta alarmante situación sufrida sobre todo por mujeres jóvenes e incluso hasta niños, no se limitan a producirse en Brasil, sino en toda América Latina, siendo México el exponente más sensible por el número de incidentes y habiendo Chile también registrado casos de personas públicamente expuestas, habiendo sufrido con esas prácticas desde 2013.

Los mensajes dejados por las adolescentes brasileñas expresan el dolor sentido por la existencia de un escenario patológico que merece atención, denotando (i) las exigencias y expectativas a la que estaban sometidas: en primer lugar, por los padres y en segundo por el resto de la sociedad, además (ii) de la maldad contenida en el acto de compartir material de esta naturaleza para humillación y exposición al ridículo.

Imaginando que era insuperable el trauma sufrido, gritaron desde el alma para que todos oyeran la ensordecedora crueldad de la agresión sufrida y supieran cuán frágil podemos volvernos, en contraste con la impavidez de las fotos estampadas en las presentaciones personales en internet, principalmente, cuando existe el objetivo pernicioso de la venganza.

Y, además, utilizaron el recurso de la abdicación a la vida como forma de redención, pues buscaron restaurar la dignidad alcanzada por la auto aplicación de la pena de muerte frente a la falta grave, ante la familia y la sociedad (practicar sexo), para exigir que fueran recordadas como mártires de la traición en su más puro significado, donde hay explotación de vulnerabilidades por el abuso de confianza, al contrario de la situación de humillación contenida en el material que fue ilegalmente diseminado.

El resultado fue instantáneo. Presentes en todos los canales de comunicación, las jóvenes estrellas de brillo solar irradiaban la luz nacida de la culpa social fabricada por los ideales de perfección que condenan la libertad de las personas (principalmente la sexual y femenina), además de ofuscar la visión de aquellos que buscan las fallas y los errores de los otros todo el tiempo para enaltecer su propio ego y avergonzar aún más a las víctimas.

Creo que deben ser evitadas las formaciones de constelaciones de esta forma, pues pueden generar inestabilidad social y son de difícil control, donde ser notado significa poner fin a la propia existencia, sobre todo porque dejamos de escuchar a las estrellas, por estar muy ocupados en la búsqueda de la perfección.

CAPÍTULO SEPTIMO
GESTIÓN Y TECNOLOGÍA DE LA INFORMACIÓN

LA RESPONSABILIDAD DE LOS ESTABLECIMEINTOS COMERCIALES EN EL SUMINISTRO DE RED WI-FI A SUS CLIENTES

Rafael Mott Farah

En una sociedad cada vez más conectada y con hábitos digitales, el suministro de Internet sin cable (Wi-Fi) por parte de los establecimientos comerciales acaba volviéndose casi un prerrequisito para continuar siendo fuerte en la competencia por clientes, los cuales prefieren utilizar este tipo de conexión a las redes 3G o 4G de su propio dispositivo, debido a su lentitud y constante inestabilidad.

En enero de 2015, las empresas *AirTight* y *EarthLink*, en colaboración, divulgaron una investigación[54] dirigida por el *IHL Group.* El estudio realizado tuvo como objeto medir el impacto del servicio de conexión gratuito en los establecimientos comerciales sobre temas como satisfacción y fidelización del cliente

No muy lejos de lo esperado, la investigación demostró que el 27,5% de las tiendas que ofrecen red Wi-Fi a sus clientes registraron un aumento significativo de los niveles de fidelidad. De igual forma el 82% de las medianas y grandes empresas de comercio minorista de los EUA ya instalaron Wi-Fi en sus tiendas, mientras que el 57% de los establecimientos ofrecen conexiones Wi-Fi tanto para clientes como para empleados.

Así, es evidente que el suministro gratuito de Internet a clientes implica una cadena de amenazas directas e indirectas, las que serán

[54] Diponible en: [www.airtightnetworks.com/home/news/pr/article/123/study-finds-28-of-retailers-report-increased-customer-loyalty-due-to-in-store-wifi.html]. Acceso en: 07.05.2015.

posteriormente analizadas en el presente artículo, tanto para el establecimiento que suministra la conexión como para el cliente que la utiliza. Sin embargo, las posibilidades de problemas jurídicos y de seguridad de información pueden ser mitigadas con el uso de las medidas preventivas.

En este punto, se hace necesario una breve explicación del procedimiento más común para la identificación de autoría en Internet:

- ✓ Primeramente, es necesario obtener el IP (*Internet Protocol)* del responsable de la práctica del acto del cual se desea identificar la autoría, así como el momento exacto en que se comete la acción, lo que se puede dar por medio del análisis de los vestigios digitales o por acción judicial ante el proveedor de aplicación.

- ✓ Con el IP y el horario en mano, es posible evaluar la acción contra el proveedor de conexión responsable (por ej.: Vivo, Claro, Net, etc.), el cual proporcionará los dados registrados de sus clientes.

Vale destacar que de acuerdo con la Ley 12.965/2014 – Marco Civil de Internet, tales datos de registro solo podrán ser suministrados por medio de una orden judicial.

Esto ocurre porque entre los principios establecidos por la ley que regula el uso de Internet en Brasil están la protección de la privacidad y la protección de los datos personales. Corroborando esta protección, el art. 7.º, VII, aporta la necesidad de consentimiento libre y expreso del usuario para la divulgación de sus datos personales, incluso registros de conexión y de acceso a aplicaciones de Internet.

En ese ámbito, imaginemos que después de todo el trámite investigativo, los datos de registro suministrados por el proveedor de conexión sean los

datos de un establecimiento comercial que provee *Wi-Fi* gratuitamente a sus clientes.

Obviamente, aquel que busca la identificación de la autoría procesará judicialmente al establecimiento para que suministre los datos que posee, de forma tal, que, ante la imposibilidad de identificación e individualización de sus usuarios, el propio establecimiento responderá por la acción ilícita, en los términos de los arts. 186[55] y 927[56] del Código Civil.

Además de la evidente aplicabilidad de los mencionados artículos del Código Civil, si el establecimiento es obligado judicialmente a presentar los datos del usuario responsable del acto ilícito y no lo hace por no tener tal capacidad, se puede aplicar también, el art. 499[57] del Nuevo Código de Proceso Civil, siendo la obligación hacer la conversión en pérdidas y daños.

Además, al proveer Wi-fi a sus clientes, observándose el carácter obviamente comercial de esta actividad, entendemos que es posible, también, la aplicación del art. 3.º, VI del Marco Civil de Internet, el cual prevé *"la responsabilización de los agentes de acuerdo con sus actividades, en los términos de la ley".* De esta forma, al incorporar un nuevo servicio con la idea de captar y fidelizar clientes, el establecimiento debe estar atento a las mejores prácticas de Seguridad de la Información, así como a su blindaje jurídico, pues está asumiendo un riesgo.

La eventual identificación de posibles autores de actos ilícitos en la red mundial de computadoras forma parte del riesgo de aquel que habilita su

[55] "Art. 186. *Aquel que, por* acción u omisión voluntaria, *negligencia o imprudencia, viole derechos y cause daños a otro*, aunque exclusivamente moral, *comete acto ilícito*

[56] "Art. 927. *Aquel que, por acto ilícito (arts. 186 y 187), cause daño a otro, queda obligado a repararlo*. Párrafo único. *Habrá obligación de reparar el daño, independientemente de culpa, en los casos especificados en ley, o cuando la actividad normalmente desarrollada por el autor del daño implique, por su naturaleza, riesgo para los derechos del otro.*"

[57] "Art. 499. La obligación solo será convertida en perdidas y daños si el autor lo requiere o si es imposible la tutela específica u obtención de la tutela por el resultado práctico equivalente.

red para acceso ajeno, de forma tal que debe sustentar la carga de no conseguir identificar/individualizar a determinado usuario.

Internet trae consigo la posibilidad de cometer una vasta gama de actos ilícitos, tantos como en la vida real, o sea, desde crímenes contra la honra y pedofilia, hasta fraudes bancarios y robo de datos, de modo que aquel que suministra la conexión debe estar al corriente de esos riesgos.

Observándose el carácter evidentemente comercial del suministro gratuito de Wi-Fi en establecimientos comerciales, queda claro la posibilidad de aplicación del Código de Defensa del Consumidor para transformar la relación entre el establecimiento y la víctima del acto ilícito en relación de consumo, en los términos de sus artículos 3.º[58] y 17[59].

De ese modo lo entendió el Tribunal Superior de Justicia[60] al decidir que la explotación comercial de Internet sujeta las relaciones de consumo, "*pues el término 'mediante remuneración', contenido en el art. 3.º, § 2.º, del Código de Defensa del Consumidor, debe ser interpretado de forma amplia, de modo tal que incluya la ganancia indirecta del proveedor".*

Se entendió, además, que, al tener conocimiento de determinado acto ilícito, aquel que posee responsabilidad sobre este *"debe actuar de forma enérgica, bajo pena de responder solidariamente con el autor directo del daño, a causa de la práctica omitida".*

En el mismo juicio, consta que "*al ofrecer un servicio por medio del cual se posibilita que los usuarios exterioricen libremente su opinión debe (…) tenerse el cuidado de propiciar medios para que se pueda identificar cada uno de esos usuarios, inhibiendo el anonimato y atribuyendo a cada manifestación una autoría correcta y determinada. (…) este debe adoptar*

[58] "Art. 3.° Proveedor es toda persona física o jurídica, pública o privada, nacional o extranjera, así como los entes sin personalidad, que desarrollan actividad de producción, montaje, creación, construcción, transformación, importación, exportación, distribución o comercialización de productos o prestación de servicios.
§ 1.° Producto es cualquier bien, móvil o inmóvil, material o inmaterial.
§ 2.°." Servicio es cualquier actividad suministrada en el mercado de consumo, mediante remuneración, incluso las de naturaleza bancaria, financiera, de crédito y de seguridad, salvo las derivadas de las relaciones de carácter laboral."
[59] "Art. 17. Para los efectos de esta Sección, *se equiparan a los consumidores todas las víctimas del acontecimiento*"
[60] REsp 1.300.161/RS, Rel. Ministra Nancy Andrighi, 3.ª T., *DJe* 26.06.2012.

las providencias que, de acuerdo con las circunstancias específicas de cada caso, estén a su alcance para la individualización de los usuarios, bajo pena de responsabilización subjetiva por culpa in omittendo*"*

Así, no quedando ninguna duda sobre la diferenciación obtenida al proveer Wi-Fi a sus clientes, ni respecto a la posibilidad de responsabilización del establecimiento que suministra Internet en el caso de la no individualización del acceso de sus usuarios, se muestra esencial el blindaje legal de las empresas para que mitiguen los riesgos y continúen ofreciendo los mejores servicios a sus clientes.

Entre las medidas que pueden ser tomadas existen tres que merecen especial atención y serán expuestas detalladamente a continuación, siendo **(i)** la elaboración de Términos de Uso, **(ii)** la creación de una *BlackList* o de una *WhiteList* y **(iii)** la implantación de metodologías que garantizan la identificación del usuario.

Los "Términos de Uso" deberán dar a conocer a los usuarios sobre el monitoreo de la red, así como dejar exento al establecimiento de cualquier daño, perjuicio o pérdida del equipo del cliente, incluso por acciones de softwares maliciosos. Es imprescindible que exista un sistema en el cual el usuario manifieste expresamente su acuerdo con el documento (*Opt In*) antes de proceder al efectivo acceso a Internet.

La individualización del acceso se puede dar de diversas formas, sea con la verificación a través de vínculo con Redes Sociales, por medio de código único enviado por SMS o hasta incluso con la solicitud de documentación del cliente, con el posterior suministro de contraseña única. En el caso de instituciones de educación, es posible vincular el acceso al código de matrícula del alumno combinado con una contraseña personal e intransferible.

Además, recomendamos la elaboración de una *blacklist* o de una *whitelist,* siendo esta una lista que permite el acceso solo a determinados dominios/direcciones IP, previamente escogidos por el establecimiento, mientras que la primera se trata de una lista de dominios/direcciones prohibidos por el establecimiento. El filtro de la *blacklist* también puede darse mediante el uso de palabras claves.

No hay ninguna objeción respecto a que el establecimiento opte por la implementación de ambas providencias al mismo tiempo, por el contrario.

Además, es necesario que se sepa por cuánto tiempo los datos en cuestión deben ser almacenados por el establecimiento, tema bastante polémico y controversial en los tribunales. Sin embargo, siendo cierto que aquel que solo suministra Wi-Fi no se encuadra en las definiciones de "proveedor" del Marco Civil de Internet, no hay que hablar sobre el plazo dispuesto en este diploma legal. Pero, frente a la relación de consumo que se configura, debemos estar atentos al plazo de cinco años, dispuesto en el art. 27 del código de Defensa del Consumidor.

Por último, el acto de proveer Wi-Fi a sus clientes genera grandes beneficios al mismo tiempo que exige del establecimiento responsabilidades, las que son inexcusables, de forma tal que se hace esencial la toma de precauciones que tengan como objetivo adecuar el establecimiento a las mejores prácticas de seguridad de la información, así como a su blindaje jurídico, para, de esta forma, mitigar los riesgos generados por la acción comercial.

DIGITALIZACIÓN ES UN PALIATIVO: ¡PIENSE EN PROYECTOS TOTALMENTE DIGITALES!

Sandra Paula Tomazi Weber

Muchas empresas ante la presión ambiental, económica y hasta de la propia evolución de la sociedad, que es cada vez más digital, piensan en la digitalización como una solución para disminuir el volumen de papel y, también, para ganar en agilidad y disponibilidad en la circulación de sus informaciones.

De hecho, la digitalización permite alcanzar todo eso, sin embargo, continúa siendo una migración de soporte, lo que reduce la capacidad de pericia ante un incidente de falsedad con relación a la identidad de quien firmó el documento, o incluso con relación a la integridad del documento. Una situación común, inclusive porque con la microfilmación, que también es una forma de migración de soporte, tal capacidad de pericia ya era reducida.

Sin embargo, no hay necesidad de permanecer en este riego, ¡pues la tendencia es que los documentos ya nazcan originalmente electrónicos!

Por consiguiente, podemos pensar que la solución son los negocios firmados en medio electrónico, y encarar la digitalización como un paliativo con relación al legado.

Necesitamos entender que documento es cualquier escrito capaz de comprenderse. El papel es solo una de las especies del género documento, en este caso el más abarcador, podemos alcanzar otros soportes, como el electrónico.

Vicente Greco Hijo, así decía "[...] no solo los papeles escritos son documentos. Documento es todo objeto del cual se extraen hechos debidos a la existencia de símbolos o señales gráficos, mecánicos, electromagnéticos, etc. Es documento, por tanto, una piedra sobre la cual estén impresos caracteres, símbolos, o letras; es documento una cinta magnética para su reproducción por medio del propio aparato, o filme fotográfico, etc." (GRECO FILHO, 2000, p. 208).

En el derecho brasileño sustentamos tal afirmación en base a los arts. 231 al 238 del Código de Proceso Penal; art. 212, II y 215 al 226 del Código Civil; arts. 405 al 429 y los arts. más recientes 439 al 441, todos del Código de Proceso Civil. En este sentido, se destaca el art. 232 del Código de Proceso Penal: "Se consideran documentos cualquier escrito o papel, públicos o particulares".

El documento electrónico, a diferencia del documento de papel, no está preso al medio por el que fue producido. Esto ocurre porque puede ser transferido y almacenado de una computadora a otra, de un disco flexible a otro, estar en varias computadoras al mismo tiempo sin perder su característica de original. Leal (2007, p. 153) explica que eso es posible porque si no hay alteraciones en la secuencia de bits, se tendrá siempre el mismo documento. *Por consiguiente, no hay por qué hablar de copia de documento electrónico, porque estos siempre son originales, y tampoco sobre limitación de su capacidad de pericia, teniendo en cuenta que no hay migración de soporte.*

El poder judicial es una referencia al estímulo de una sociedad cada vez más *Paperless*, ya que desde 2006, con la Ley 11.419, pasó a estimular la tramitación de los procesos en formato electrónico, e hizo familiar en su medio palabras y términos como certificado digital, archivos

electrónicos, entre otros. Esa familiaridad es muy buena, ya que las pruebas electrónicas son cada vez más frecuentes y fundamentales, si no, veamos:

RECURSO DE REVISTA. VALIDEZ DE LOS HORARIOS REGISTRADOS EN EL PUNTO ELECTRÓNICO. HORAS EXTRAS. La Corte a quo, soberana en el análisis del conjunto fáctico-probatorio de los autos, concluyó que la prueba producida por el reclamante no logró demostrar la invalidez de los registros del punto electrónico. (TST, RR 13030009200750405713 0300-09.2007.5.04.0571, Rel. Augusto César Leite de Carvalho, j. 02.05.2012).

ACCIÓN DE COBRAR. Empréstito hecho al reo a través de depósitos bancarios Reo rebelde Alegación de tratarse de donación que no quedó aprobada. *Mensaje vía documento electrónico (e-mail) confesando la existencia de la deuda, enviada a la autora no impugnado en contestación.* Presunción de veracidad de los hechos narrados en la inicial que no fue eliminada por pruebas en contra. Sentencia mantenida. Art. 252, del RITJESP Recurso negado (TJ/SP, Apelación 0125971-11.2008.8.26.0100, Rel. Des. Ligia Araújo Bisogni, j. 14.09.2011).

INDEMNIZACIÓN– INTERVENCIÓN DEL MINISTERIO PÚBLICO – INNECESARIO – LESIÓN – RESPONSABILIDAD – MÉDICO – HOSPITAL – CDC – APLICABILIDAD. [...] En los términos de la Ley 8.078/1990, es objetiva la responsabilidad del hospital, dependiendo, sin embargo, de la prueba de culpa, relativa a los profesionales de medicina [...] El incumplimiento del deber de elaborar una historia clínica leal e inteligible, no puede beneficiar a aquel que se descuidó de su obligación profesional, que tenía el deber de producir la prueba. Fragmento [...] *considero que solamente demostraron fuerza probatoria las copias de las historias*

clínicas de las páginas 52 y 53 de los autos de la medida cautelar y página 235, de la acción judicial principal, por tratarse de impresos emitidos por la computadora del hospital, conteniendo la fecha y la hora en que fueran producidos, siendo imposible asegurar lo mismo para el resto del material. (TJ/MG: Apelación Civil 1.0142.04.006571-6/002, Rel.: Des. Antônio Bispo, Fecha de publicación: 26.02.2010).

Es posible percibir por los juicios citados que la evolución del registro de entrada y salida del empleado del papel hacia el formato electrónico (Ordenanza 1.510/09 – Registrador Electrónico de Punto) fortaleció su credibilidad ante el poder judicial. Que el e-mail, independientemente de estar firmado o no con certificado digital ICP- Brasil, es aceptado y utilizado para demostrar negocios firmados entre las partes. Y que, por último, la historia clínica del paciente, aunque generada en un sistema fuera de los estándares del Consejo Federal de Medicina, puede ser aceptada por el Juez, en defensa de la víctima, dado que el médico no cumplió con su obligación de registrar en el papel los datos de forma legible.

Ante esta realidad, donde los testigos son las máquinas y el documento no es sólo el papel, no hay por qué temer y negar la necesidad de rever los modelos de negocio e inclusive la forma de fírmalos desde el inicio en formato digital.

Desde noviembre de 2013, la Agencia Tributaria Federal disciplinó la entrega de documentos en formato digital para unirlos al proceso digital o al dossier de atención, por medio de la Instrucción Normativa 1.412. El procedimiento es hecho a través de la utilización del Programa Generador de Solicitud de Compilación de Documentos (PGS) y como forma de autenticación, fue adoptada la firma digital ICP-Brasil.

Otra reglamentación en el medio electrónico ocurrió en el ámbito del Consejo Nacional de Seguros Privados – CNPS, órgano responsable por establecer las directrices y normas de la política de seguros privados. La Resolución CNSP 294/2013, del 06.09.2013, viabilizó la comercialización de productos del seguro (de vida y otras modalidades diversas) y previdencia complementaria, a distancia, principalmente vía internet. Incluso, permitiendo el uso de otras formas de autenticación, además del certificado ICP-Brasil.

La referida Resolución en su art. 9.º obliga al Contratado a enviar mensajes informativos al Contratante a lo lardo de la vigencia de las coberturas y en el momento apropiado para cada situación, contemplando, al menos, la confirmación de la contratación del seguro y el número de proceso Susep; las coberturas y/o beneficios contratados y los respectivos valores de garantía y/o de capital asegurado; alerta sobre el fin de la vigencia del seguro contratado, etc.

Siempre que el ramo de desempeño de la empresa sea reglamentado, es importante consultar al órgano responsable y sus normativas para verificar si hay alguna restricción que inviabilice la adopción del formato electrónico. Lo que hemos percibido es que, en algunos casos, hay exigencias que necesitan ser cumplidas, como las citadas en el caso anterior.

El ordenamiento jurídico en vigor, de modo general, favorece la libertad de las formas para los contratos consensuales, o sea, aquellos que se perfeccionan con confluencia de manifestaciones de voluntad (art. 107 de nuestro Código Civil). Esto significa que, en todo contrato, para el que no exista una formalidad legal prevista, se puede obtener la manifestación

de voluntad por cualquier procedimiento hábil e idóneo, incluso el formato electrónico, sea con el uso de certificado ICP-Brasil u otro.

El poder judicial, incluso, acepta la ejecución de contratos donde los testigos firmaron de forma electrónica:

PROCESAL CIVIL. AGRAVIO DE INSTRUMENTO. EJECUCIÓN DE TÍTULO EXTRAJUDICIAL. EXCEPCIÓN DE PRE-EJECUCIÓN. CONTRATO ELECTRÓNICO. FIRMA DIGITAL. *VALIDEZ*. INCLUSIÓN DEL FIADOR DESPUÉS DE LA CITACIÓN DE LO EJECUTADO. POSIBILIDAD. ART. 264 DEL CPC. INAPLICABILIDAD. …ausencia de título ejecutivo a causa de la inexistencia de dos firmas. (art. 585, II, del CPC).

"…el contrato fue firmado por testigos, aunque se trate de firma digital; conviene resaltar que, debido a las innovaciones electrónicas, la forma del contrato puede ser diferente, pero no desvirtúa su esencia."

(TRF-2 – AG: 201302010129860, Rel.: Juez Federal de Apelación José Antonio Lisboa Neiva, *DJ*: 18.12.2013, 7.ª T. Especializada, Fecha de Publicación: 14.01.2014).

Por tanto, el camino no es seguir utilizando el papel para huir de lo nuevo y continuar digitalizándolo, si la idea es descartarlo. Entendemos que el rumbo a seguir es:

- Conocer su operación, mapear todo el flujo, y entender por qué es hecho de esta forma;
- Verificar si hay algún impedimento para que la operación sea firmada, desde su origen, en documento electrónico;

- Si hay alguna obligación para que la operación en formato electrónico ocurra y si es posible atenderla;
- Crear una cultura de uso del medio electrónico, para que la nueva solución sea acogida por todos los involucrados.
- Adoptar la digitalización sólo como un medio y no como un fin;
- Actualizar su política de gestión documental para manejar los documentos físicos, digitalizados y electrónicos.

Referencias bibliográficas:

GRECO FILHO, Vicente. *Direito Processual Civil Brasileiro*. 14 ed. São Paulo: Ed. Saraiva, 2000.

LEAL, Sheila do Rocio Cercal Santos. *Contratos Eletrônicos*: Validade Jurídica dos Contratos via Internet. São Paulo: Editora Atlas, 2007.

PINHEIRO, Patricia Peck. *Direito Digital*. 5 ed. São Paulo: Saraiva, 2013.

CONCIENTIZAR SOBRE SEGURIDAD DE LA INFORMACIÓN ES PROTEGER SU NEGOCIO

Victor Auilo Haikal

Toda reflexión y análisis de temas relevantes sobre Seguridad de la Información deben abordar los componentes fundamentales de redes de la información – personas, procedimientos, políticas, hardware, software, datos y redes – bajo la perspectiva de proteger la confidencialidad, disponibilidad, integridad, autenticidad y legalidad implicadas.

Por más que se refuercen los controles de seguridad y las medidas de protección que comprendan el grupo de Recursos de Tecnología de la Información y Comunicación – RTICS (hardware, software, datos y redes), los incidentes tienden a ocurrir por la conocida debilidad humana, factor presente en hasta el 95% de los casos, según un estudio elaborado por IBM[1]. Las fallas más comunes son:

- Configuración equivocada del sistema;
- Gestión inadecuada de correcciones (patches);
- Utilización de nombres de usuario y contraseñas predeterminados, o esta última de fácil adivinación;
- Pérdida de laptops y otros dispositivos móviles;
- Filtración de la información por digitación equivocada de e-mail; y, comportamiento el más significativo,
- Doble clic en adjunto de e-mail infectado o clic en link de internet no seguro.

El componente humano puede sufrir por amenazas digitales y contribuir a que se produzcan crímenes o actos ilegales, por diversos factores, entre ellos[2]:

- No estar acostumbrado a internet o ser un usuario reciente;
- Ser una persona ingenua;
- Tener baja capacidad de percepción o tenerla dañada, ya sea por alguna condición física o psicológica;
- Desespero, ganancia, carencia u otro disturbio emocional;
- Simplemente estar en el lugar equivocado en el momento equivocado.

Dado que la falla del componente humano es previsible, se debe reforzar los controles de seguridad activos en los dispositivos utilizados para mitigar la exposición a vulnerabilidades, denominados *Endpoint Detection and Response* (EDR), cuya traducción es Detención y Respuestas a Incidentes en los Terminales de Acceso, que comprenden el escaneo en tiempo real de virus, scripts maliciosos, direcciones de internet no confiables y potenciales contenidos falsos en redes sociales.

Tener procedimientos y políticas relacionadas con los sistemas de información en adecuación con el Derecho digital, actualizados y bien definidos, es prerrequisito para la ejecución de las tareas de organización y producción de las empresas, pero pueden no surtir el efecto deseado si se abordan aisladamente.

Tomando los posibles incidentes anteriores como desafíos a ser superados, tenemos que la instrucción correcta y la orientación adecuada de la utilización de los RTICS son esenciales para disminuir el número de incidentes y preservar los activos intangibles de la empresa y la continuidad de los negocios, **teniendo en cuenta que están directamente relacionados al comportamiento del usuario.**

La falsa impresión de que los cuidados con el comportamiento tendrán solamente impacto en la utilización con fines particulares de los RTICS no se sustenta, ya que tareas corporativas son ejecutadas esencialmente por personas y, la mayoría de ellas contienen aspectos similares a las particulares. Por tanto, dirigir los cuidados y las preocupaciones a la utilización de los RTICS por las personas es proteger todo el sistema.

La dependencia cada vez mayor de las redes de información se refleja directamente en el aumento del número de incidentes reportados de forma repetida a lo largo de los años por las empresas especializadas, mereciendo realce el registro de los secuestros de datos (ransomware).

Los casos involucrando esos ataques crecieron un 113% de 2013 a 2014, con un aumento sensible en el último cuatrimestre [3]. Adicionalmente, el *phishing* dirigido creció un 43% en las empresas de más de 2.500 trabajadores [4] y los archivos .doc quedaron en primer lugar entre las amenazas detectadas, con un 38% de las incidencias, superando al .exe, que tuvo un 22,6% de esta modalidad de *phishing*[5].

Es importante destacar que la concientización debe tener como premisa la existencia inevitable de vulnerabilidades, y por eso, las orientaciones no pueden limitarse a eventos o prácticas aisladas, debiendo ser ejecutadas de forma abarcadora. Este trabajo necesita tener como objetivo la detección tanto de las vulnerabilidades no identificadas por los usuarios como de aquellas que generaron dudas y que resultaron en elecciones equivocadas por parte de esos usuarios.

La precaución es similar a las vacunas y deben ser aplicadas periódicamente para no perder la eficacia, especialmente ante el dinamismo en la evolución y sofisticación de los ataques de *hackers mal intencionados,* ni que sus acometidas de compromiso de seguridad sean descubiertas

Para tener éxito, es indispensable que las campañas de concientización estén en sintonía con el escenario tecnológico actual, ya previendo las próximas posibles amenazas, identificando los puntos comunes en todas ellas y el elemento de ingeniería social que puede ser parte de la puerta de entrada de un ataque masivo.

Debemos recordar que, en un escenario económico desfavorable, que se produzca cualquier perjuicio como consecuencia de un incidente de Seguridad de la información puede ser, incluso, más sensible.

Entonces, se recomienda programar campañas de concientización como prioridad para los sectores de Seguridad de la Información, Recursos Humanos, *Compliance*, Marketing, Financiero y Jurídico, cuya preocupación con la productividad será completada por la sensible disminución de pérdidas, generando un mayor rendimiento de inversiones para la empresa.

Referencias bibliográficas:

[1] IBM. IBM Security Services 2014 Cyber Security Intelligence Index. Disponible en <http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf>, acceso en 25 oct 2015

[2] CROSS, Michael. *In Scene of the Cybercrime Edition: Second Edition*. Elsevier, 2008: Ipswich, Estados Unidos, p. 555-596.

[3] SYMANTEC. *Internet Security Threat Report vol. 20.* Disponible en https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf, acceso en 25 oct 2015, p. 94

[4] SYMANTEC, op. cit., p. 71.

[5] Ídem, p. 76.

¿CÓMO BLINDAR CONTRATO DE ERP Y EVITAR DOLORES DE CABEZA?

Sandra Paula Tomazi Weber

Es esencial tener un *contrato bien hecho*, para mitigar riesgos y preservar la relación entre las partes. Principalmente cuando estamos hablando de un contrato de prestación de servicios de implantación de sistema.

Una de las implementaciones más críticas es la ERP (*Enterprise Resource Planning)*, un conjunto de software interrelacionados que proporcionan el gerenciamiento completo de la empresa, interconectando varios departamentos, como finanzas, recursos humanos, logística, compras, ventas y producción, entre otros.

Estamos hablando de una prestación de servicios que impacta a todo el negocio e involucra a todas las áreas, dada al desempeño del sistema. Por consiguiente, pasar por un proceso de implementación de ERP por sí solo no es nada fácil, todavía más si viene acompañado de algunas de las siguientes situaciones:

a) Implementación atrasada, con el cronograma siendo revisado varias veces y pareciendo que nunca evoluciona;
b) Falta de usuarios clave;
c) La frecuente substitución de consultores, perdiéndose todo el historial;
d) El pago previsto por el servicio ya fue realizado y el sistema no entró en producción;
e) El layout no se adecua al proceso de la empresa porque en realidad es necesario personalizarlo;
f) Uno o dos módulos están implementados, pero no sirve de nada ya que es necesario tener el todo.

Esos son sólo algunos de los percances que surgen a lo largo del camino. Entonces, ¿qué hacer? Es importante que TI y el departamento jurídico estén bien alineados para blindar esa minuta. Firmar un contrato es esencial, pues la regla del juego ¡debe estar en el juego!

Primer Consejo:

¡Debemos tener mucho cuidado con las propuestas que tratan de cuestiones contractuales!

Segundo Consejo:

> Art. 427 del CC: La propuesta de contrato obliga al proponente, si lo contrario no resulta de sus términos, de la naturaleza del negocio, o de las circunstancias del caso.

El Jurídico tiene que estar implicado desde el comienzo, incluso desde la fase de la propuesta, de ser posible, y definitivamente antes del "De Acuerdo". Eso permite que el abogado ya identifique si en el documento hay tentativas que van más allá de las cuestiones de negocio, como precio, plazo, entre otros

Tercer Consejo:

¡Haga las consideraciones iniciales! Deje claro desde el inicio del contrato, por medio de "Consideraciones", cuál es la intención de las partes con aquella contratación. Tal práctica es relevante, ya que ante una discusión judicial, puede auxiliar al Juez a entender cuál era la INTENCIÓN de las partes en el momento de la

contratación y así auxiliarlo a encontrar la mejor solución para el caso

Cuarto Consejo:

Tenga un ¡GLOSARIO! Defina el entendimiento que se debe tener sobre los términos que puedan generar diversas interpretaciones, como, por ejemplo, manutención correctiva, manutención preventiva, personalización, error en el sistema, etc.

Quinto Consejo:

¡Describa de forma clara y objetiva el servicio contratado! Si la propuesta comercial no está clara, esta es la oportunidad de intentar atenuar el riesgo. Ponga por escrito lo pactado para evitar discusiones sobre lo que de hecho está en la mira.
Aproveche este momento para redactar una cláusula donde quede establecido que la implementación del sistema sólo será considerada concluida, válida y efectiva después de la realización de todos las pruebas y la posterior homologación por el contratante de todos los módulos objeto de contratación.

No siempre una implementación parcial responde a las necesidades de la empresa, deje eso claro, desde el inicio. ¡Lo que está siendo contratado es un sistema, no módulos! No siempre eso está claro, y el poder judicial acaba teniendo que decidir lo que hace que el proceso se extienda todavía más y tenga una dependencia mayor del resultado de la pericia técnica.

Sexto Consejo:

Jurisprudencia:

APELACIÓN CIVIL – CONTRATO DE IMPLANTACIÓN DE SOFTWARE Y SERVICIOS – INCUMPLIMIENTO PARCIAL POR PARTE DE LA CONTRATADA – RESCISIÓN A PEDIDO DE LA CONTRATANTE – RESTITUCIÓN DE LOS VALORES PAGADOS – DERECHO RECONOCIDO SÓLO CON RELACIÓN A LOS MÓDULOS EFECTIVAMENTE ADQUIRIDOS Y NO IMPLANTADOS – CÁLCULO DE LA CUANTÍA POR ARBITRIO – DAÑOS MATERIALES CON LA CONTRATACIÓN DE OTRA EMPRESA – DERECHO NO RECONOCIDO – HONORARIOS LEGALES - DISTRIBUCIÓN PROPORCIONAL A LA PÉRDIDA EXPERIMENTADA POR CADA PARTE. (TJMG, Ap. 1.0024.07.804216-5/001, Rel. Arnaldo Maciel, j. 19.03.2013).

Jurisprudencia:

Caso: Prestación de servicios de suministro e implementación de Software. Rescisión del contrato. Restitución e Indemnización. Acción procedente. R$ 180.000,00.

"Valiéndose del ejemplo de una empresa contratada para el desarrollo de un carro personalizado que, después del plazo acordado, no concluye ninguno de los módulos necesarios para el funcionamiento del vehículo, ocasionando la ineficacia del trabajo inconcluso a una hipotética tercera empresa contratada para la finalización del proyecto." (TJSP, Ap. 9134212 – 58- 2007. 8.26.0000, Rel. Lino Machado, j. 29.02.2012).

En una implementación del sistema es esencial la colaboración entre las partes y la implicación de ambas en la ejecución del trabajo. Esto ocurre porque la contratada tiene el *know how* sobre la metodología de la implementación, pero la contratante tiene la experiencia y el conocimiento de las rutinas del negocio. De ahí la necesidad de la figura del usuario clave, que además de replicar lo que aprendió sobre el funcionamiento del sistema es también quien apoya en los detalles del proceso, en la fase de pruebas y en la homologación.

A continuación, presentamos un caso donde el sistema por sí mismo no respondía a las necesidades de la contratante, siendo necesario realizar personalizaciones. Sin embargo, estas no se realizaron y la contratada alegó que eso era de responsabilidad de la contratante, que debería hacer el gerenciamiento del proyecto como fue firmado en el contrato. Sucede que en el contrato esta actividad estaba sin descripción. ¿Cómo gerenciar algo que no se conoce? Para el juez de este caso el gerenciamiento debería consistir solo en la entrega de las informaciones de la contratante a la contratada, ya que esta no tiene el conocimiento para realizar dicha personalización.

Caso: Prestación de servicios y licencia de software. La rea alega que las personalizaciones no fueron realizadas por culpa de la autora. Hecho no demostrado. Acción de rescisión contractual PROCEDENTE. Devolución de valores R$101.632,08.

(TJSP, Ap. 9204111-17.2005.8.26.0000, Rel. Cláudio Godoy, j. 14.02.2012).

Por tanto, ¡detalle las actividades y las responsabilidades en el contrato! Eso evita discusiones sobre quién debe hacer qué y en qué momento.

Puede ser definido en la propuesta, en el Anexo Contractual, en el cronograma o en el propio contrato.

Séptimo Consejo:

En un contrato de implantación de sistema es indispensable que el pago esté vinculado a entregas o actividades. Eso evita que el contratante finalice de realizar el pago antes de recibir lo que fue contratado. Cuando eso ocurre el contratante pierde su poder de negociar, su fuerza de presión para que el servicio ocurra y acaba siendo el último de la fila. No son raras las renegociaciones de plazo. Incluso cuando no hay un cronograma de trabajo ya montado es posible vincular el pago a las actividades, pues toda implementación posee una metodología de trabajo con fases definidas. Se recomienda, además, que cada etapa o actividad sea homologada por la contratante.

¡El siguiente es un caso en el cual esta vinculación marcó la diferencia completamente! La contratada entregó el trabajo, pero con ajustes pendientes, errores en el sistema que necesitaban ser arreglados. Tales correcciones llevaron dos años. Como el pago estaba vinculado a la implementación debidamente homologada, no le correspondía a la contratada recibirlo antes. Motivo por el cual perdió la acción de cobro.

Caso: Alquiler de Software. Cobro de Pago. Acción Improcedente.

La autoría alega que la implementación ocurrió el 02.02.1998 y que, aunque la arrendataria haya señalado algunos puntos pendientes para la perfecta utilización del software, habría utilizado la herramienta sin ningún pago, desde 1998 al 2000, cuando fueron concluidos los pendientes y ajustes existentes sobre el Software.

El juez juzgó anticipadamente el mérito, pues en el contrato estaba claramente descrito *que el pago por el alquiler, manutención y soporte técnico sólo sería exigido después de 182 (ciento ochenta y dos días) contados desde la fecha de implementación y aceptación del software.* No hay necesidad de producción de pruebas. (TJSC, Apelación Civil) 2007.040589-2, rel. Des. Ronei Danielli, j. 24.05.11).

Octavo Consejo:

¡Es importante poner por escrito el cronograma de los trabajos! Tener un plazo es esencial para verificar eventuales atrasos ya durante la ejecución (aunque sean etapas intermedias), así como para caracterizar un incumplimiento contractual en caso de que este no sea cumplido.

La mayoría de los casos que llevan a la rescisión de los contratos de prestación de servicios de implementación de ERP es debido al no cumplimiento del plazo establecido para la conclusión de los trabajos.

Caso: Acción de indemnización, buscando la autora la restitución – de los valores por ella desembolsados con motivo de la no implementación del sistema en los términos contratados. Sentencia de procedencia de la acción. Recurso inadmisible.

La rea se comprometió, mediante contrato escrito, a prestar servicios de consultoría para la implementación del' software conocido como [...] para agilizar procesos operacionales de gestión, finanzas, – contraloría, materiales, almacenes, ventas y distribución, transportes, actividades de paquete de servicios y manutención en la empresa dirigida al transporte de cargas. Así, *pasado el plazo contractual sin que el sistema haya entrado en operación efectiva, habiendo, además, subsidios que indican el abandono del servicio por la rea, debe ella indemnizar a la autora por perjuicios sufridos.* (TJ/SP, Apelación 992.07.026280-1, Rel Des. Kioitsi. Chicuta, j. 28.01.2010).

Es posible también en el contrato vincular eventuales multas por incumplimiento del plazo, dando un límite máximo, bajo pena de anulación de contrato.

Noveno Consejo:

¡Incluir la obligación de Confidencialidad! Esta debe estar presente en la propuesta comercial, en el contrato e incluso en el documento anterior, pues a veces para elaborar la propuesta ya se hace necesario proveer informaciones sobre el negocio.

Décimo Consejo:

También necesitamos estar preparados por un cambio de proveedor en caso necesario. Para ello es recomendado incluir una cláusula de Reenvío de las informaciones y documentación. La Contratada correrá con los costos de ese reenvío ante anulación o rescisión contractual por su culpa.

Décimo Primer Consejo:

La personalización es un tema delicado en la mayoría de las implementaciones de sistema. Esto se debe a que muchos atrasos en la conclusión del proyecto o gastos excedentes se derivan de las personalizaciones no previstas y que solo fueron identificados a lo largo de la ejecución de los trabajos. Un consejo para intentar por lo menos atenuar esos gastos es intentar compartir con el desarrollador el costo. ¿Cómo es eso? Muchas personalizaciones son hechas para un cliente y después incorporadas como mejorías al sistema beneficiando a otros. Incluya una cláusula en el contrato para tratar previamente sobre los siguientes tipos, así como sobre el precio:

- Desarrollos hechos exclusivamente para la CONTRATANTE;
- Desarrollos que serán incorporados a la plataforma, hechos mediante solicitud del CONTRATANTE;
- Desarrollos que serán incorporados a la plataforma, que no fueron realizados mediante solicitud del CONTRATANTE.

Décimo Segundo Consejo:

Es importante redactar una clausula sobre la propiedad intelectual principalmente en los casos que involucren código de fuente, tales como servicios de desarrollo, personalización o mejoría de softwares.

Los derechos autorales sobre los desarrollos de software contratados bajo encomienda serán del contratante, salvo disposición contraria entre las partes (Ley 9.609/1998, art. 4.º).

Cuando por una cuestión de costo o incluso de estrategia de mercado la contratante cede la propiedad de lo que fue desarrollado para que sea comercializado por la contratada en el mercado, pero quiere una garantía de que podrá a lo largo del tiempo usufructuar y tener una continuidad de lo que fue contratado, aunque la contratada desista de ese mercado, ella podrá recurrir a la cláusula de *escrow*, que no es más que el depósito del código de fuente y de su documentación técnica a un tercero de buena fe.

Décimo Tercer Consejo:

Algunos contratos de implementación de sistema terminan también en trabajo de Manutención. Cuando esto suceda no olvide de especificar claramente cuál es el tipo de manutención contemplada. Ejemplo: correctiva, adaptativa (que incluye actualización en adecuación a la legislación) y evolutiva.

Alerta: Al tratarse de manutención programada, dependiendo del ramo de actividad de la empresa, no basta un plazo de 24 horas, es importante que estas nunca ocurran cerca de determinadas fechas, como, por ejemplo, cierre de mes, fechas conmemorativas (cuando el ramo es comercio minorista), entre otras.

Establezca, además, un acuerdo de nivel de servicio (conocido también como ANS o SLA), para dejar claro el tiempo de respuesta y resolución ante una llamada en curso al soporte. Además de los plazos de atención, es importante que conste también las cláusulas penales y en qué situación será posible una rescisión motivada.

Décimo Cuarto Consejo:

El prestador del servicio necesita conocer y actuar de acuerdo con la Política de Seguridad de la Información de la contratante. El tratamiento de las informaciones y de los datos compartidos entre las partes debe seguir la referida política, así como la norma de clasificación de la información y demás normativas aplicadas. Por tanto, es necesario incluir una cláusula sobre Seguridad de la Información.

Décimo Quinto Consejo:

Genere una documentación de todo lo que fue re-pactado a lo largo del período de implementación, ya sea por e-mail, acta de reunión o adenda contractual. Principalmente temas relacionados al plazo, al cronograma, actividades ejecutadas por cada parte o personalización, pues son los puntos más discutidos en acciones judiciales que tratan sobre rescisión contractual o indemnización como consecuencia de la implementación del sistema

El contrato de prestación de servicios de implementación de ERP debe ser como un prospecto de medicamento, o sea, debe reflejar las expectativas de las partes, así como los derechos y obligaciones, ¡además de contemplar el mayor número de situaciones posibles! Un contrato bien escrito aporta celeridad en la resolución de conflicto y muchas veces evita que las partes recurran al poder judicial.

RECUPERACIÓN DE INGRESOS EN RUPTURA DE SLA

Márcio Mello Chaves

En tiempos de recesión económica y momento político conturbado, la postura de las empresas de recortar gastos es unánime. La revisión de los costos fijos, con el objetivo de reducir cuánto la empresa gasta, normalmente es la primera acción tomada. Sin embargo, pocos practican o siquiera poseen conocimiento de la posibilidad de recuperar parte de los valores desembolsados por el incumplimiento de un SLA

Usualmente, utilizado de forma interdepartamental en la empresa, el *Service-Level Agreement* (SLA) o Acuerdo de Nivel de Servicio – ANS también puede ser parte integrante de un contrato de prestación de servicios, por el cual son establecidos los parámetros empleados para medir los servicios, y las consecuencias / penalidades en caso de que no sean cumplidos.

El SLA tiene como finalidad cuidar por la debida prestación de los servicios contratados dentro de la expectativa de las partes, o la debida reparación en caso de incumplimiento. A pesar de ser utilizado usualmente para servicios de Telecomunicaciones, suministro de energía, atención y soporte, principalmente en *call centers*, puede ser aplicado en los más diversos tipos de servicios, principalmente cuando la deficiencia en la prestación de los servicios impone riesgos para el contratante.

En este aspecto, varios serían los riesgos previsibles que podrían ocasionar la utilización de SLA: desempeño, cuando el bien/servicio no alcanza los niveles contratados; tiempo de respuesta al llamado, cuando el soporte no atiende según lo previsto; interrupción, cuando haya

pérdidas relacionadas a la interrupción/restablecimiento del servicio; calidad, cuando el proyecto no cumpla determinado nivel; plazo, cuando la implementación o prestación no ocurra hasta una determinada fecha fatal que perjudique un lanzamiento o fecha prevista; entre otros.

Con el objetivo de evitar o mitigar esos riesgos, dos ítems se vuelven esenciales en un SLA: (i) los indicadores a ser seguidos en la medición del suministro de los servicios contratados y (ii) las penalidades objetivas de acuerdo con cada incumplimiento, parcial o total. Además, la posibilidad de compensación de las penalidades con el pago de los servicios o de la aplicación de un plan de contingencia en caso de imposibilidad del suministro se hacen fundamentales para facilitar su aplicación.

A pesar de poder ser utilizados los más variados indicadores, además de la disponibilidad del servicio, merecen relevancia: Average Speed to Answer – ASA, o tiempo medio de respuesta; Time Service Factor – TSF, o porcentaje promedio de tiempo del servicio; First-Call Resolution – FCR, o porcentaje de resolución en la primera llamada; Turn-Around Time – TAT, o tiempo para concluir determinada tarea y Mean Time To Recover – MTTR, o tiempo de restablecimiento después de falla en el servicio

Las penalidades, por su parte, van desde multas simples, como un 3% del valor del contrato; multas proporcionales, como del 2% en el caso de disponibilidad mayor o igual a 97% e inferior al 98% y del 3% en el caso de disponibilidad mayor o igual al 96% e inferior al 97%; la contratación de terceros para suplir la carencia derivada del incumplimiento, entre otros. Obviamente, en caso de falla total por el contratado, las penalidades deben prever también la rescisión motivada con sustitución del prestador de servicio e indemnización por las pérdidas y daños sufridos por el contratante.

Definidos los parámetros del SLA y firmado el contrato, el procedimiento de recuperación de ingresos pasa al monitoreo y la documentación de su ejecución. Estos procedimientos comprenden desde el registro de las comprobaciones de atención de los indicadores establecidos, hasta la preservación de las comunicaciones realizadas entre las partes, principalmente por medio de la formalización cuando se identifica el incumplimiento.

La preservación implica todas las pruebas generada a lo largo de la ejecución del contrato, tales como e-mail, mensajes instantáneos (SMS, WhatsApp), logs de acceso a sistemas, prints de pantallas (incluso con la elaboración de Actas Notariales) y control de inventario. La formalización del incumplimiento, por su parte, implica la comunicación formal de la violación de los parámetros definidos con el objetivo de computar las penalidades previstas, por medio de e-mails y Notificaciones Extrajudiciales, dejando clara la identificación del incumplimiento.

Por tratarse de una parte integrante de un contrato, la recuperación de ingresos por ruptura de SLA supone, además de la definición del nivel de importancia para el servicio, la negociación con las áreas comerciales, redacción detallada de los indicadores y penalidades, así como el seguimiento y el registro de las incidencias durante la ejecución de las actividades contratadas.

Todo ese seguimiento de la fase de discusión, entrega, control de calidad y eventual fase de salida y transición del prestador debe ser, por tanto, hecho por un gestor de contrato que, practicando todas esas recomendaciones, cuidará para que haya la debida recuperación para el contratante.

Por último, mucho más allá del incumplimiento total comúnmente tratado, que resulta en el término de la relación contractual con eventual aplicación de multa, la recuperación de ingresos en ruptura de SLA posee una diferenciación. Esta diferenciación consiste en la posibilidad de mantener la relación entre el contratante y el contratado, aun en caso de que la discusión respecto a la ruptura sea llevada a la justicia. Así, la recuperación de ingresos por ruptura de SLA tiene el objetivo de restablecer el equilibrio contractual afectado cuando la prestación de servicios es fallida, ocasionando, por tanto, la aplicación de la penalidad prevista en el contrato.

Las empresas deben actuar preventivamente en la implantación de estos procedimientos para permitir su aplicación en futuras contrataciones. Reactivamente, la acción es también estratégica, pues diversos pueden ser los contratos que posean potencial de recuperación de valores para la empresa, cuantía que puede marcar la diferencia en la superación durante momentos económicos difíciles.

LA UTILIZACIÓN DE LA FIRMA ELÉCTRONICA BIOMÉTRICA EN LA FORMACIÓN DE LOS CONTRATOS

Sandra Paula Tomazi Weber

Con la llegada de internet y el crecimiento del comercio online, la contratación electrónica se volvió cada más popular, siendo más frecuente la utilización de contratos formados por medio de un “clic en ok”, e-mail, entre otros.

Sin embargo, muchos olvidan que antes de internet ya ocurrían contrataciones inter-sistémicas mediante el EDI, plataforma que hacía posible la realización de transacciones de negocio de forma automatizada,

por medio del intercambio de órdenes de compra y venta generalmente entre empresas, después de una larga fase de negociación y por intermedio de redes cerradas.

Lo que llama la atención es que desde la década del 70 las empresas ya buscaban algún medio para sustituir el modelo tradicional de contratación, esto es, aquel celebrado en papel, por otro más eficiente y económico.

Años después volvemos al mismo punto, a saber, la discusión de la sustitución del papel, sin embargo, incrementada en otras motivaciones, como, por ejemplo, mitigar la deterioración y pérdida de documentos únicos, principalmente como consecuencia de desastres naturales; la necesidad de localizar con mayor facilidad los documentos, que generalmente están almacenados en grandes volúmenes; garantizar un mayor nivel de seguridad y confidencialidad, al restringir el acceso a las informaciones.

Es en este escenario que pasamos a encontrar en el mercado soluciones de contratación electrónica, no sólo para promover la contratación realizada como resultado de las relaciones que se forman mediante internet, sino también entre persona y sistema dentro de un ambiente de red cerrada.

En Brasil las bases para decidir el modelo de contratación electrónica deben pasar por el análisis de los siguientes puntos:

- A pesar del Código Civil no haber previsto de forma expresa los contratos electrónicos, lo hizo indirectamente cuando: a) dispuso sobre la libertad de forma en las contrataciones no solemnes; b) consideró como contratación entre presentes la realizada por teléfono y otros medios semejantes; c) substituyó

la noción de contratos por correspondencia epistolar, prevista en el Código Civil de 1916, por la de contrato entre ausentes.

- El contrato electrónico no es otra cosa que el contrato en su concepto clásico, sin embargo, formado a través del medio electrónico.
- El contrato electrónico, para tener validez, requiere desde el inicio que sean observados los requisitos previstos en el artículo 104 del Código Civil, tales como las capacidades de las partes, el objeto lícito y posible, determinado o determinable, el consentimiento y la forma prescrita o no defendida en ley.
- El modelo de contratación electrónica adoptado no puede afectar la eventual formalidad exigida en ley, bajo pena de ser considerado un acto jurídico inválido[61].
- Las partes, en caso de formación de un contrato electrónico, pueden o no estar presentes. La identificación de la parte, y consecuentemente la comprobación de si esta goza o no de capacidad para contratar, siempre fue una preocupación en cualquier modalidad contractual (física o electrónica). Incluso porque los fraudes crecen cada día más, mientras que también aumenta la dificultad en evitarlos, aún en caso de contratos firmados en papel con firma autógrafa; sea porque muchas personas no mantienen su documento de identidad actualizado (lo que dificulta verificar por la foto si la persona es aquella que dice ser o hacer la comparación entre las firmas) o incluso

---

[61] ACCIÓN CAUTELAR DE EXHIBICIÓN DE DOCUMENTO. CONTRATO ELECTRÓNICO. **INEXISTENCIA DE FORMA ESPECIAL**. IMPOSIBILIDAD JURÍDICA DEL PEDIDO. Tratándose de contrato electrónico interpersonal, en el cual las partes interactúan en la manifestación de sus voluntades, para la formación de su proprio vínculo, independientemente de la forma especial, no hay como exigir la presentación del contrato por parte de la demandada, incluso porque la propia demandante demuestra que los términos del contrato fueron libremente deliberados mediante propuesta y aceptación por medio de correo electrónico. Apelación denegada (TJRS, Apelación Civil Nº 70013028261, Décima Segunda Cámara Civil, Relator: Dálvio Leite Dias Teixeira, Juzgado el 30/03/2006, subrayado nuestro)

porque la mayoría de las veces no se exige el reconocimiento de la firma en notaría. Ante esta situación, recurrir a la tecnología puede ser una manera de mitigar ese riesgo, como, por ejemplo, usando firmas electrónicas o digitales. El riesgo no es mayor porque el contrato haya dejado de ser en papel.

- Actualmente, no hay rigor de forma para los contratos, excepto cuando la ley lo prevé expresamente, pues basta la declaración volitiva para establecer el vínculo obligatorio entre los contratantes.
- Esa libertad de forma encuentra su sostén legal en el artículo 107 del Código Civil que determina: "La validez de la declaración de voluntad no dependerá de forma especial, sino cuando la ley expresamente lo exija"
- En el caso de formalidad prevista, se debe verificar la existencia: a) de veda expresa a la celebración por medio electrónico; b) de formalidades que excluyen la posibilidad de utilización de este medio, o incluso c) de exigencia del uso del certificado ICP-Brasil para firmar el contrato, en caso de que decida celebrarlo en medio electrónico. No podemos olvidar que el documento electrónico posee el mismo estatus legal de documento público o particular, de acuerdo con el artículo 10 de la MP 2200-2 de 2001, que instituye la Infraestructura de Claves Públicas Brasileña – ICP-Brasil.
- Los contratos se forman en el momento en que es aceptada la propuesta, también conocida por oferta o policitación. Por consiguiente, la manifestación de voluntad de las partes constituye el punto fundamental en la formación de los contratos. El derecho brasileño no posee ningún precepto que

prohíba la declaración de la voluntad transmitida por medios digitales, lo importante es el recibimiento y entendimiento por el destinatario de la declaración de voluntad. No es relevante la forma cómo se exterioriza o el medio utilizado para la comunicación de la voluntad, salvo los casos en que la ley prevé una forma específica. Según el artículo 112 del Código Civil: "En las declaraciones de voluntad se atenderá más a la intención en ellas corporificada que en el sentido literal del lenguaje"

- Por la legislación brasileña en vigor, el contrato se considera celebrado en el lugar en que fue propuesto (artículo 435 del Código Civil), independientemente del contrato ser celebrado entre ausentes o presentes.
- Tratándose de una contratación internacional, la obligación resultante del contrato se considera constituida en el lugar en que reside quien lo propone, a tenor del artículo 9º y § 2º de la Ley de Introducción a las normas del Derecho Brasileño. Hay quien invoque la autonomía de la voluntad, así como los artículos 62 y 63 del Código de Proceso Civil y el compendio 335 del Tribunal Supremo Federal para utilizar la cláusula de elección del foro. Está, además, quien no entiende que, si la relación es de consumo, debe prevalecer el foro del consumidor, pues el Código de Defensa del Consumidor es una nueva de orden público. El anteproyecto para la modificación del Código de Defensa del Consumidor resuelve eso al cambiar el artículo 101 determinando que es nula la cláusula de elección del foro y será competente el foro del domicilio del consumidor, en las demandas en que el consumidor residente en Brasil sea reo y el consumidor, cuando sea autor de la demanda, podrá escoger

el foro de su domicilio, del domicilio del proveedor o aun donde fue celebrado o ejecutado el contrato.

- El contrato siendo electrónico pasa a tener como original el documento electrónico, siendo el impreso solo una copia.
- Es en el documento electrónico que se instrumentaliza el contrato y ocurre la manifestación de las partes en contratar.
- En Brasil fue instituida la Infraestructura de Claves Públicas Brasileña – ICP-Brasil, para garantizar la autenticidad, la integralidad y la validez jurídica de documentos en forma electrónica.
- El fundamento para la validez de un documento electrónico comienza por el hecho de que el documento original no está intrínsecamente relacionado a la idea de un documento en papel, sino directamente asociado a su capacidad de pericia y de comprobación de manifestación de voluntad de las partes, esto es, de la prueba de autoría e integridad del documento, sea físico o electrónico.
- La integridad del documento está relacionada con la garantía de que el mismo no fue alterado a lo largo del tiempo.
- El requisito de autenticidad tiene relación a la identificación de las partes contratantes.
- Al optar por un modelo de contratación electrónica es esencial observar los requisitos de validez del contrato, como ya fue mencionado, así como adoptar una solución tecnológica que garantice la integridad y la autenticidad del documento.

Y para utilizar la firma electrónica biométrica, ¿qué bases debemos pautarnos?

Al contrario de lo que se piensa, la biometría es una técnica bastante antigua, habiendo registros de su utilización en el Egipto Antiguo, específicamente, por los habitantes del Valle del Nilo, que la empleaban en situaciones de negocio del día a día.

Oficialmente, el primer método biométrico reconocido fue del francés Alphonse Bertillon, a finales del siglo XIX, y consistía en la combinación de medidas físicas colectadas (tales como altura, tamaño, tronco, largo y ancho de la cabeza, de la oreja derecha, del pie izquierdo, del dedo medio izquierdo y también del antebrazo izquierdo) con el color del cabello, de los ojos y una foto de frente y de espaldas. Todo eso era archivado para comparaciones futuras. (PINHEIRO, 2008, p. 40)

El método descrito anteriormente se llamaba antropometría o Bertillonage, adoptado inicialmente por la policía de París en 1882, y después se diseminó por toda Europa y por Estados Unidos. Aunque, considerando principalmente la cantidad de medidas a ser recolectadas, ese método fue sustituido a finales del siglo XIX por el sistema de impresiones digitales desarrollado por el británico William James Herschel (1833 – 1917) (PINHEIRO, 2008, p. 40-41)

Canedo (2002) explica que el uso moderno de la biometría tuvo sus inicios en 1858, cuando Herschel pasó a recolectar impresiones digitales en el reverso de los contratos. Él se encontraba con dificultades en lograr que las personas cumpliesen los acuerdos comerciales y pasó a utilizar esta técnica como medio de prueba de lo que fue acordado entre las partes.

De acuerdo con Pinheiro (2008, p. 42), la primera clasificación de los tipos de impresiones digitales fue hecha por el inglés Francis Galton en 1892, y todavía es utilizada hasta hoy. Para el referido autor, las impresiones digitales son el identificador más usado en la interpretación de una

evidencia física para propósitos legales, o sea, en el campo de la identificación forense.

Sin embargo, no podemos olvidar que los sistemas biométricos están en constante proceso de desarrollo y diversos otros tipos, además de la impresión digital, ya están siendo utilizados.

La prueba de ADN[62] es una forma de autenticación biométrica ya bien aceptada por el poder judicial, a pesar de no ser 100% segura.

En Brasil verificamos la utilización de la biometría también en el proceso de obtención de pasaportes; para tener acceso a áreas restringidas de un ambiente físico o electrónico; para identificar un elector; para la confirmación de presencia en cursos, entre otros.

Podemos definirla como una ciencia que permite, por medio de la recolección de las características biológicas del individuo, identificarlo en el momento de la manifestación de la voluntad de contratar, funcionando

---

[62] "PROCESO CIVIL. PRUEBAS. CERCENAMIENTO. En la acción de investigación de paternidad, el autor tiene el derecho a la realización de la prueba técnica que corresponda a los mayores avances de la ciencia (actualmente, el examen de ADN), así como a la producción de la prueba testimonial oportunamente requerida – aunque el resultado del análisis hematológico llevado a efecto recomiende la improcedencia del pedido; el juicio anticipado de la lid sin que la instrucción sea la más amplia posible cercena indebidamente la actividad probatoria del autor. Recurso especial conocido y aceptado (STJ, Resp. 790750/SP, relator Ministro Ari Pargendler, Tercer Grupo, juzgado el 16/05/2006).
"INVESTIGACIÓN DE PATERNIDAD. PRUEBA. ANÁLISIS DE ADN. RECUSA DEL REO. 1. La recusa sin motivos del investigado a someterse al análisis de ADN constituye un elemento de prueba seguro para abrigar la convicción sobre la paternidad. 2. El comportamiento procesal desarrollado por la parte es, en sí mismo, un valioso elemento de prueba, revelando que el reo deliberadamente abdicó su derecho de revelar la verdad biológica, quedando claro que así procedió por saberla contraria a sus intereses. Incidencia del art. 231 del CCB. 3. Si el reo se recusó a someterse al análisis de ADN, sabiendo que este sería la única prueba capaz de dilucidar hechos es imperiosa la procedencia de la acción, con la aplicación de la presunción de la paternidad de que trata el Compendio 301 del STJ. 4. Es litigante de mala fe quien se recusa a producir la prueba pericial, que era imprescindible para comprobar sus alegaciones, volviendo débil al cuadro probatorio, y viene a alegar, en sede del recurso, la fragilidad del cuadro probatorio. Recurso infundado". (TJRS, Apelación Civil: AC 70047163761 RS, Relator Sérgio Fernando de Vasconcellos Chaves, juzgado el 13/06/2012)

literalmente como una forma de tener seguridad que aquella persona es quien dice ser, o sea una autenticación biométrica.

El sistema de biometría puede estar basado en técnicas fisiológicas o comportamentales, y dependiendo del nivel de seguridad que se quiere tener, puede optarse por usar más de un elemento. Los principales elementos biométricos son: Reconocimiento Facial, Geometría de la Mano, Identificación del Iris, Reconocimiento de la Retina, Reconocimiento de Voz, Impresión Digital y Reconocimiento de la Firma Manuscrita.

La firma manuscrita o autógrafa es un método de identificación biométrica por características comportamentales (considerando características únicas del trazo, presión, velocidad). La diferencia respecto al método al que estábamos acostumbrados es que ahora es recolectada en un dispositivo electrónico, habiendo en el mercado soluciones que hacen ese procedimiento a través de un tablet.

Por tanto, no estamos inventando nada nuevo. Al contrario, estamos utilizando la biometría, uno de los métodos más antiguos de la identificación de personas, y que asociándole recursos tecnológicos con el fin de brindar mayor seguridad a la contratación electrónica.

A lo largo del tiempo, en Brasil, aprendimos a utilizar la firma digital con el certificado ICP-Brasil, incluso porque esta pasó a ser exigida por diversos órganos para la realización de ciertos actos. La Secretaría de la Agencia Tributaria Federal brasileña, por ejemplo, desde 2010 hizo obligatorio el uso de la firma digital con certificado ICP para la transmisión de declaraciones y demostrativos de las empresas tributadas en base al lucro real, al lucro presumido o al lucro arbitrado.

Pero no podemos olvidar que en Brasil la MP 2200-2 de 2001 permite a las partes, por medio de acuerdo entre ellas, escoger la utilización de otro

medio de comprobación de la autoría y de la integridad de documentos en forma electrónica, mediante el §2º del artículo 10. Lo que va al encuentro de los principios de la autonomía de la voluntad, de la libertad de forma, del *pacta sunt servanda* y de la buena fe.

Los autores Therrien y Tronco se cuestionan si el reconocimiento biométrico es suficiente para firmar un documento y hacerlo válido ante el derecho, pues para ellos esta técnica conlleva una inseguridad sobre lo que se está firmando, comprometiéndose así la manifestación de la voluntad, además de también no asegurar la integridad del documento.

Estamos en desacuerdo con el referido autor, pues entendemos que el uso de la biometría aporta mucha seguridad jurídica a las relaciones contractuales.

Primeramente, porque es una forma de identificación prácticamente incuestionable, pues se realiza por medio de las características físicas y comportamentales únicas de una persona. Como vimos, el certificado digital puede ser prestado, mientras que las características biométricas no. Por consiguiente, aun el certificado teniendo toda la tecnología de la encriptación asimétrica, no brinda la seguridad de que la persona sea quien dice ser.

En segundo lugar, tenemos que entender que es posible crear una solución que integre la biometría de conjunto con otros mecanismos que puedan dar garantía de la integridad y de que la manifestación de voluntad ocurrió sobre el documento. Esta ya era una de las visiones de Miguel Pupo Correia sobre el tema.

El *timestamp* (también conocido como cuño de tiempo), por ejemplo, sirve como evidencia de que la información digital existía en una determinada fecha y hora. Sería una alternativa para apoyar en la comprobación de integridad. Otra opción sería el registro del contenido

de la minuta contractual en una Notaría de Títulos y Documentos. La pregunta que también tenemos que hacernos es ¿cuál es la garantía que tenemos hoy de la integridad de un documento de papel? ¿Hay una rúbrica? ¿Cuál es la seguridad que esta nos brinda? Podemos utilizar el recurso de la pericia tanto en un documento físico como electrónico.

El hecho es que por una cuestión cultural todavía somos una sociedad muy apegada al papel y acabamos por poner varios obstáculos para la contratación electrónica, dando la impresión de que esta es menos segura. Sin embargo, esa creencia no es verdadera, ya que según la tecnología escogida se consigue aumentar el grado de seguridad.

También es posible adoptar modelos de contratación electrónica donde cada una de las partes haga uso de la firma electrónica biométrica y otra utilice el certificado ICP-Brasil, con el fin de aprovechar de aquella la seguridad de que el contratante es quien dice ser, y del otro lado el mecanismo de la encriptación asimétrica para garantizar la integridad del documento.

Para contrataciones en masa, el uso de la firma biométrica para ambas partes o en un modelo híbrido como anteriormente demostrado, además de proporcionar mayor seguridad en la identificación del individuo, es económicamente más viable. Esto se debe a que el contratante asume integralmente el costo de la solución biométrica, y los equipos adquiridos pueden ser utilizados varias veces. En el caso del certificado ICP-Brasil, correspondería al contratante adquirirlo, ya que no tendría sentido que el contratado corriese con ese costo.

En el derecho portugués, a pesar de la preferencia por el certificado digital, el legislador no excluye otras técnicas, estableciendo varias modalidades de firma electrónica, entre ellas la biometría. Y a cada una de ellas se le confiere un valor probatorio. La firma electrónica calificada

es legalmente equivalente a la firma autógrafa en papel, y cuando es certificada por una autoridad acreditada, equivale a una firma reconocida. Hay también quien defiende que la firma biométrica, cuando corresponde al mecanismo de firma manual en un tablet, asociada a la encriptación y a *Hash* destinados a garantizar la integridad del contenido, es una firma electrónica calificada. En otras situaciones ella se tiene como avanzada. Lo que indica al juez que la firma electrónica biométrica posee un grado de confianza más alto. (PADRÃO, 2012, p. 46 - 59)

El derecho colombiano, por su parte, se basa en el principio de la equivalencia funcional y equipara la firma electrónica y la firma manuscrita cuando aquella: a) Permite identificar el autor de la acción del documento electrónico; b) Permite atestar que el contenido refleja la manifestación del autor, que él de hecho estuvo de acuerdo con lo que está escrito; c) Es confiable y apropiada para el acto al cual se le destinó.[63]

Para el legislador colombiano, la firma electrónica biométrica puede ser equiparada a una firma manuscrita en papel, pues en principio atiende los requisitos del artículo 7º. Sin embargo, para confirmar este entendimiento, será siempre importante analizar en la práctica la tecnología biométrica adoptada.

Ante lo expuesto, podemos concluir que es posible firmar contratos utilizando la firma biométrica como forma de manifestación de voluntad de las partes.

También podemos concluir que la biometría puede ser encuadrada en el párrafo 2º del artículo 10 de la MP 2200-2 de 2001, basta asociarla con algún mecanismo que garantice la integridad del documento.

---

[63] Artículo 7 º, de la Ley 527/1999: "Firma. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:
a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;
b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.
Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma."

En Brasil, no hay ley específica sobre biometría, sin embargo, ella está relacionada directamente a los conceptos de intimidad, privacidad e imagen del individuo. Para que la recolección del dato biométrico no hiera tales derechos, se recomienda la autorización previa del individuo propietario de las características captadas, informando por medio de un término cuál será la condición del uso, la forma de almacenamiento de esta y el período de conservación. Así concluimos la tercera hipótesis planteada.

El tema abordado supone en especial una ruptura de paradigmas, pues su utilización va más allá de sus bases legales o de instrumentos técnicos para hacerla viable – que incluso ya constatamos que es posible -, y está relacionado a una práctica cultural. Muchas personas confunden la relación contractual con el instrumento "contrato", en papel. El contrato puede ser verbal, en papel o en un documento electrónico. Como ya fue dicho, no estamos creando nuevas amenazas, pues el riesgo de fraude en la firma o de alteración de contenido existe hace tiempo. La propuesta es demostrar que existen otros modelos, y que, dependiendo de la tecnología empleada, pueden ser hasta más seguros. Creemos que la biometría es una de ellas.

REFERENCIAS BIBLIOGRÁFICAS:

BARBAGALO, Erica Brandini. **Contratos eletrônicos:** contratos formados por meio de redes de computadores: peculiaridades jurídicas da formação do vínculo. São Paulo: Saraiva, 2001.

BRASIL, Angela Bittencourt. Assinatura digital não é assinatura formal. **Jus Navigandi**, Teresina, año 5, n. 48, 1 dic. 2000. Disponible en:

<http://jus.com.br/revista/texto/1783>. Acceso en: 24/10/2012.

CANEDO, José Alberto. **Conceitos sobre biometria**. Fórum Biometria (a). Nov, 2002. http://www.forumbiometria.com/fundamentos-de-biometria/62-definicao-de-biometria.html. Acceso en 19 ago. 2012.

CAVALCANTE, Adalberto Luiz Sobral; BACCI, Márcio Demetrio; HOKAMA, Marçal de Lima. **Assinatura de Documentos Digitais através da Biometria no Exército Brasileiro**. Disponible: <www.ensino.eb.br/artigos/artigo_biometria.pdf> Acceso en: 02 nov. 2012.

CORREIA, Miguel Pupo. **Assinatura Electrónica e Certificação Digital**. Disponible en

< http://www.apdi.pt/pdf/Assinatura_elect.pdf >. Acceso en: 24 oct. 2012.

DE LUCCA, Newton. **Aspectos jurídicos da contratação informática e telemática**. São Paulo: Saraiva, 2003.

DINIZ, Maria Helena. **Tratado Teórico e Prático dos Contratos**. 4. ed. v1. São Paulo: Saraiva, 2002.

DOTTI, René Ariel. **Proteção da Vida Privada e Liberdade de Informação**. São Paulo: RT. 1980.

DURVAL, Hermano. **Direito à imagem**. São Paulo. Editora Saraiva. 1988.

GARCIA, Iberê Anselmo. **A Segurança na Identificação: a Biometria da Íris e da Retina**. Tutor: Prof.º Dr. Irene Batista Muakad. São Paulo: USP, 2008. Disertación (Departamento de Derecho Penal, Medicina Forense y Criminología)

JIMENE, Camilla do Vale. **O valor probatório do documento eletrônico**. São Paulo: Sicorezza Editora, 2010.

KAYSER, Pierre. **La protection de la vie privée: protection du secret de la vie privée**. Marseille. Presses Universitaires d' Aux-Marseille, 1984.

KANASHIRO, Marta Mourão. **Biometria no Brasil e o Registro de Identidade Civil**: novos rumos para identificação. Tesis en Sociología. Universidad de São Paulo, São Paulo, 2011.

LAWAND, Jorge José. **Teoria geral dos contratos eletrônicos**. São Paulo: Editora Juarez de Oliveira, 2003.

LEAL, Sheila do Rocio Cercal Santos. **Contratos Eletrônicos: Validade Jurídica dos Contratos via Internet**. São Paulo: Editora Atlas, 2007.

LUCON, Paulo Henrique dos Santos.Competência no comércio eletrônico e no ato ilícito eletrônico. *In*: NEWTON, De Lucca; SIMÃO FILHO, Adalberto (coord.). **Direito & Internet: Aspectos Jurídicos Relevantes**. São Paulo: EDIPRO, 2001. cap. 15, p.351-370.

MARQUES, Antônio Terêncio G. L. **A prova documental na Internet**. Curitiba: Juruá, 2007.

MARTINS, Guilherme Magalhães. **Formação dos contratos eletrônicos de consumo via Internet**. Rio de Janeiro: Forense, 2003.

PADRÃO, Afonso. **Assinaturas Electrónicas, Documentos Electrónicos e Garantias Reais**. Revista do Centro de Estudos de Direito do Ordenamento, do Urbanismo e do Ambiente (RevCEDOUA). 2012, p. 45-81.

PANICHI, Raphael Antonio Garrigoz. Meios de Prova nos Contratos Eletrônicos, realizados por meio da Internet. **Revista de Direito Privado**. São Paulo: Revista dos Tribunais, v.4, n.16, p. 260-272, oct/dic. 2003.

PERÉZ, Marco. **El Tratamiento Legal de la Firma Electrónica en Colombia y en el**

Derecho Uniforme. REVIST@ e – Mercatoria. Vol 1, N.◦ 1. 2002.

PINHEIRO, José Maurício. Biometria nos Sistemas Computacionais Você é a Senha. Rio de Janeiro: Editora Ciência Moderna: 2008.

PINHEIRO, Patricia Peck. **Direito Digital**. 4 ed. São Paulo: Saraiva, 2010.

PINHEIRO, Patricia Peck. **O Direito Digital como Paradigma de uma Nova Era**. In: WOLKMER, Antonio Carlos; LEITE, José Rubens Morato [Org.]. Os "novos" direitos no Brasil. São Paulo: Saraiva, 2012.

RADACK, Shirley. **Biometric technologies: helping to protect information and automated transactions in information technology systems**. NIST, 2005. Disponible en: http://www.itl.nist.gov/lab/bulletns/bltnsep05.htm. Acceso en: 20/10/2012.

RECHSTEINER, Beat Walter. **Direito internacional privado**: teoria e prática. São Paulo: Saraiva, 2004.

SOUZA, Vinicius Roberto Prioli de. **Contratos Eletrônicos & Validade da Assinatura Digital**. Curitiba: Juruá, 2009.

STRINGHER, Ademar. **Aspectos Legais da Documentação em Meios Micrográficos, Digitais e Eletrônicos**. São Paulo: CENADEM, 2003.

THERRIEN, Cristiano; TRONCO, Marlise. **Biometria e Identificação Civil**: aspectos técnicos e questões jurídicas. Fotaleza: Diálogo Jurídico, 2006.

VACCA, John R. **Biometrics Technologies And Verification Systems**. Burlington: Butterworth-Heinemann, 2007.

CAPÍTULO OCTAVO

REPERCUSIONES JURÍDICAS EN LA ERA DIGITAL

NUEVA LEY DE CRÍMENES DIGITALES

Patricia Peck Pinheiro y Victor Auilo Haikal

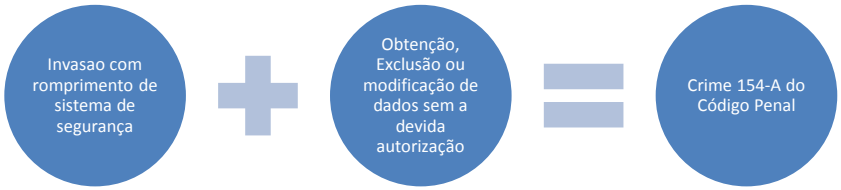
¡Internet ya no es una tierra sin ley! Con la puesta en vigor de las leyes 12.735 y 12.737, ambas del 2012, tenemos la aplicación penal de normas específicas sobre los crímenes digitales propios, aquellos cometidos contra los datos, las informaciones o los sistemas de información, al contrario de los crímenes digitales impropios, donde los sistemas de información sirven solo como medio para practicar el delito.

¿Qué cambia con las nuevas leyes? El principal cambio es que ahora el usuario debe tener más cuidado en proteger sus dispositivos, también hay una mayor capacidad para responsabilización de aquellos que invaden los dispositivos ajenos para apropiarse de datos. Las penas varían, de una detención de tres meses hasta la reclusión de dos años, siendo los agravantes para aumento de la pena el perjuicio económico, la divulgación o filtración de los datos en internet, u obtención de contenido de comunicaciones electrónicas privadas, secretos comerciales o industriales, informaciones confidenciales, o el control remoto no autorizado del dispositivo invadido.

La ley 12.737, ley Carolina Dieckmann, trajo consigo el tipo penal de invasión ilegítima de sistemas de información, amplió el tipo del crimen de inhabilitación de servicio público (art. 266 del Código Penal) y equiparó

la tarjeta magnética a un documento particular, para que la falsificación de tarjetas de débito y crédito, *per si,* sean castigables.

No obstante, el tipo penal de invasión necesita algunas condiciones para que el crimen sea configurado, por la siguiente fórmula:



Invasión con ruptura del sistema de seguridad + Obtención, Supresión o modificación de datos sin la debida autorización = Crimen 154-del Código Penal

Además, recibirá las mismas penas de invasión aquel que instale una vulnerabilidad en un sistema de información para obtener ventaja indebida, por ejemplo, un backdoor o una configuración para que algunas puertas de comunicación a internet queden siempre abiertas.

El usuario de gadgets y dispositivos informáticos comunes están protegidos contra hackers y personas mal intencionadas que abusan de confianza o buscan intencionalmente invadir el dispositivo para perjudicar a su propietario, con la supresión o alteración de datos, para que queden inutilizables, o incluso, apropiarse de datos de la computadora como informaciones íntimas y privadas, como fotos, documentos y videos.

Además, las empresas poseen mayor protección jurídica contra el espionaje digital, pues la obtención de secretos comerciales y/o

informaciones confidenciales definidas por ley, ahora también se encuadran en la ley.

Por su parte, la ley 12.735, Ley Azevedo, que entró en vigor en la misma fecha, poco mantuvo de su proyecto original, restando solamente dos disposiciones jurídicas. La primera indicando que las Policías Judiciales, mediante reglamentación, deberán preparase para el combate de crímenes digitales y que en casos de crimen de discriminación (ley 7.716 de 1989), el Juez podrá solicitar la retirada del contenido discriminatorio no solo de radio, TV o internet, sino de cualquier medio posible.

Sin embargo, se observa que las penas son bajas, permitiendo el encuadramiento de los crímenes como pequeño potencial ofensivo, lo que no se adecua a la protección de los activos intangibles, la piedra angular de la sociedad de la información. Muchas veces una apropiación indebida de datos puede ser más perjudicial que un hurto común, y por eso no debería haber una pena más baja; sobre todo en casos de espionaje que pueden llevar a la competencia desleal.

Esas leyes no agotaron los tipos penales digitales, pues es imposible que no se considere como crimen la indisponibilidad de sistemas de información de entidades privadas, como sitios de comercio electrónico o de bancos, o la diseminación de virus y otros códigos maliciosos, con motivo de que toda la sociedad esté cada vez más interconectada.

Tampoco hubo cuidado del legislador al indicar que la invasión necesita obtener, modificar o suprimir los datos, pues el chismorreo o el envío de datos a terceros pueden desviarse del tipo penal, además de considerar que invadir un dispositivo sin mecanismo de seguridad tampoco es crimen. Sin mencionar que la falta de obligación de conservación de logs

de conexión y acceso pueden inviabilizar la instrucción criminal por la dificultad en identificarse al agente.

En ese sentido, la legislación argentina desde 2008 prevé disposiciones más completas, sobre todo en la hipótesis de violación de confidencialidad de las informaciones privadas, lo que no dependería de la violación del sistema de seguridad, según el cambio del artículo 153 de su Código Penal, bastando el acceso a las informaciones sin autorización para la caracterización del crimen.

Tomando al ejemplo colombiano, se perciben dos tipos penales más abarcadores y no por eso menos precisos, pues la ley nº 1.273 de 2009 fue acertada al capitular conductas específicas como denegar el servicio, *phishing* por medio de páginas de internet, creación o diseminación de software malicioso y además la violación de datos personales, con penas más severas que la ley brasileña.

Finalmente, para que se aproveche la ley para la protección de sus dispositivos es indispensable:

- Utilizar la protección de contraseña, código o datos biométricos para impedir el acceso no autorizado. Esto vale para computadoras de mesa, notebooks, tablets, smartphones y reproductores de audio o video portátiles;
- Dejar un sistema de firewall o detección de intromisión siempre activo y con perfil de actividades maliciosas siempre actualizado para evitar falsos positivos.
- Siempre que note actividad sospechosa, comunicarla a las autoridades policiales y buscar ayuda de especialista inmediatamente, además de evitar usar o dispositivo para que las pruebas digitales sean preservadas en caso de pericia.

LA LEGALIDAD DEL PAGO DE DERECHOS AUTORALES RELATIVOS A LA EJECUCIÓN PÚBLICA SOBRE EL *STREAMING*

Milena Mendes Grado

Internet representó un gran avance tecnológico para la humanidad en las últimas décadas. Posibilitó que las interacciones entre las personas se volviesen mucho más rápidas, eliminando las distancias y retrasando el tiempo. La legislación no logra seguir la velocidad a la que las relaciones en Internet ocurren, sin embargo, esta no puede ser un territorio sin ley, como pretendía John Barlow en su "*Declaration of the Independence of Cyberspace*". De esta forma, las leyes de cada país, en la medida de los posible, son aplicadas a las situaciones fácticas ocurridas en Internet.

Una de las nuevas tecnologías que llegaron con internet fue el *streaming*, cuya definición ordinaria es la distribución de archivos de sonido o archivos multimedia por Internet. Esta tecnología brinda a las personas la posibilidad de escuchar música, ver videos, filmes y programas que usualmente eran transmitidos por radio y televisión, a través de internet. Esta modalidad de transmisión de datos e informaciones multimedia ha sido cada vez más difundida, pues posibilita al usuario la interacción con cualquier dispositivo que disponga de acceso a internet (celulares, *tablets*, etc.) desde cualquier lugar. Sin embargo, la legislación brasileña, principalmente la Ley de Derechos Autorales (Ley n° 9610/98) no hace ninguna mención expresa al *streaming*.

El artículo 68 de la Ley de Derechos Autorales Brasileña determina que no pueden ser utilizadas en ejecución pública o representación: obras teatrales, composiciones musicales o literario-musicales ni fonogramas

sin previa y expresa autorización del autor. Por su parte, el párrafo 2º de ese mismo artículo define como ejecución pública la utilización de composiciones musicales o literario-musicales, mediante la participación de artistas, remunerados o no, o la utilización de fonogramas y obras audiovisuales, en lugares de frecuencia colectiva, por cualquier proceso, inclusive la radiodifusión o transmisión por cualquier modalidad, y la exhibición cinematográfica. El cobro de derechos autorales sobre la ejecución pública está hoy en Brasil bajo la tutela de ECAD – Agencia Central de Recaudación y Distribución.

La legislación brasileña define la ejecución pública de manera diferente de otras legislaciones de los países de América Latina.

De esa forma, el objetivo de este trabajo es verificar si la ECAD (órgano de gestión colectiva de derechos) puede cobrar por el *streaming*, teniendo en cuenta la actual Ley de Derechos Autorales Brasileña. Sin embargo, para que sea hecha esta evaluación, será necesario entender el fundamento de la ley haciendo un análisis de los conceptos por esta presentados, unido a un análisis de derecho comparado, en especial, respecto a América Latina, Europa y Estados Unidos y de las escasas decisiones brasileñas sobre el tema.

ANÁLISIS DE LA LEY DE DERECHOS AUTORALES BRASILEÑA

La legislación que trata de derechos autorales, en especial la parte que trata de la ejecución pública, sufrió algunas alteraciones desde su nacimiento en Francia y Estados Unidos, pero el fundamento para el ejercicio de derechos autorales sobre la ejecución pública permanece igual: el público.

Vale destacar que el "público" también justificó la forma de cobrar los derechos sobre la ejecución pública por medio de la gestión colectiva de derechos, actualmente ejercida por la ECAD en Brasil, porque está la imposibilidad de que los autores concedan autorizaciones para todas las ejecuciones y presentaciones públicas; es algo inviable.

Así, para entender el concepto, es esencial que se sepa, exactamente, quién es ese público y cuál es el uso hecho por ese público que configuraría la ejecución pública.

En entrevista realizada por correo electrónico a la ECAD[64], el órgano entendió que el concepto de uso público no tiene relevancia para la caracterización de la ejecución pública porque el uso público sería toda y cualquier utilización del derecho autoral con fines públicos. Sin embargo, este entendimiento, parece enfocarse solo en una interpretación positivista, sin analizar aspectos históricos ni tampoco aspectos semánticos de la norma.

La legislación brasileña permite la utilización de la obra en forma de reproducción, distribución y comunicación al público. Estas tres acciones permiten que la población tenga acceso a las obras, por consiguiente, son actos de puesta a disposición del público.

La Ley de Derechos Autorales brasileña menciona la puesta a disposición del público cuando se refiere a la reproducción (Art.30), a la distribución (Art. 2º, IV) y a la comunicación con el público (Art. 2º, V). El artículo 30 de la Ley de Derechos Autorales asevera que, en el ejercicio del derecho de reproducción, el titular de los derechos autorales podrá poner a disposición del público la obra, en la forma, lugar y por el tiempo que desee. Por su parte, el artículo 2º, en sus incisos IV y V, conceptualiza la distribución como la puesta a disposición del público mediante alquiler, venta o cualquier otra forma de transferencia de posesión y de propiedad

64 BRETAS, C. **Entrevista** [mensaje personal]. Mensaje recibido por <milenagrado@gmail.com> el 5 de mayo de 2014.

y la comunicación con el público como acto mediante el cual la obra es puesta al alcance del público que no configure distribución.

Refuerza el entendimiento de la existencia del concepto de la puesta a disposición del público la posición del Hermano Durval[65] en discusión sobre la naturaleza jurídica de la reproducción en discos: "Es la puesta a disposición del público y no su ejecución pública lo que caracteriza la edición de la obra musical grabada en la matriz y multiplicada en discos".

De esa forma, la ejecución pública es una categoría dentro de la comunicación con el público, la cual, a su vez, es una especie del género puesta a disposición del público.

Cuando una obra es puesta a disposición del público, el público en este caso es un conjunto de personas, una población. Por otro lado, en una evaluación semántica de la expresión "la comunicación al público", dentro del contexto de la ley brasileña, la cual trae como ejemplos lugares de frecuencia colectiva y las transmisiones, se concluye que la expresión significa, en realidad, no sólo un conjunto de personas o una población, sino que es utilizada específicamente como un conjunto de espectadores

Estando comprobado que la puesta a disposición del público comprende actos de reproducción, distribución y comunicación con el público, no se puede equiparar los conceptos de puesta a disposición del público y comunicación con el público. Un análisis legalista indicaría que la comunicación con el público sería la puesta a disposición del público, cuando no estén caracterizados actos de reproducción o de distribución; sin embargo, ese entendimiento posibilitaría confundir género y especie y, por consiguiente, se confundirían los conceptos.

La diferencia que permite clasificar los conceptos en género y especie es exactamente la comprensión de la palabra público, em casa una de esas ideas. Como fue mencionado, cuando se hace referencia al público en puesta a disposición del público, esta designa una población, por su parte,

[65] DURVAL, Hermano. **Direitos autorais nas invenções modernas.** Río de Janeiro: Andes, 1956. p.181

cuando hay una referencia en comunicación con el público, esta representa un conjunto de espectadores, una audiencia.

De esta forma, el hecho de que algo esté al alcance del público, por ejemplo, disponible en internet, no significa que haya una comunicación con el público, dando paso al necesario pago de derechos autorales a la ECAD

La ley de Derechos Autorales brasileña específica que son actos de comunicación con el público: la representación pública y la ejecución pública. Ambas hacen alusión a los lugares de frecuencia colectiva, a la transmisión y a la exhibición cinematográfica. En lo que se refiere a la frecuencia colectiva y a las exhibiciones cinematográficas, se identifica fácilmente el público como un conjunto de espectadores.

En lo que se refiere a las transmisiones, hay que considerar que ese conjunto de espectadores no necesita estar definido e identificado. En el caso de las transmisiones, no es posible identificar una audiencia física, pero, aun así, hay claramente un conjunto de espectadores, una audiencia y, por tanto, un público.

Vale resaltar, sin embargo, que el fundamento de la ejecución pública no es el hecho de ser definido o indefinido. Ante todo, debe ser público. Y para ser público, y también para no haber confusión con el concepto de puesta a disposición del público, es necesario que haya simultaneidad.

Ese es el entendimiento de José de Oliveira Ascensão[66], quien señala que "en la radiodifusión, la recepción es privada. Pero se vio el carácter público de la comunicación en la simultaneidad de las recepciones".

---

66 ASCENSÃO, J. de O. **Direito autoral**, Río de Janeiro: Renovar, 1997. p.197.

Por consiguiente, el concepto de ejecución pública puede ser definido como un uso de composiciones musicales o literario-musicales, fonogramas u obras audiovisuales por un conjunto de espectadores simultáneamente.

Derecho Comparado

Brasil posee pocas decisiones sobre la gestión colectiva de los derechos autorales en los casos de *streaming*, razón por la cual es muy importante buscar referencias externas para complementar la investigación realizada. Esas referencias estarán centradas en Estados Unidos y en la Unión Europea.

La tecnología del *streaming* fue desarrollada en los Estados Unidos y, por tanto, la legislación y la jurisprudencia de ese país sobre el tema están más perfeccionadas y consensuadas.

Además, la legislación brasileña tiene muchas de sus raíces en la legislación europea y con el derecho autoral no es diferente. Las principales fuentes de la legislación brasileña de derecho de autor poseen inspiración francesa, de ahí la relevancia por buscarse los parámetros europeos.

Además, es importante entender cómo los países vecinos de América Latina, que también sufrieron las mismas influencias de Estados unidos y Europa, se han comportado ante este tema.

En la decisión del Segundo Circuito de la demanda entre ASCA[67] (*American Society of Composers, Authors and Publishers*) v. *United States of America* se debatía sobre la posibilidad de cobro de la performance pública, concepto similar al de ejecución pública, en el caso de *downloads*. No se trata, exactamente, de la misma situación, ya que los conceptos de

[67] ESTADOS UNIDOS DE AMÉRICA. United States Court of Appeals, Second Circuit. United States v. ASCAP, 485, F. Supp. 2d 438 (S.D.N.Y. 2007)

download y *streaming* son diferentes, y presentan juicios muy significativos, que pueden ser perfectamente aplicado en este escenario.

La decisión argumenta que la Ley presenta como concepto de performance los actos de escenificar, presentar, danzar, actuar y todos esos actos exigen la percepción contemporánea. Así, se definió que como los *downloads* no eran performances musicales de percepción simultánea, no deberían estar incluidos en el concepto de performance pública y no ocasionarían el cobro de la ASCAP:

> *"In answering the question on if whether a download is a public performance, we turn to Section 101 of Copyright Act, which states that "to perform a work means to recite, render, play, dance or act it, either directly or by means of any device process." 6 17 U.S.C§ 101. (…)*
> *The ordinary sense of the words "recite", "render" and "play" refer to actions that can be perceived contemporaneously. (…)*
> *The downloads at issue in this appeal are not musical performances that are contemporaneously perceived by the listener".*

La decisión, en otras palabras, entiende que la palabra pública, del concepto de performance pública, está relacionada a una audiencia indeterminada y no hay una población indeterminada.

Por su parte, la Dirección Europea 2001/29/EC, que buscaba armonizar la legislación de los Estados Miembros en materia de derecho de autor y de derechos conexos, establece que los Estados Miembros deben prever a

favor de los autores el derecho exclusivo de autorizar o prohibir cualquier comunicación al público de sus obras, por cable o inalámbricas, incluyendo su puesta a disposición del público para hacerlas accesibles a cualquier persona a partir del lugar y en el momento por ella escogido.

De esa forma, la Directiva Europea establece una diferenciación clara entre comunicación al público y puesta a disposición del público, y por lo que se interpreta del concepto presentado sobre la programación *on demand*, que es accesible a cualquier persona a partir del lugar y en el momento por ella escogido, y que estaría clasificada como puesta a disposición del público. Ese entendimiento es reforzado por la lectura de los ítems 23 y 24 de las consideraciones de la Directiva.

La Directiva pretende la protección autoral para ambas situaciones, pero en ningún momento establece equivalencia entre los conceptos o determina que ambos actos ocasionarían el cobro por ejecución pública. El cobro sobre ejecución pública, o sea, por órganos de gestión colectiva de derechos, debe ser efectuado sólo sobre la comunicación con el público.

Todavía a respecto del tema, la decisión de 2012, fruto de la disputa entre el órgano de gestión colectivo de Derechos Autorales de Italia y Marco Del Corso[68], permite inferir que hay diferencias entre los actos de comunicación al público y los actos de puesta a disposición del público, siendo que esos últimos no generarían cobros por el órgano de gestión colectiva:

[68] ITALIA. SENTENCIA DEL TRIBUNAL DE JUSTICIA (Tercera Sección). Derechos de autor y derechos conexos en la sociedad de la información — Aplicabilidad directa, en el ordenamiento jurídico de la Unión, de la Convención de Roma, del Acuerdo TRIPS y del WPPT — Directiva 92/100/CE — Artículo 8.°, n.° 2 — Directiva 2001/29/CE — Concepto de 'comunicación al público' — Comunicación al público de fonogramas difundidos por la radio en el consultorio de un dentista. 15 de marzo de 2012. Disponible en: <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130de6736c86d2847430ea9d5804702fb7160.e34KaxiLc3eQc40LaxqMbN4OaNyKe0?text=&docid=120443&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=50122> Acceso en 29 de junio de 2014.

> "Con sus cuarta y quinta cuestiones, el órgano jurisdiccional de reenvío se pregunta si la difusión gratuita de fonogramas, efectuada en un consultorio de un dentista, en el ámbito del ejercicio de una profesión liberal, en beneficio de los clientes, que de ella disfrutan independientemente de su voluntad, constituye una «comunicación al público» o una «puesta a disposición del público», en la acepción del artículo 3.°, n. 2, apartado b), de la Directiva 2001/29, y si esa difusión da derecho al recibimiento de una remuneración para los productores fonográficos.

Al respecto, nótese desde ya que el órgano jurisdiccional de reenvío refiere, en el enunciado de dichas cuestiones, el artículo n.°2, apartado "b", de la Directiva 2001/29, relativo al derecho exclusivo de los productores de fonogramas de autorizar o prohibir la puesta a disposición del público, por cable o inalámbrica, de sus fonogramas, de modo que sean accesibles para cualquier persona a partir del lugar y en el momento por ella escogido.

Como resulta de la exposición de motivos de la propuesta de la Directiva 2001/29 [COM(1997)628], corroborado por el vigésimo quinto argumento de esa directiva, "la puesta a disposición del público, en el consentimiento de la referida disposición, tiene como objetivo las «transmisiones interactivas a pedido», que se caracterizan por el hecho de que cualquier persona puede acceder a partir del lugar y en el momento por ella escogido". Concluye, entonces, que "resulta de la decisión de reenvío que, en el proceso principal, solo se encuentra en causa la radiodifusión de música en un consultorio de dentista, destinada a los clientes que en él se encuentran, y no la transmisión interactiva a pedido".

Po último, cumple destacar que la legislación de América Latina, en general, es diferente a la brasileña y estipula que la puesta a disposición al público está sujeta al cobro por el órgano de gestión colectiva, no diferenciando la puesta a disposición del público de la ejecución pública. En ese sentido, véase la legislación colombiana, por ejemplo:

> Artículo 168* Desde el momento en que los artistas intérpretes o ejecutantes autoricen la incorporación de su interpretación o ejecución en una fijación de imagen o de imágenes y sonidos, no tendrán aplicación las disposiciones contenidas en los apartes b) y c) del artículo 166 y c) del artículo 167 anteriores. Párrafo 1 Sin perjuicio de lo contemplado en el párrafo anterior, los artistas intérpretes de obras y grabaciones audiovisuales conservarán, en todo caso, el derecho a percibir una remuneración equitativa por **la comunicación pública**, **incluida la puesta a disposición** y el alquiler comercial al público, de las obras y grabaciones audiovisuales donde se encuentren fijadas sus interpretaciones o ejecuciones. En ejercicio de este derecho no podrán prohibir, alterar o suspender la producción o la normal explotación comercial de la obra audiovisual por parte de su productor, utilizador o causahabiente. Este derecho de remuneración se hará efectivo a través de las sociedades de gestión colectiva, constituidas y desarrolladas por los artistas intérpretes de obras y grabaciones audiovisuales, conforme a las normas vigentes sobre derechos de autor y derechos conexos.

Por tal razón, el tema no es muy controversial en los países de América Latina, con excepción de Brasil. Además, en cualquier lugar del mundo, es importante considerar la dificulta de efectuar este tipo de cobro de pequeños y medios negocios que pueden hospedar sus sitios en otros países o usar mecanismo para dificultar el cobro. Al final, sólo las grandes corporaciones acabaron pagando los derechos sobre la ejecución pública en esas circunstancias.

Las decisiones brasileñas sobre el tema

Las pocas decisiones sobre el tema en Brasil tendían a entender que no procedería el cobro sobre la ejecución pública en las hipótesis de *streaming*. A continuación, se presentan algunas de esas pocas decisiones.

En el proceso nº 0174958.45.2009.8.19.0001/RJ, la ECAD exigía el pago de los derechos autorales sobre la ejecución pública alegando que la TNL PCS S/A (portal TERRA) estaba haciendo comunicación al público por medio de *simulcasting* y *streaming* a través de la herramienta Sonora, parte del portal en cuestión. El portal TERRA se defendió alegando que alcanzaba a sus clientes solo en la modalidad de *on demand*, lo que configuraría la hipótesis de distribución digital y no de ejecución pública. La decisión de la primera instancia señaló que las modalidades de *simulcasting* y *streaming* solo reproducirían la emisora Oi FM en la computadora y como los derechos autorales sobre la programación ya estaban pagados, cobrar por su reproducción online constituiría un *bis in idem*. En la decisión final, en embargos infractores se entendió que *simulcasting* sería un mero ejercicio de radiodifusión, razón por la cual el cobro por la ECAD caracterizaría *bis in ídem* y el *webcasting* sería una transmisión individual y dedicada, restringida sólo a la localidad de aquel usuario, razón por la cual no comportaría el pago a la ECAD.

En el proceso nº 0173652-06.2010.8.26.0100/SP, em que la ECAD demandaba a la Asociación de las Emisoras de Radio y Televisión del Estado de Sao Paulo – AESP, en la sede de apelación entendieron los jueces de apelación que la transmisión por internet era transmisión simultánea de la programación de radio convencional, no habiendo espacio para considerar una transmisión diferenciada o independiente, lo que originaría la contribución a título de derechos autorales.

Por último, la decisión de la apelación civil nº0019591-47.2013.8.19.0014/RJ trata, exclusivamente, de la modalidad de *simulcasting*, entendida como radiodifusión, y no habiendo más de una utilización de la obra musical transmitida, no es posible realizar el cobro sobre el mismo hecho generador.

Las decisiones brasileñas presentan algunos equívocos. El primero de ellos está relacionado a las modalidades de *streaming*. En la mayoría de las hipótesis, se dividieron las modalidades de *streaming* en *simulcasting* y *webcasting*, y esa división no parece correcta porque el *webcasting* (*streaming* en la web) es género al cual el *simulcasting* pertenece. Por la lectura de los juicios, lo ideal sería presentar los conceptos *live streaming* (lo que conocemos como en vivo) y *on demand* (programación por solicitud del espectador)

Además, técnicamente el *simulcasting* es una retransmisión y no puede ser considerada ejercicio de radiodifusión, pues es necesaria la concesión pública para tal ejercicio.

Es importante considerar, además, que el argumento para no pagar en caso de transmisión individual y dedicada, tampoco se justifica porque, aun siendo individual, es posible que estos individuos estén haciendo un uso público.

Las decisiones brasileñas parecen estar de acuerdo con la ley, pero la "razón de decidir" no estaría correcta por no considerar el fundamento de esta, que sería la existencia de un público que percibe la obra simultáneamente.

De inmediato, ante ese concepto, ya se excluye la modalidad de *streaming on demand*, pues en esa modalidad no hay simultaneidad, cada persona recibe aquella obra en el momento que desea, y eso no los hace un conjunto de espectadores. La obra es simplemente puesta a disposición del público en Internet. El simple hecho de poner la obra a disposición de los usuarios no configura la ejecución pública.

En el caso de la modalidad *live streaming*, hay la simultaneidad necesaria para la formación de una audiencia, aunque de forma remota. Sin embargo, aun así, queda una duda: si ya hay un cobro de derechos autorales sobre ejecución pública sobre aquella exhibición de la obra en aquel momento, ¿sería posible un nuevo cobro?

La Ley de Derechos Autorales dispone que es considerada ejecución pública la transmisión por cualquier modalidad. La modalidad *live streaming* tiene la simultaneidad necesaria para la caracterización de la ejecución pública. Sin embargo, el fundamento del pago de derechos autorales sobre la ejecución pública es la exhibición de la obra para un público (conjunto de espectadores) simultáneamente. Por consiguiente, ese es el hecho generador, y si ya hubo un pago sobre ese hecho generador, realmente un nuevo cobro significaría *bis in idem*, decidió acertadamente la jurisprudencia brasileña. Es cierto que hay dos modalidades de transmisión, pero hay sólo un hecho generador, o sea, sólo una ejecución pública

Ocurre que, recientemente, después de una audiencia pública, el Tribunal Superior de Justicia – STJ de Brasil decidió que era posible el cobro de los derechos autorales sobre la ejecución pública. Esa decisión fue muy criticada por abogados y doctrinadores, sin embargo, debe marcar las decisiones de aquí en adelante.

Conclusión

A pesar de la decisión del STJ, en Brasil, a nuestro entender la ejecución pública tiene fundamento en el uso público. El significado de uso público es en realidad un uso por el público, que en este caso es un conjunto de espectadores.

Esta conclusión es posible porque la legislación de Derechos Autorales brasileña, indirectamente, nos presenta el concepto de puesta a disposición al público, que engloba actos de reproducción, distribución y comunicación al público. La puesta a disposición del público es el acto de hacer más accesible al público, y el acto comunicación al público es el acto mediante el cual la obra es puesta al alcance del público. En esos dos conceptos, la diferenciación ocurre en función de la palabra público, que en la primera significa un conjunto de personas, una población, y en el segundo significa un conjunto de espectadores.

Para que se configure un conjunto de espectadores es necesario el aspecto de la simultaneidad. De esta forma, el cobro por los derechos de autor sobre la ejecución pública en el caso de *streaming* sólo es posible en los servicios de *live streaming* que poseen esa característica de contemporaneidad de la recepción por los espectadores. Los servicios de *streaming on demand* se configuran sólo como puesta a disposición del público y no hay razón para el cobro por la ECAD, porque no está formada

una audiencia, no hay simultaneidad, y cada una de las personas tienen acceso individual, en un momento distinto.

Por consiguiente, el cobro por la ECAD de derechos autorales sobre la ejecución pública debe recaer sólo por la modalidad *live streaming*, que permite la configuración del público en la acepción del concepto de comunicación al público y, consecuentemente, de ejecución pública, ya que hay simultaneidad en la recepción de la obra por los espectadores.

Por su parte, aunque en los demás países de América Latina sea posible el cobro por la mera puesta a disposición del público, es importante evaluar la forma en que se cobran esos derechos, debido a que difícilmente los órganos de gestión colectiva alcanzaron pequeños y medios negocios, lo que puede generar desigualdad e inseguridad jurídica.

REFERENCIAS BIBLIOGRÁFICAS

ABRÃO, Eliane Y. **Direitos de autor e direitos conexos**. São Paulo: Editora do Brasil, 2002.

ASCENSÃO, José de Oliveira. **Direito autoral**. 2ª ed., rev. y ampl.. Río de Janeiro: Editora Renovar, 1997.

BITTAR, Carlos Alberto. **O direito de autor nos meios modernos de comunicação**. São Paulo: Editora Revista dos Tribunais, 1989.

DURVAL, Hermano. **Direitos autorais nas invenções modernas.** Río de Janeiro: Andes, 1956.

SANTOS, Manoel J. Pereira dos. Parecer execução pública musical na Internet: rádios e TVS virtuales. **Revista ABPI**, nº 103, Nov/ Dic. 2009.

DE LA NECESIDAD DE INCLUSIÓN DE URL EN ÓRDENES JUDICIALES.

Victor Auilo Haikal

El Recurso Especial nº 1.306.157-SP juzgado por el Superior Tribunal de Justicia[69] está en total sintonía con buena parte de los excesos cometidos en internet, especialmente en plataformas de diseminación de contenido, sea una red social, un microblog o un portal de broadcasting, como YouTube, en el que existen ofensas dirigidas a una persona, sea natural o jurídica.

Según lo postulado por los ministros que juzgan, internet se vuelve cada vez más un ambiente perverso y hostil, en vez de un ambiente donde sólo son cultivadas las relaciones interpersonales con objetivos constructivos, corteses y educados. El exceso de críticas, juicios y discursos de odio o agresión es resultado del fenómeno social de diseminación de la sensación colectiva de injusticia, donde cualquier vicisitud pasa a ser tratada como un mal mayor a ser combatido, dando margen a aquellos que buscan hacer justicia por medios propios.

Por eso, los que juzgan argumentaron respecto a la importancia de que las empresas prestadoras de servicios de divulgación de contenido posean herramientas aptas para efectuar la remoción de ciertos materiales que causan daños a terceros de forma masificada y rozando el anonimato, vedado por la Constitución en su artículo 5º, IV.

---

[69] BRASIL. Tribunal Superior de Justicia. Recurso Especial nº 1.306.157-SP. DERECHO CIVIL. OBLIGACIÓN DE HACER Y NO HACER. VIDEOS DIVULGADOS EN SITIO DE COMPARTICIÓN (YOUTUBE). IMITACIÓN FRAUDULENTA IMPLICANDO LA MARCA Y MATERIAL PUBLICITARIO DE LOS AUTORES. OFENSA A LA IMAGEN Y AL NOMBRE DE LAS PARTES. DEBER DE RETIRADA. INDICACIÓN DE URL'S. INNECESARIO. INDIVIDUALIZACIÓN NECESITA EL CONTENIDO DEL VIDEO Y EL NOMBRE A ÉL ATRIBUIDO. MULTA. REFORMA. PLAZO PARA LA RETIRADA DE LOS VIDEOS (24 H). MANUTENCIÓN. Disponible en: < https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=33741219&num_registro=201102315501&data=20140324&tipo=91&formato=PDF >. Acceso en: 16 feb 2016.

Sin embargo, la tarea de retirar cierto contenido del aire en internet es casi hercúlea, porque la facilidad con que se vuelve a publicar cierto material y la dispensa de formas más severas y cautelosas de registro e identificación de usuarios genera un escenario muy desfavorable para las víctimas, sin saber de dónde viene el tiro para intentar defenderse.

Entre las cuestiones abordadas por los Ministros, las que merecen una discusión específica son: (i) la necesidad de anotar la URL[70], (ii) la aplicación de filtros previos para contenidos que ya recibieron y (iii) el tiempo mínimo para la remoción de los contenidos marcados como ilegales, dañinos o ilegítimos.

Los daños a los derechos de la personalidad son de absoluta claridad y no son puntos de discusión en la sentencia. La violación de derechos autorales en este caso específico es cuestionable, pues existe el empleo del recurso de la parodia, permitida por la legislación autoral en vigor[71] y no se vislumbra obtención de lucro o de desvío de la clientela de la propietaria del video; de lo contrario, es una protesta.

Las páginas a ser exhibidas en internet poseen como factor único de identificación e inequívoco su URL, la indicación de la dirección exacta de localización es necesaria para que se tenga seguridad de lo que se necesita ser removido, en casos similares al analizado.

Eso se debe a que, aunque los proveedores de aplicación por el Marco Civil de Internet[72] ofrezcan una plataforma para que terceros envíen contenidos, no es razonable que estos tengan como responsabilidad detectar el material ilegítimo en sus archivos, como fue decidido por la Corte Superior, en voto expresado por la Excma. Min. Nancy Andrighi en la Rcl. 5072, sobre todo porque el ofendido necesita indicar lo que le causa daño y para evitar la censura como parte del pedido determinado, exigido

[70] Uniform Resource Locator, dirección que señala directamente a un lugar inequívoco de internet, pudiendo ser una página o un archivo.
[71] Artículos 46, VIII y artículo 47 de la ley 9.610 de 1998.
[72] Ley 12.965 de 2014, artículo 5º, VII. En vigor a partir del 23 de junio de 2014.

por el Código de Proceso Civil, artículo 286, *caput*[73], que también compone el principio de adstricción, solo se difiere de aquello que es requerido.

Ese raciocinio merece atención, sobre todo porque la orden judicial debe ser determinada o determinable, como requisito de validez de todo acto jurídico, de acuerdo con el Código Civil en su artículo 104, II combinado con el artículo 185 del mismo Diploma. De esta forma, se establece con precisión lo que se debe retirar del aire mediante la identificación inequívoca de la página a remover, ante la miríada de direcciones que internet posee.

Observando que existen decisiones pugnando por la responsabilidad de remoción de contenido sin la necesidad de una URL específica, el Marco Civil de Internet en su artículo 19, §1º, expresamente determinó como debe ser expedido el mandato judicial para la retirada del contenido por los proveedores de aplicación.

> *"§ 1º La orden judicial de la cual trata el* caput *deberá contener, bajo pena de nulidad, identificación clara y específica del contenido señalado como infractor, que permita la localización inequívoca del material."*

Ante este comando legal, es natural que la identificación no se limite a la URL de las páginas a ser removidas, ya que el contenido a ser eliminado también puede ser detectado de otras formas, dada la versatilidad que el estado de la técnica actual posee.

Archivos de computadoras puede ser comparados por la secuencia de bytes que poseen, además de por la forma en que son reproducidos para cognición humana, lo que facilita la interpretación automatizada de su contenido y agiliza el escaneo de materiales por la indexación promovida por sistemas debido a la identidad del código binario.

[73] En el momento de la primera publicación de este trabajo estaba en vigor la Ley nº 5.869 de 1973. Con la entrada en vigor de la Ley nº 13.105 de 2015, revocándose la anterior, el artículo correspondiente es el 322. (N.A.)

Con la mención de que hubo un Dictamen Técnico en el proceso, fue destacado el fragmento declarado por el *expert*, asentando la posibilidad de efectuarse la comparación de una secuencia de *frames*[74] con otra, utilizando la función *hash*[75], por ejemplo.

En especial, debido a que el sistema YouTube realiza un procesamiento de material al ser enviado a sus servidores, efectuando interpretación de formato del archivo y posterior compresión y codificación para ser reproducido en su interfaz. Así, existe la posibilidad técnica del uso de filtros, pues se consigue programar el sistema para rechazar todos los archivos enviados cuyo *hash* sea idéntico al material que fue objeto de decisión judicial mientras hay un procesamiento del video.

Así, habrá criterios objetivos para que el sujeto de derecho perjudicado solicite al proveedor de aplicación no solamente la eliminación de una URL, sino también de todos los archivos cuyo *hash* sea idéntico al contenido ofensivo o función similar capaz de identificar un archivo de computadora de forma exacta.

Algunos filtros ya existen, especialmente para identificar material pornográfico, ya que el sistema de YouTube es capaz de identificar material adulto sin la necesidad de verificación humana, dada la gravedad de crímenes como la pedofilia, por ejemplo.

Sin embargo, la alteración más simple en el contenido a ser reproducido puede generar una gran diferencia en el código de programación, dificultando la comparación automatizada entre los archivos, imponiéndose la verificación humana o de algoritmos más sofisticados.

Verificando que buena parte de los videos diseminados no sufre alteración de su contenido, la identificación previa por filtros puede aumentar la efectividad de la medida tomada por la víctima ante el proveedor de aplicación. Por eso, en caso de que el autor identifique el código *hash* de

[74] Imagen estática correspondiente a un instante de un video

[75] Algoritmo empleado en archivos de computadora generando un código único que lo identifica. En caso de que 1 byte sea alterado del archivo original, todo el *hash* es modificado.

los archivos que merecen ser removidos y en el futuro filtrados, no habrá ofensa a lo previsto por el Marco Civil de Internet, pues hay identificación objetiva de aquello que se pretende remover para expedición de la orden por el magistrado y se utilizará un criterio objetivo de naturaleza computacional para combatir la ilegalidad sufrida.

La ausencia de URL fue justificada en la decisión como no siendo impeditiva para la remoción del material ordenado por el Excmo. Min. Felipe Salomão, al menos para aquellos que guardarían el mismo título, pues con escaneo en texto claro habría chance de segar el material replicado.

No obstante, tal raciocinio no se reviste de total seguridad jurídica, pudiendo haber títulos con el mismo nombre y contenido totalmente distintos, lo que no permitiría la remoción automatizada, pero ciertamente filtraría una cantidad plausible para posterior filtro humano.

Es importante también subrayar que el mismo Ministro expuso haber un defecto en la prestación del servicio, representado por la imposibilidad de realizar un escaneo para la eliminación del contenido combatido, lo que no parece adecuado, ya que el defecto del producto o servicio está vinculado a la seguridad esperada por el consumidor cuando es colocado en el mercado [76].

El modo de suministro del servicio y los resultados están relacionados directamente al comportamiento humano, pues si no existiese mal uso de la herramienta, ni siquiera sería necesario el empleo de la tutela jurisdiccional para la protección de los derechos a la personalidad y al autor, actualmente atacados por videos enviados a YouTube.

[76] Artículos 12, §1º y 14, §1º del Código de Defensa del Consumidor

Tal circunstancia se desprende del principio de la inimputabilidad de la tecnología. No se culpan a los productores de armas de fuego por homicidios o a los fabricantes de carro por atropellamiento. *Mutatis mutandis*, el proveedor de servicio para facilitar la transmisión de contenido por seres humanos no merece que su herramienta sea calificada como defectuosa si no consigue impedir que sus usuarios cometan actos ilícitos o crímenes.

Pero, cuando el servicio ofrecido atiende satisfactoriamente a los comandos jurisdiccionales que están al alcance de su propietario, basta ser solicitado adecuadamente por el operador del derecho en la causa, cuya *expertise* en tecnología de la información es obligatoria, para obtener resultados más eficientes.

Por último, se discutió cuál sería el plazo balanceado para el cumplimiento de la orden judicial por grandes proveedores de aplicación, cuestionado por el presidente del Grupo, Excmo. Min. Raul Araújo, que presentó el raciocinio de que grandes corporaciones poseen dificultades para atender a las requisiciones judiciales en tan corto plazo, que se pierden en su estructura interna de "jerarquía reverencial", a veces.

Data maxima venia, este es el tipo de obstáculo que empresas que proveen servicios o productos cuya naturaleza es la tecnología de punta jamás deberían osar reclamar, toda vez que posee total dominio de la técnica para optimizar sus procesos y sobre todo entender cuáles son los riesgos a los que terceros de buena fe está sujetos debido al mal uso de lo que les es ofrecido.

Aunque exista el principio de la inimputabilidad de la tecnología para exentar al medio de culpa por su uso, de otro lado está el principio del deber de atención, que impone al proveedor el deber de tomar las

precauciones necesarias para minimizar los daños ocasionados por el uso de aquello que pone en circulación en el mercado.

Por consiguiente, poseer un procedimiento eficiente para tratamientos de incidentes es imperioso, habiendo sistemas que comportan perfectamente tal sed de urgencia, de sofisticación y precisión compatibles con la posición del mercado que los grandes *players* de la tecnología de la información y comunicación ocupan.

Los contenidos en internet poseen un excepcional poder de diseminación y atomización. En cuestión de minutos una información puede recorrer millones de personas. Admitir un plazo de 5 días para la remoción de contenidos es excesivo, pues frustra totalmente la tutela de protección a los derechos de la personalidad, debido a la presión a la que la víctima está sometida y a la condición de vulnerabilidad a la que estará sujeta, con reflejos directos en su rutina, imagen y reputación.

Por eso, el plazo de 24h es adecuado y razonable, pues tiene como objetivo el cese de los daños a la personalidad tan rápido cuanto sea posible, atendiendo a los anhelos incrustados por la determinación de la dignidad de la persona humana como principio fundamental de la Constitución Federal y a la protección que el Código Civil confiere a los derechos de la personalidad tanto a la persona natural, como a la jurídica.

IP NAT: LA RESPONSABILIDAD DE LOS PROVEEDORES DE CONEXIÓN

Rafael Mott Farah

Con la masificación de los accesos a Internet, se desprende la necesidad del intercambio urgente de tecnología de conexión para la versión 6 del

protocolo IP, más conocida como IPv6, debido al agotamiento de las direcciones IPv4, que ya no es capaz de soportar el acceso a Internet para toda la población. Como medida de transición, los proveedores de conexión utilizan el IP NAT, asumiendo para sí el riesgo de la imposibilidad de individualización de sus usuarios, como será mejor demostrado en el presente estudio.

La versión 4 del protocolo IP, conocida comoIPv4, es bastante utilizada por los proveedores de conexión, sin embargo, esta se demuestra ineficiente e incapaz de gestionar toda la demanda, principalmente en los grandes centros urbanos, pues las direcciones IPv4 fueron asignadas regionalmente de forma nada eficaz.

Su proyecto prevé 32 bits de enderezamiento, pudiendo generar hasta 4 billones ($4x10^9$) de direcciones distintas. Aunque el problema de su distribución geográfica fuese resuelto, todavía no sería suficiente, pues todo terminal que se conecta a internet necesita una dirección IP, sea un *smartphone*, una computadora, un *tablet* o cualquier otro dispositivo.

Teniendo en cuenta la necesidad de una nueva tecnología para suplir el desfasaje del IPv4 sobrevino la versión 6 del protocolo IP, conocida como IPv6, pudiendo generar hasta 340 decillones de direcciones ($3,4x10^{38}$), lo que acabaría por resolver el problema del agotamiento de direcciones, sin embargo, el problema objeto del presente artículo es precisamente los cuestionamientos jurídicos resultantes de la transición entre estas tecnologías, específicamente el uso de la tecnología IP NAT.

Sin adentrarnos en la parte estrictamente técnica de la cuestión, la solución encontrada por los proveedores de conexión fue la utilización de la tecnología IP NAT, la cual funciona, en líneas generales, como si fuese un enorme ruteador casero, o sea, provee la misma dirección IP a

diferentes máquinas, siendo posible la individualización del acceso solamente por medio de la puerta de conexión o puerta mágica.

O sea, tal tecnología permite que varios usuarios accedan a Internet, al mismo tiempo, por la misma dirección IP

En ese sentido, Anatel, por medio de su Informe nº 6/2014-ORCN/SOR, de 31.03.2014, vino a sanar algunas dudas acerca de las medidas paliativas de transición entre el IPv4 y el IPv6, explicitando mejor el funcionamiento de la tecnología IP NAT:

> *El uso de NAT (*Network Address Translation*). El NAT tradicional es una técnica definida por la RFC 3022 -* Traditional IP Network Address Translator (Traditional *NAT). NAT permite que los terminales de una red privada puedan acceder, transparentemente, a terminales en una red externa. Usa una traslación entre direcciones IP públicos y privados. Direcciones IP públicos son aquellos clasificados por el IANA como ruteables en la red pública. Las direcciones IP privadas no pueden ser ruteadas en las redes públicas, y fueron destinadas a la comunicación en ambientes IP privados, como en redes locales (RFC 1918 -* Address Allocation for Private Internets)*. La traslación es hecha por medio de la correspondencia entre un IP válido para un IP privado. Externamente, el terminal destino de la comunicación asumirá, como dirección de origen, el IP válido del equipo que marca el límite entre las redes públicas y privada, como es ejemplificada en la figura siguiente. Esa técnica tiene la gran ventaja de permitir que varios usuarios, en una red privada, puedan utilizar una única dirección IP pública para acceso a la red externa. La gran desventaja de esta técnica es la dificulta*

de la identificación del terminal de origen del tráfico, lo que genera una dificultad importante para las actividades de investigación de crímenes cibernéticos. (s.n.)

En el mismo documento, Anatel además alerta, en su ítem 5.11.5, que la utilización de la tecnología IP NAT trae consigo una gran desventaja, en la identificación de sus usuarios, posibilitando que ciber-infractores permanezcan bajo el manto del anonimato, en los siguientes términos.

> *"5.11.5. NAT dificulta la identificación de los usuarios y posibilita la realización de ataques cibernéticos sin la identificación del origen."*

Además, la Asociación Brasileña de Internet (Abranet)[77], también reconoce los riesgos de la implementación de esta nueva tecnología de conexión a Internet.

> *"Como forma de agilizar la transición en el sistema de direcciones de Internet en Brasil, las operadoras fueron "incentivadas" a adoptar NAT, sigla en inglés para 'traducción de direcciones de red' – o, más recientemente, CGNS, o carrier-grade NATs, que básicamente son NATs en la escala de las grandes teles. En sí, son equipos de red que viabilizan la compartición de direcciones – una extensión adoptada*

[77] Disponible en [http://www.abranet.org.br/Noticias/Anatel-amplia-exigencia-de-certificacao-IPv.6-nos-equipamentos-527.html#.VdynbiVVhVI]. Acceso en: 31.08.2015.

> *globalmente ante el fin de las direcciones IPv4. Pero esa compartición tiene implicaciones, específicamente en la identificación de usuarios en casos de investigaciones o procesos judiciales"*

De esta forma, queda exhaustivamente el conocimiento de los riesgos causados por el uso de esta tecnología por los proveedores de conexión.

Responsabilidad por el uso de la tecnología IP NAT

A pesar de las observaciones realizadas por la propia Anatel, los proveedores de conexión insisten en la utilización de tal tecnología, asumiendo el riesgo por su uso. Bastaría la interrupción de la venta de paquetes de suscripciones para que no existiese el riesgo, sin embargo, los proveedores buscan el lucro desenfrenado, no observando o sin importarse por los riesgos provenientes de la naturaleza del negocio escogido.

De este modo, para que sea posible la individualización de los usuarios de proveedores de conexión que utilizan la tecnología antes mencionada, es necesario el suministro de la puerta de origen (o puerta lógica), sin embargo, tropezamos con algunos embrollos jurídicos en este punto, si no, veamos.

El riesgo asumido por los proveedores de conexión es agravado con la vigencia de la Ley 12.965/2014 – Marco Civil de Internet – que dispone la "*no obligación de los proveedores de aplicaciones a la conservación de las puertas de origen*", definiendo, también, qué se entiende por registros de acceso a aplicaciones.

> *"Art. 15. El proveedor de aplicaciones de internet constituido en la forma de persona jurídica y que ejerza esa actividad de*

forma organizada, profesionalmente y con fines económicos deberá mantener los respectivos registros de acceso a aplicaciones de internet, bajo secreto, en ambiente controlado y seguro, por el plazo de 6 (seis) meses, en los términos del reglamento."

"Art. 5.º Para los efectos de esta Ley, se considera:

(...)

VIII - registros de acceso a aplicaciones de internet: el conjunto de informaciones referentes a la fecha y hora de uso de una determinada aplicación de internet a partir de una determinada dirección IP."

O sea, en momento alguno el Marco Civil de Internet obliga a los proveedores de aplicaciones al almacenamiento de las puertas de origen, de forma que, en el caso de no haber la conservación de la puerta de origen y en que la conexión utilizada para el cometimiento de acto del que se busque la identificación en internet se dé por medio de la tecnología IP NAT, no restarán medios para que sea individualizado el usuario responsable por determinado acto cometido en Internet.

De esa forma, muy a pesar de que la medida paliativa sea aconsejada, con advertencias, por la propia Anatel, los proveedores de conexión que optaron u opten por su implementación deberán estar atentos a los riesgos causados, teniendo en cuenta su responsabilidad objetiva, en los términos del art. 927 del Código Civil.

"Art. 927. Aquel que, por acto ilícito (arts. 186 y 187), cause daño a otro, queda obligado a repararlo.

> *Párrafo único. Habrá obligación de reparar el daño, independientemente de culpa, en los casos especificados en ley, o cuando la actividad normalmente desarrollada por el autor del daño implique, por su naturaleza, riesgo para los derechos del otro."*

Además, el Código Civil conceptúa acto ilícito en su art. 186, siendo cierto que aquel que viole el derecho y cause daño a otro, por acción u omisión voluntaria, negligencia o imprudencia comete acto ilícito y tiene el deber de reparar el daño causado. Ciertamente, no hay cómo separar negligencia e imprudencia de los proveedores de conexión cuando ocurre la utilización de la tecnología antes mencionada.

> *"Art. 186. Aquel que, por acción u omisión voluntaria, negligencia o imprudencia, viole derecho y cause daño a otro, aunque exclusivamente moral, comete acto ilícito."*

En ese sentido, a pesar del art. 927 del Código Civil, elucida el Profesor Luiz Roldão de Freitas Gomes[78], *in verbis*:

> "Inequívocamente, se afilió el legislador aquí al concepto de riesgo creado. En las palabras del inolvidable Maestro, profesor y juez de apelación Serpa Lopes (Curso de direito civil. Vol. V, p. 155) '*por el propio acto de actuar, el hombre goza de todas las ventajas de su actividad, creando riesgos de perjuicios para los otros, de lo que resulta el justo peso de los encargos*'. Según el Prof. Caio Mário da Silva Pereira (Responsabilidade civil. Forense, 1989. p. 300) esta tiene lugar '*cuando la actividad normalmente desarrollada por el autor del daño implica, por su naturaleza, riesgo para los derechos de otro*'. Es más ventajosa que la concepción del riesgo-provecho, ya que no impone al perjudicado el peso de

[78] GOMES, Luiz Roldão de Freitas, in "Aspectos controvertidos do Novo Código Civil" – coordinadores: Arruda Alvim; Joaquim Portes de Cerqueira César y Roberto Rosas – escritos en homenaje al Ministro José Carlos Moreira Alves. São Paulo: Ed. RT, 2003. p. 457.

demostrarlo a favor del autor del daño, menos aún cuestiona sobre su naturaleza, si es de orden económica, o no. 'Lo que se encara es la actividad en sí misma, independientemente del resultado bueno o malo que de ella provenga para el agente (...)'. '*La idea fundamental de la teoría del riesgo puede ser simplificada, al decirse que, cada vez que una persona, por su actividad, crea un riesgo para otro, debería responder por sus consecuencias perjudiciales*'. Va en ello un problema de causalidad. En el Derecho Italiano, Massimo Bianca (Responsabilitá civile. Milano: Giuffrè, 1994. p. 686 e SS.) explica que la responsabilidad objetiva se incluye en la noción y disciplina del ilícito y revela idéntico fundamento: la violación del deber de respeto al otro. Corresponde a la exigencia prevalente de tutelar a terceros también contra hechos no culpables de aquellos que, mediante actividades o cosas, exponen a los otros a un peligro no completamente evitable, aunque con empleo de la diligencia adecuada a la naturaleza de las actividades o de la cosa. Está de acuerdo con el principio de justicia social, según el cual el riesgo de daños a terceros inevitablemente conexos a una actividad o cosa debe ser soportado por quien la ejerce o usa la cosa." (s.n.)

Corroborando tal entendimiento, instruye el doctrinador Sílvio de Salvo Venosa[79]:

> "(...) bajo ese prisma, quien, con su actividad, crea un riesgo debe soportar el perjuicio que su conducta acarrea, incluso porque esa actividad de riesgo le proporciona un beneficio."

No obstante lo ya expuesto, aun ha de ser observada la relación de consumo existente entre el proveedor de conexión y aquel que se sintió

[79] VENOSA, Sílvio de Salvo. Direito Civil: Responsabilidade civil, 2. ed. São Paulo: Atlas, 2002, p. 36.

perjudicado por algún usuario, cliente del proveedor en cuestión, en los términos de los arts. 3º y 17 del Código de Defensa del Consumidor.

> *"Art. 3° Proveedor es toda persona física o jurídica, pública o privada, nacional o extranjera, así como los entes sin personalidad, que desarrollan actividad de producción, montaje, creación, construcción, transformación, importación, exportación, distribución o comercialización de productos o prestación de servicios.*
>
> *§ 1° Producto es cualquier bien, móvil o inmóvil, material o inmaterial.*
>
> *§ 2° Servicio es cualquier actividad ofrecida en el mercado de consumo, mediante remuneración, inclusive las de naturaleza bancaria, financiera, de crédito y de seguros, salvo las derivadas de las relaciones de carácter laboral."*
>
> *(...)*
>
> *"Art. 17. Para los efectos de esta Sección, se equiparan a los consumidores todas las víctimas del evento."*

Así, no hay que hablar de la posibilidad de permitir que el consumidor asuma el compromiso de la imposibilidad de la identificación de eventual usuario de Internet, así como no hay forma de obligar a los proveedores de aplicaciones de Internet a proveer el almacenamiento de las puertas de origen, teniendo en cuenta la ausencia de previsión legal.

De esa forma, es evidente la responsabilidad de los proveedores de conexión ante la imposibilidad de identificación de sus usuarios, por el art. 927, del Código Civil.

A pesar de lo ya expuesto, en caso de que sea determinado a proveedores de conexión, en sede de anticipación de tutela, el suministro de las informaciones acerca de determinado usuario y la orden sea imposible de ser cumplida ante la elección de utilización de la tecnología IP NAT para el abastecimiento de conexión a sus clientes de conjunto con la ausencia del almacenamiento de puertas de origen por los proveedores de aplicaciones, aún hay la posibilidad de la conversión de la imposibilidad del cumplimiento de la obligación de hacer en pérdidas y daños, con fundamento en el art. 499 del Nuevo Código de Proceso Civil.

> *"Art. 499. La obligación solamente será convertida en pérdidas y daños si el autor lo requiere o si es imposible la tutela específica o la obtención de tutela por el resultado práctico equivalente."*

Así, es evidente el riesgo al cual se exponen los proveedores de conexiones al suministrar acceso a Internet, más allá de sus posibilidades técnicas seguras, a sus clientes.

Conclusión

Ante todo lo expuesto, se puede decir que el suministro de internet a sus clientes por medio de la tecnología IP NAT es capaz de generar condenaciones por la vía judicial a los proveedores de conexión, sea por la responsabilidad objetiva (art. 927, del Código Civil) o por la conversión de la imposibilidad de la obligación de hacer en pérdidas y daños (art. 499, del Nuevo Código de Proceso Civil).

Tal responsabilidad no puede ser soslayada por el argumento de que la utilización de esta tecnología es una orientación de Anatel, puesto que la agencia realiza la recomendación de la tecnología con advertencias acerca de la individualización de los accesos a Internet.

Tampoco merece prosperar el argumento utilizado por los proveedores de conexión de que "bastaría que los proveedores de aplicaciones almacenasen las puertas de origen" para que el problema fuese resuelto, ya que se demostraría grave afronta al principio de la legalidad, positivado en el art. 5, inc. II, de la Constitución Federal, teniendo en cuenta la falta de obligación legal para este almacenamiento.

> *"Art. 5º Todos son iguales ante la ley, sin distinción de cualquier naturaleza, garantizándose a los brasileños y a los extranjeros residentes en el País la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los términos siguientes:*
>
> *II - nadie será obligado a hacer o dejar de hacer alguna cosa si no en virtud de ley."*

De esa forma, en caso de que entiendan por la inequívoca necesidad de almacenamiento de las puertas de origen por el proveedor de aplicación, de conexión o aún por ambos, la salida jurídica es la presentación de nuevo proyecto de ley, pues modificaciones a las definiciones dispuestas en el artículo 5º de la Ley 12.965/2014 no están en la pauta de la reglamentación del Marco Civil de Internet.

Además, la solución técnica es la adopción definitiva e inminente del protocolo IPv6 en detrimento del protocolo IPv4 y de la medida anodina utilizada actualmente por los proveedores de conexión, objeto del presente estudio y que trae riesgos a los propios proveedores, así como a toda la sociedad, al aumentar la sensación de impunidad en Internet.

Por último, queda demostrado el riesgo jurídico inobservado o ignorado por los proveedores de conexión en caso de utilización de la tecnología IP NAT para el suministro de internet a sus clientes, así como el riesgo de la ineficacia de las decisiones judiciales, teniéndose en cuenta la presumible imposibilidad de la identificación de autoría de acciones cometidas en la Red Mundial de Computadoras.

REALIDAD AUMENTADA: ¿FICCIÓN JURÍDICA?

Márcio Mello Chaves

El constante desarrollo de los dispositivos electrónicos personales ha posibilitado la presencia de la Realidad Aumentada[80] de forma cada vez más notable en la vida moderna. El acceso a bajo costo a computadoras personales, cámaras digitales, *tablets* y *smartphones* con un significativo poder de procesamiento de datos está acercando la realidad antes restringida a ficciones científicas a nuestro día a día.

Mientras la Realidad Virtual intenta recrear mundos que se asemejen al nuestro, como en los premiados filmes *Avatar* y *Matrix*, la Realidad Aumentada llega para invertir esa situación, introduciendo una nueva gama de informaciones en la realidad que ya conocemos, estando presentes en productos innovadores dirigidos al consumidor final.

Esa tecnología viene siendo empleada en diversas industrias, entre ellas: (i) en el comercio electrónico, donde usuarios pueden "probarse" ropas y accesorios usando su webcam; (ii) en el entretenimiento, en especial la millonaria industria de los videojuegos y transmisiones deportivas, donde el jugador pasa a utilizar su propio cuerpo como *joystick*; (iii) en la publicidad, donde anunciantes insertan los logotipos de sus marcas y slogans en ambientes públicos; sin hablar (iv) de los proveedores de acceso y contenido que distribuyen gafas que permiten la visualización de

[80] Término derivado de la expresión en inglés *augmented reality*, término supuestamente acuñado por el investigador de Boeing, Tom Caudell, en 1990.

diversos servicios que interactúan con el mundo real, e incluso (v) en las herramientas y funcionalidades empleadas desde la industria automotriz y aeronáutica hasta dispositivos médicos, como guantes especiales utilizados en el manejo de piezas virtuales y del propio cuerpo humano en cirugías a distancia.

Pero, en definitiva, ¿qué es la Realidad Aumentada? Según el concepto creado por Ronald Azuma[81], la Realidad Aumentada "*es un ambiente que comprende tanto realidad virtual como elementos del mundo real, creando un ambiente mixto en tiempo real*".

Por más ficticio y virtual que pueda parecer ese ambiente mixto, creado en tiempo real, la propia definición de lo que es la Realidad Aumentada permite que vislumbremos inevitables reflejos en el mundo jurídico, de acuerdo con el contenido digital que es introducido en el mundo real, siendo motivo de preocupación en diversas áreas del Derecho.

En los derechos de Propiedad Intelectual, valen los mencionados ejemplos de inserción de logotipos de marcas en un lugar público, como en una instalación de mobiliario urbano o incluso en un monumento natural. ¿Podría la conocida cadena de supermercados proyectar su logotipo de marca en el famoso monumento natural del Pan de Azúcar en Río de Janeiro, por medio de una aplicación que se vale de la Realidad Aumentada para exponer al consumidor a su marca? O, aún más, ¿podría un competidor valerse del mismo monumento para exhibir su propio logo en alusión a la marca de la empresa competidora? Tales situaciones traen a colación cuestiones que involucran los derechos marcarios[82] y la propia

[81] Científico e investigador renombrado en el medio de la Realidad Aumentada.

[82] Artículo 130 de la Ley de Propiedad Industrial (LPI): "*Al titular de la marca o al depositante le es además asegurado el derecho de: I - ceder su registro o pedido de registro; II - licenciar su uso; y III - velar por su integridad material o reputación.*"

competencia[83], y encuentran en las legislaciones específicas limitaciones de uso para asegurar los derechos de sus detentores.

Otros importantes derechos de propiedad intelectual que pueden ser afectados son los derechos sobre los dibujos industriales[84] y los derechos autorales[85]. Así, la utilización de formas tridimensionales protegidas, como dibujos industriales de embalajes de productos de una famosa marca de refrescos, obras visuales de un conocido pintor protegidas por derechos autorales e incluso los trazos arquitectónicos de un renombrado

[83] El artículo 195 de la LPI enumera diversas situaciones que caracterizan a la práctica de la competencia desleal, entre ellas aquel que: *I - publica, por cualquier medio, falsa afirmación, en detrimento de competidor, con el fin de obtener ventaja;*
II - presta o divulga, acerca de competidor, falsa información, con el fin de obtener ventaja;
III - emplea medio fraudulento, para desviar, en provecho propio o ajeno, clientela de otro;
IV - usa expresión o signo de publicidad ajenos, o los imita, de modo que se cree confusión entre los productos o establecimientos;
V - usa, indebidamente, nombre comercial, título de establecimiento o insignia ajenos o vende, expone u ofrece para venta o tiene en stock de producto con esas referencias;
VI - sustituye, por su propio nombre o razón social, en producto de otro, el nombre o razón social de este, sin su consentimiento; VII – se atribuye, como medio de publicidad, recompensa o distinción que no obtuvo;
VIII - vende o expone u ofrece para venta, en recepción o involucramiento de otro, producto adulterado o falsificado, o de él se vale para negociar con producto de la misma especie, aunque no adulterado o falsificado, si el hecho no constituye crimen más grave;
IX - da o promete dinero u otra utilidad a empleado de competidor, para que el empleado, faltando al deber del empleo, le proporcione ventaja;
X - recibe dinero u otra utilidad, o acepta promesa de paga o recompensa, para, faltando al deber de empleado, proporcionar ventaja al competidor del empleado;
XI - divulga, explota o se vale, sin autorización, de conocimientos, informaciones o datos confidenciales, utilizables en la industria, comercio o prestación de servicios, excluidos aquellos que sean de conocimiento público o que sean evidentes para un técnico en el asunto, a que tuvo acceso mediante relación contractual o laboral, incluso después del término del contrato;
XIII - vende, expone u ofrece a la venta producto, declarando ser objeto de patente depositada, o concedida, o de dibujo industrial registrado, que no lo sea, o mencionarlo, en anuncio o papel comercial, como depositado o patentado, o registrado, sin serlo;
Pena - detención, de 3 (tres) meses a 1 (un) año, o multa.

[84] El artículo 195 de la LPI garantiza la protección al dibujo industrial, así considerado como "*la forma plástica ornamental de un objeto o el conjunto ornamental de líneas y colores que pueda ser aplicado a un producto, proporcionando resultado visual nuevo y original en su configuración externa y que pueda servir de tipo de fabricación industrial.*"

[85] La Ley de los Derechos Autorales – LDA - (Ley Federal 9.610/1998) define en el art. 7º que: "*son obras intelectuales protegidas las creaciones del espíritu, expresas por cualquier medio o fijadas en cualquier soporte, tangible o intangible, conocido o que se invente en el futuro*."

arquitecto, sin la debida autorización de sus legítimos detentores, exponen a quien las utiliza a riesgos resultantes del uso indebido.

Aun en el ámbito de los derechos de Propiedad Intelectual, vale destacar que el nivel de interacción de los objetos virtuales introducidos en el mundo real también involucra complejos lenguajes computacionales, ciertamente protegidos por derechos de *software*[86]. Aquí, la inserción de códigos de programación que resulten en la interacción de un videojuego con usuarios del mundo real encontrará reflejos que sobrepasan el mundo virtual.

A pesar de ser diversos los ejemplos de interferencia de la Realidad Aumentada en los derechos de Propiedad Intelectual, las implicaciones no terminan ahí: también son innegables las afectaciones a diversos otros derechos, desde el derecho de imagen hasta la propia privacidad.

La Constitución de la República define en su artículo 5º, X que "*son inviolables la intimidad, la vida privada, la honra y la imagen de las personas*", asegurando derecho a la indemnización por cualquier daño material o moral que sea resultante de esa violación. Bajo ese prisma, la inserción de informaciones privadas de habitantes de determinado lugar en mapas electrónicos, por ejemplo, *Google Maps* o *iOS Maps*, violan derechos de privacidad. Así como la utilización de la Realidad Aumentada en la creación de un avatar ridículo para sustituir la imagen de determinado político opositor durante una disputa electoral puede resultar en la violación de la honra.

Esos son sólo algunos ejemplos de cómo la tecnología puede afectar esos derechos individuales.

[86] Ley del Software (9.609/1998): *Art. 1º: Programa de computadora es la expresión de un conjunto organizado de instrucciones en lenguaje natural o codificado, contenido en soporte físico de cualquier naturaleza, de empleo necesario en máquinas automáticas de tratamiento da información, dispositivos, instrumentos o equipos periféricos, basados en técnica digital o análoga, para hacerlos funcionar de modo y para fines determinados.*

Diversas son las aplicaciones del uso de la Realidad Aumentada, de la misma forma que diversas también son las consecuencias de ellas derivadas, que repercuten en diversos institutos del derecho, inclusive en el derecho penal[87]. Su utilización por los actuales medios tecnológicos y en las más variadas finalidades demanda cautela para evitar la violación de derechos de terceros, generando pasivos muchas veces desconocidos o desestimados. Así, el debido análisis de riesgo de la utilización de la Realidad Aumentada frente a la legislación vigente resulta de gran valía para que el uso de esa fascinante tecnología no la convierta en un problema bastante real para quien la utiliza.

GOOGLE: ¿STANDARD OIL DE NUESTROS TIEMPOS?

Milena Mendes Grado

En noviembre de 2014, el parlamento europeo aprobó una resolución aconsejando a la Comisión Europea a adoptar un proyecto para forzar una escisión de los servicios de búsqueda de los demás servicios de grandes empresas, como Google. En principio, para imponer una escisión, es necesario que la empresa a la cual se imponga la escisión esté actuando deslealmente, influyendo sobre el mercado consumidor de forma negativa, o sea, es necesario que haya un monopolio ilícito. Resta, entonces, saber si las conductas de esas empresas son efectivamente ilícitas.

Recientemente, en 2017, fue aplicada una multa billonaria a Google en Europa teniendo en cuenta prácticas de competencia ilícitas, por favorecimiento a través su sistema de búsquedas del comparador de precios que también le pertenece.

En 1909, los Estados Unidos procesaron a la compañía Standard Oil, que era presidida y controlada por John Rockefeller. En 1904, la compañía

[87] La violación de los derechos de Propiedad Industrial, Derechos Autorales y Programas de Computadora, por ejemplo, imponen penas que van hasta 1 año de detención, sin perjuicio de la indemnización por los daños causados.

detenía el 91% (noventa y un por ciento) del control de la producción de petróleo y el 85% (ochenta y cinco por ciento) de las ventas finales. Las autoridades concluyeron que la posición dominante de Standard Oil era consecuencia de prácticas desleales como disminución de precios en ciertos lugares para suprimir empresas competidoras, contratos que impedían el libre comercio, espionaje, monopolio de la infraestructura, entre otros. A pesar de fomentar la Era de Oro americana, así como Standard Oil, otras empresas también fueron procesadas por el Estado en base al Sherman Antitrust Act, creado por John Sherman, con el objetivo de proteger la libre competencia.

La decisión del parlamento europeo y de la Comisaría Europea para la Competencia busca impactar, principalmente, a Google, que detiene más del 90% (noventa por ciento) del servicio de búsqueda. Está muy claro que Google es la Standard Oil de los días de hoy en lo que se refiere al dominio del mercado, sólo que a un nivel global. Y el día a día sólo comprueba eso, ya que es común que las personas se pregunten "¿cómo yo hacía eso antes de Google existir?".

Es incuestionable que los servicios de búsqueda prestados por Google son de infinita utilidad, pudiendo ser considerados, inclusive, servicios de utilidad pública. En otras palabras, son servicios que adquieren tal relevancia para la colectividad y que pueden ser prestados directamente por conveniencia por el Estado o por medio de concesión o permiso, pero que, no obstante, son destinados a la utilización directa del individuo.

De hecho, en Brasil, el Marco Civil de Internet, Ley nº 12.965/2014 considera, en su artículo 7º, a Internet como indispensable para el ejercicio de la ciudadanía y en la actual coyuntura, Google es indisociable del concepto que tenemos y del uso que hacemos de Internet, razón por

la cual es necesario evaluar a Google bajo una perspectiva de interés público versus privado.

Muchos servicios de utilidad pública admiten un monopolio natural porque dependen de una fuerte infraestructura y la construcción de una nueva infraestructura para fines competitivos no compensa, pero esos monopolios naturales la mayoría de las veces están regulados por el Estado.

Para el Parlamento Europeo, la cuestión es que los servicios de búsqueda de Google, directa o indirectamente, están asociados a otros de fin totalmente comercial, y se sospecha que el servicio de búsqueda privilegie sus propios productos en los resultados de búsquedas. Además, nada impide que algunos servicios de terceros también sean favorecidos en detrimento de otros, o sea, que el buscador controle lo que es proporcionado a sus usuarios.

Aparentemente, eso puede no ser considerado una práctica desleal, porque se trata de una empresa favoreciendo sus propios productos, y no hay nada más común. Además, el mercado está abierto para que otros buscadores se desarrollen.

En este punto es importante trazar un paralelo con la Standard Oil. La empresa no comenzó como una superpotencia, esa posición en el mercado fue conquistada de varias formas que hoy son indiscutiblemente ilícitas y que en aquella época aún no estaban normadas. La Standard Oil construyó una infraestructura de oleoductos, entre otros, indispensable para el progreso de Estados Unidos, o sea, el servicio inicialmente prestado pasó a ser fundamental para la población. Ocurre que, al mismo tiempo que ese servicio era prestado buscando atender a la población, pasó también a ser utilizado para ampliar la hegemonía de la empresa.

Vale destacar, no obstante, que las prácticas adoptadas por la Standard Oil son muy diferentes a las adoptadas por Google. Sin embargo, es muy importante recordar que las épocas son diferentes, nuevos modelos de negocios surgieron y prácticas comerciales evolucionaron, así como la tecnología.

Google es el modelo de servicios disponible, a pesar de otras empresas intentar establecer competencia. El hecho es que las reglas aplicadas para ese tipo de servicio son las reglas utilizadas por el propio Google. Pero ¿esas prácticas pueden ser consideradas legales?

La intención de este artículo no es demonizar a Google, muy al contrario, los beneficios públicos conjugados a los servicios prestados por Google son tantos que sobrepasaron los límites privados. Ante eso, deben ser permeados de imparcialidad y transparencia y tal vez, una de las formas de alcanzar esos parámetros, sea una escisión del buscador de otros servicios.

Asimismo, mucho más allá de ser un servicio de utilidad pública, Google lidia con informaciones muy preciosas para la humanidad, por ejemplo, creatividad, conocimiento y privacidad. Y, en este punto es que parecen estar concentrados los mayores problemas.

Los riesgos de un monopolio de esa naturaleza no están limitados al favorecimiento de los propios servicios, sino que también están relacionados al control del acceso a la información y al control de la privacidad. Cuanto más Google desarrolle nuevos productos, más esas informaciones son aglutinadas y más el individuo pierde la libertad de elección, teniendo en cuenta que el individuo es conducido a los contenidos relacionados con sus búsquedas anteriores. Además, donde

quiera que él esté y lo que sea que haga, puede ser identificado por una única empresa.

Para ejemplificar ese control, hoy para que un contenido en Brasil sea removido de cualquiera de los servicios de Google, es necesario una orden judicial. Se pretendió que eso fuese así, y no por simple notificación extrajudicial, para que no correspondiese al Notificante el poder de decisión sobre conceptos subjetivos como ofensa, prejuicio, etc. Sin embargo, de acuerdo con los propios términos de uso de Google, este puede remover un contenido que no esté de acuerdo con sus reglas. Así, el Notificante no puede tener el poder para definir esos conceptos subjetivos, pero Google puede.

Puede hasta ser que las conductas de Google, a priori, no sean ilícitas del todo, pero ¿cuáles son los riesgos de que este administre y controle una cantidad inmensa de informaciones? ¿Hay mayor interferencia y coerción que esa? Así, como la empresa es un cuarto poder, ¿no sería el servicio de búsquedas un nuevo poder? En todo el mundo, mercados importantes para la población son regulados para evitar el control sólo por una empresa, como energía y telecomunicaciones. Entonces, ¿cuál es la razón para no regular el mercado de la tecnología? La respuesta, normalmente, es libertad, pero ¿no se está violando la libertad de elección?

PLANEAMIENTO TRIBUTARIO PARA NEGOCIOS DIGITALES

Márcio Mello Chaves

No es novedad para nadie que el mundo de los negocios se mueve a una velocidad extrema, donde surgen nuevos modelos y estructuras a cada

momento. Desde el *boom* de las puntocom ocurrido en los años 2000, hemos visto un continuo desarrollo de los modelos de negocios *online*, con ofertas de productos y servicios cada vez más innovadores, desafiando, principalmente, la definición de las reglas jurídicas aplicables a cada uno de ellos.

En ese escenario, no sería razonable imaginar que el legislador deba tener un poder que roce el de un médium para prever, antes incluso de cualquier evento, las relaciones que de allí se derivarán para, de esa forma, ser capaz de prescribir las conductas esperadas de los seres humanos. Existiendo esa dificultad para definir qué regla jurídica es aplicable a la propia definición de determinado negocio, identificar la regla que define los efectos tributarios de ese negocio es una tarea todavía más difícil. Esto ocurre porque, si es difícil para el propio derecho privado definir la propia naturaleza de un negocio, ¿qué se dirá de definir las reglas tributarias a él aplicables con reflejos en la esfera pública?

Tenemos como ejemplo los sitios de compras colectivas, que causaban dudas en cuanto a la real naturaleza del servicio prestado por el sitio de compras colectivas, si estos serían una mera intermediación de negocios entre consumidor y el efectivo prestador/proveedor. Otros casos más recientes, como la promoción de ventas de productos de minoristas en perfiles de redes sociales, generando el recibimiento de valores y beneficios a título de comisión, también traen a colación discusiones relacionadas al efecto tributario a las operaciones realizadas. Ante esas cuestiones, ¿serían los valores recibidos y repasados ingresos propios y, así, deben ser tributados, en su integralidad, por los sitios, como es el caso del PIS/COFINS? ¿O los valores tributables en el ambiente del sitio serían sólo aquellos restantes después del repaso? ¿Sería el ingreso tributable del sitio la integralidad de los valores que transitaron por su

caja o sólo aquella parcela que se refiere a su comisión por la intermediación del negocio?

Además, en un mercado extremadamente competitivo como el digital, la adopción de reglas tributarias más blandas puede ser fundamental para la viabilidad del negocio como un todo, sea por propiciar un menor costo tributario, sea por evitarse la sujeción a riesgos fiscales innecesarios que pueden comprometer la salud financiera de cualquier negocio.

Así, ante las indefiniciones e incertidumbres que permean la conducción de los negocios *online*, es fundamental pensar el modelo de negocio a ser implantado, no sólo bajo la perspectiva comercial, sino también bajo la perspectiva tributaria. El concepto de planeamiento tributario debe ser asociado a todos los modelos de negocios *online*, independientemente de su dimensión, con el fin de obtener una mejor eficiencia fiscal. A fin de cuentas, todo tipo de negocio comporta un análisis previo sobre cuál es la mejor estructura a ser escogida bajo la perspectiva del costo tributario.

METATAGS Y PUBLICIDAD FRAUDULENTA

Milena Mendes Grado

En decisión del 11 de julio de 2013[88], el Tribunal de Justicia de la Unión Europea decidió que el uso de metatags irreales y fraudulentas en páginas en internet configura publicidad engañosa. No hay precedentes judiciales latinoamericanos en ese sentido y a pesar de la utilización de metatags no ser novedad, esa puede ser una nueva arma para cohibir la competencia desleal, violación de marca, así como el irrespeto al consumidor.

Las metatags son informaciones y palabras clave (keywords) insertadas en el código fuente de la página de internet (webpage) con la finalidad de brindar a los mecanismos de búsqueda datos sobre el contenido de esa página. Esas informaciones y palabras clave facilitan, por tanto, la

[88] Fuente: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62011CJ0657:PT:HTML, acceso en 29/11/2013 a las 14:23

indexación de acuerdo con los intereses de localización del autor de la página. De esa forma, el autor de la página puede intentar manipular el sistema de búsqueda insertando palabras claves que no coinciden con el contenido real, para que sea más fácilmente indicado en resultados de búsqueda de estos mecanismos, además, puede intentar eludir a los "crawlers" repitiendo las mismas palabras, verdaderas o no, para ganar mayor realce en los resultados. Vale resaltar, no obstante, que, en cuanto a esa última técnica, los sistemas de búsqueda más conocidos ya poseen recursos que identifican esa repetición y no muestran la página.

Es incuestionable la importancia de los mecanismos de búsqueda como herramienta de marketing. Entre los tres sitios más accedidos en Brasil, dos son mecanismos de búsqueda[89]. Además, normalmente los e-consumidores, aquellos que hacen compras on-line, navegan en buscadores antes de efectuar las compras[90]. Ante eso, tener realce en los resultados de las búsquedas de los motores puede ser una gran ventaja competitiva en el mercado.

El caso concreto que motivó la decisión del Tribunal de Justicia de la Unión Europea trataba de una disputa entre empresas que fabricaban máquinas y líneas de elección automática con tecnología a láser, siendo que la Rea utilizaba como metatags de su sitio el nombre de los productos de la Autora.

La decisión, entre otras cuestiones, discutió si el concepto de publicidad definido en el artículo 2º, n° 1, de la Directiva 84/450/CEE, del Consejo, modificada por la Directiva 2005/29/CE del Parlamento Europeo de conjunto con el Consejo, así como en el artículo 2º, apartado "a", de la Directiva 2006/114/CE del Parlamento Europeo y del Consejo incluía la utilización de metatags.

[89]Fuente:http://www.infomoney.com.br/minhas-financas/gadgets/noticia/2961393/sites-mais-acessados-brasil-segundo-site-alexa, acceso en 29/11/2013 a las 14:05

[90] Fuente: http://www.ibope.com.br/pt-br/conhecimento/artigospapers/Paginas/Fluxo-de-navegacao-dos-internautas-para-sites-de-comercio-eletronico-brasileiro.aspx, acceso en 29/11/2013 a las 14:16

Esos artículos definen como publicidad cualquier forma de comunicación hecha en el ámbito de una actividad comercial, industrial, artesanal o liberal, teniendo como objetivo promover el suministro de bienes o de servicios. El Tribunal entendió que ese concepto abarcaba medios indirectos de comunicación cuando son susceptibles de influir en el comportamiento económico del consumidor y afectar al competidor, situación que se entendió que estaba ocurriendo de hecho, en la medida en que en la búsqueda de productos de la Autora, aparecía el sitio de la Rea en el resultado de la búsqueda, a continuación de la Autora, pudiendo el consumidor entender el resultado como una alternativa a los productos de la Rea o como si el sitio de la Rea comercializase los productos de la Autora.
De ese juicio podemos entender que la metatag por sí sola no puede ser publicidad. No obstante, cuando la intención de la metatag es incentivar el consumo y desviar la clientela no es sólo publicidad, sino publicidad engañosa.

Ese entendimiento está en correspondencia con el ordenamiento jurídico latinoamericano y puede ser adoptado por la jurisprudencia. El Código de Defensa del Consumidor brasileño en su art. 37, párrafo primero, aduce que "es engañosa **cualquier modalidad de información o comunicación de carácter publicitario**, entera o parcialmente falsa, o, por cualquier otro modo, incluso por omisión, **capaz de inducir a error al consumidor** respecto a la naturaleza, características, calidad, cantidad, propiedades, origen, precio y cualquier otro dato sobre productos y servicios". Según Lucia A. L. de Magalhães Dias[91], la publicidad es la forma clásica de dar a conocer un producto, un servicio o una empresa con el objetivo de despertar el interés por la cosa anunciada, crear prestigio para el nombre o para la marca del anunciante o, incluso, difundir cierto estilo de vida. En ese mismo sentido, en los demás países latinoamericanos, la publicidad engañosa es aquella que de cualquier

[91] DIAS, Lucia Ancona Lopez de Magalhães. Publicidade e Direito. São Paulo: Editora Revista dos Tribunais, 2010, p. 23

manera puede inducir al consumidor a error, afectando su comportamiento económico. La metatag cuando busca instigar al consumidor es una modalidad de información o comunicación de carácter publicitario y cuando busca infringir la lealtad competitiva induce al consumidor a error.

Además, es indiscutible que cuando la metatag engañosa busca desviar la clientela, se cuida de competencia desleal, como dispone la Ley de Propiedad Industrial Brasileña (art. 195), siendo esta conducta similar a la compra de adwords que notoriamente pertenezcan a un competidor, como fue decidido por el TJ/SP:

> *"Considerando que ambas empresas actúan en el mismo ramo comercial, tal práctica es manifiestamente abusiva, ya que posibilita a la rea desviar la clientela que busca específicamente los productos comercializados por la autora, beneficiándose injustamente del prestigio que la marca de esta goza en el mercado. No se discute, por tanto, la ilicitud de la conducta, bien cohibida con la fijación de multa conminatoria." TJ/SP. Apelación n°990.10.127612-7. Relator: Enio Zuliani. 23/09/2010.*

Ese mismo entendimiento es aplicado también en los demás países latinoamericanos, por ejemplo, en Chile[92].

Es posible también argumentar que hay violación marcaria, ya que la Rea estaba utilizando la marca de los productos del Autor como metatag, sin embargo, ese entendimiento no está totalmente consensuado, hay opiniones en el sentido de que por tratarse de una violación "invisible" no estaría infringiendo la protección marcaria.
Por tanto, las empresas pueden exigir que sus competidores alteren sus metatags cuando son fraudulentas o engañosas y causantes de desvío de clientela, o que dejen de usar signos que pertenezcan a terceros. Como

[92] Acepta.com S.A con South Consulting (2013), Corte de Apelaciones de Santiago, Segunda Sala, rol 484-13, 24 de marzo de 2014.

las metatags no son visibles y pueden ser alteradas, habiendo sospecha, es necesario que haya una preservación de prueba. Así, lo ideal es hacer un print de la pantalla mostrando el *view source*, así como conseguir un acta notarial que compruebe la forma de aparición en los resultados de los mecanismos de búsqueda. Con esos indicios, si es necesario, es posible, además, requerir judicialmente una medida cautelar de producción anticipada de prueba para, posteriormente, entrar con la acción para la remoción e indemnización por eventuales daños.

Además, es posible hacer una denuncia a los órganos reguladores por publicidad engañosa. La punición por publicidad engañosa puede ser una estrategia adoptada por el perjudicado a fin de que la eventual condenación del infractor tenga efectos más amplios, alcanzando no sólo a los involucrados, sino también a una colectividad de consumidores.

CAPÍTULO IX

LOS LÍMITES DEL ESPIONAJE Y DE LA PRIVACIDAD EN LAS REDES DE COMUNICACIÓN

QUÉ PUEDEN HACER LAS EMPRESAS ANTE EL ESPIONAJE DE ESTADOS UNIDOS

Caroline Teófilo da Silva

Con la revelación hecha por *Edward Snowden* acerca del monitoreo realizado por Estados Unidos por medio de programas de vigilancia, el diario norteamericano *Washington Post*[93] publicó los dos principales mecanismos de espionaje utilizados por la NSA – *National Security Agency*:

[93] Fuente del Reportaje: [http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/]. Acceso en 28.08.2013.

- *"Upstream"*, que recolecta los datos transmitidos vía internet a través de los cables de fibra óptica que conectan a América del Norte al resto del mundo;

- "*Prism*", que recolecta las informaciones de las empresas americanas proveedoras de aplicaciones de internet, por ejemplo, Microsoft, Google, Facebook, YouTube y Apple.

Siendo así, fueron identificadas tres formas de monitoreo. La primera está relacionada con la infraestructura física de las redes, ya que gran parte de las informaciones que circulan por internet pasa por Estados Unidos, que mantiene la gran mayoría de los servidores raíz.

La otra forma está relacionada con la facultad lógica y posee una justificación legal. La legislación americana, *CALEA – Communications Assistance for Law Enforcement Act*[94], obliga a la instalación de *backdoors* en las redes de telecomunicaciones americanas, a fin de permitir interceptaciones por las agencias de inteligencia de Estados Unidos. Debido a la obligación legal, todas las operadoras de telecomunicaciones y fabricantes de equipos de computación deben instalar en sus equipos *backdoors* que permitan el acceso remoto del gobierno americano a los datos intercambiados.

Y, por último, como gran parte de la población usa internet y está en las redes sociales, los proveedores de internet constituyen la tercera forma de espionaje. Sólo no conseguimos afirmar, todavía, si los datos son proporcionados por las empresas o si son recolectados a través de *backdoors* directamente por el gobierno americano.

[94] Fuente de la Legislación: http://askcalea.fbi.gov/calea/. Acceso en 28.08.2013.

El caso de espionaje trajo algunas preocupaciones, en gran parte relacionadas a la protección de la privacidad de los individuos y de las informaciones corporativas, principalmente cuando hablamos de *cloud computing* y redes sociales, ya que, no solamente los individuos, sino las empresas utilizan estos ambientes.

Brasil también fue señalado como uno de los países monitoreados por el gobierno norteamericano, siendo las empresas de telecomunicaciones nacionales acusadas de cooperar con empresas de telefonía estadounidenses.

Así, el exministro de relaciones exteriores, Antônio Patriota, solicitó que el gobierno americano "detuviese" el espionaje. No obstante, los Estados Unidos alegan que mantendrán el monitoreo para rastrear posibles amenazas terroristas, como forma de protección a los ciudadanos americanos y de todo el mundo, en base al *USA Patriot Act*[95], sección 215, que permite el monitoreo cuando es relevante para una investigación nacional.

Paralelamente, pero de manera bastante modesta, las medidas adoptadas por Brasil fueron:

1. verificar si las empresas de telecomunicaciones con sede en Brasil violaron el secreto de comunicaciones telefónicas, previsto como crimen en la Ley de Interceptación Telefónica (Ley 9.296, de 24 de julio de 1996) y en la Ley de Soberanía Nacional, art. 13, I (Ley 7.170, de 14 de diciembre de 1983), sea a través de la compartición de informaciones o por medio de su infraestructura tecnológica;

2. incluir una disposición en el Marco Civil de Internet que obligue a las empresas extranjeras proveedoras de aplicaciones de internet a

[95] Fuente de la Legislación: [http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf]. Acceso en 28.08.2013.

mantener los datos de los brasileños en *data centers* localizados en territorio nacional;

3. pedir justificaciones a Estados Unidos sobre todo lo que fue espiado, además de reclamar ante el Consejo de Seguridad de la ONU.

Pero ¿todo eso hará que cese el monitoreo realizado por Estados Unidos o protegerá los datos de los ciudadanos y de las empresas brasileñas? Probablemente, no.

El Marco Civil de Internet no va a resolver el problema del espionaje de datos si no prohíbe la replicación. A pesar de las empresas estar obligadas a mantener los datos en Brasil, nada les impide tener una copia de estos dados en sus países de origen, o viceversa. En caso de que eso no ocurra, es posible afirmar que el monitoreo no afectó en nada al Marco Civil, tan sólo aceleró su aprobación.

Con relación al *Cloud Computing* (computación en la nube), la gran incidencia del monitoreo realizado por Estados Unidos puede disminuir temporalmente su utilización o desalentar nuevos contratos. Sin embargo, se cree que no acabará o reducirá considerablemente su uso. Tal vez, los usuarios de la nube opten por utilizar empresas cuyas bases de datos no están localizadas en Estados Unidos y el tránsito no pase por allí.

Las empresas de telecomunicaciones, por su parte, y el gobierno están preocupados por su infraestructura tecnológica, dado que muchos de los equipos utilizados son adquiridos de empresas norteamericanas que están sujetas a aquella legislación. Por tanto, no se puede garantizar que estas

mismas empresas fabriquen equipos distintos para atender a diferentes legislaciones.

Pero, en términos prácticos, ¿cuál es la mejor forma de mitigar los riesgos de las actividades de espionaje? A continuación, siguen algunas sugerencias a ser observadas:

Cloud Computing

Antes de contratar servicios de *Cloud Computing,* considere qué informaciones pueden ir a la nube (ej. solo informaciones internas o públicas) y qué tecnología será utilizada para garantizar la confidencialidad, disponibilidad e integridad de las informaciones, por ejemplo, la autenticación fuerte y encriptación de los datos, que pueden dificultar la acción de terceros en tener contacto con las informaciones.

Redes Sociales, Repositorios Digitales y Correo Electrónico

Se indica prohibir la compartición de informaciones confidenciales o críticas para el negocio en ambientes digitales fuera de la infraestructura tecnológica de la empresa, por ejemplo, repositorios en la *web*, correo electrónico particular o servicios en la nube de forma general.

Adicionalmente, los empleados deben ser orientados a no comentar con otras personas cuestiones relacionadas con la empresa, como rutinas de trabajo, agendas de compromiso, proyectos y datos de clientes en las

redes sociales, sea en *chats* habilitados por ellas, o incluso en redes sociales, para evitar así la filtración de informaciones.

Estas medidas pueden darse por medio de programas de capacitación en Seguridad de la Información, con la inserción de cláusulas en las normativas internas, en los contratos de trabajo y en los contratos con prestadores de servicios, además de la aplicación de directivas en los sistemas que impidan el acceso a ciertos sitios o servicios.

Encriptación

Se recomienda, además, que todas las informaciones confidenciales o críticas del negocio sean encriptadas antes del envío, a fin de dificultar el acceso por personas no autorizadas.

Estas medidas no impiden el monitoreo realizado por Estados Unidos o por terceros, pero son importantes para preservar la confidencialidad de las informaciones de la empresa y de los individuos, protegiendo sus activos y evitando incidentes.

¿EL ESPIONAJE DIGITAL ES LEGAL?

Patricia Peck Pinheiro

¿Qué es espionaje digital, en definitivas? ¿Qué cambió en el mundo del espionaje desde el episodio de Garganta Profunda, fuente secreta del *Washington Post* sobre el escándalo del Watergate, y más recientemente del caso Julian Assange y de Edward Snowden? ¿Y en el ámbito empresarial, que va desde casos como el de Madame Coco Chanel al Petrobras?

Enterarse de una información secreta obtenida de forma privilegiada sería el concepto básico de espionaje. A continuación, surge la relación de interés sobre la información, para quién esta pueda agregar valor y convertirse en un conocimiento. Por eso es que hoy el espionaje viene muchas veces asociado al concepto de filtración de información, que significa revelar a un tercero no autorizado una información secreta obtenida de forma legítima o clandestina, pero sin que su propietario sepa que esta sería compartida con otros o hecha pública.

A pesar del daño que el espionaje puede generar, es claro que existen casos excepcionales en que el fin justifica los medios, y que, si no fuese por el espionaje, las personas no tendrían cómo saber la verdad de los hechos.

Ahora bien, de acuerdo con manuales militares, espiar involucra directamente un servicio de inteligencia, o sea, de obtención de información. Y protegerse contra el espionaje implica un servicio de contrainteligencia, o sea, de seguridad de la información. Y uno no existe sin el otro. Esto pone en evidencia que formamos parte de la Sociedad del Conocimiento, donde estamos casi todo el tiempo espiando o siendo espiados. Es muy difícil mantener una posición totalmente neutra.

Siendo así, si el espionaje es una técnica, un *modus operandi* que hoy posee cada vez más herramientas tecnológicas para ser ejecutado, este representa poder y puede determinar el dominio político o económico de una institución sobre otra (en el caso de espionaje industrial o comercial) o incluso de un país sobre otro, llegando a generar, en este último caso, la propia guerra digital, que es la guerra de los datos.

Según un informe del FBI (www.ic3.gov), cuanto más conectados estamos, mayor es la posibilidad de que estemos siendo espiados

electrónicamente, lo que es facilitado por la falta de hábito de seguridad digital a nivel endémico-cultural.

Dicho eso, ¿cuándo un acto de espionaje entre países sería legítimo? ¿Habría una manera de hacer el espionaje legal? Véase los casos involucrando a Alemania, China, Estonia, Nueva Zelandia, Australia, India, Irán, Iraq y Rusia. ¿Cómo queda la legislación, no sólo de cada país, sino a nivel global?

Veamos el efecto 9/11 que generó el *Patriot Act* en los EUA, cuya sección 215 da poder jurídico para que la Autoridad Americana use cualquier medio que le permita tener acceso ilimitado a una información que pueda contribuir a la protección o seguridad nacional del país. En otras palabras, le da carta blanca para observar cualquier trasiego de datos que pueda ser relevante en una investigación para combatir amenazas a la seguridad nacional (que traducimos hoy como combate al terrorismo).

¿Qué significa eso para los demás países, incluso los aliados? Que el Congreso Americano (legislativo) creó una especie de cheque en blanco que afirma que prácticamente todo lo que sea contra los EUA es terrorismo. Vale resaltar que en Brasil no tenemos nada que se asemeje o se equipare a eso, todavía.

Bien, en cualquier momento de la historia humana es y siempre fue muy peligroso el uso de institutos como el del flagrante preparado, de la interceptación o incluso de la tortura, bajo la justificación de dar mayor seguridad a la colectividad, en caso de que no haya sido muy bien acompañado por el debido proceso legal para que no haya arbitrariedad de la autoridad ni abuso de poder.

En el ámbito privado, las leyes de hoy protegen mejor a las empresas contra el espionaje. Tenemos la previsión legal de varios crímenes, desde

la revelación de secreto por el art. 154 del Código Penal, el nuevo art. 154-A (aportado por la Ley 12.737/2012, más conocida como Ley "Carolina Dieckmann", que muestra el uso de información no autorizada de celebridad – ente privado), al crimen de interceptación previsto en la Ley 9.296/1996.

No obstante, en el ámbito público, especialmente entre países, hay una carencia de definición de reglas claras, de cómo será este juego político internacional, global, sin fronteras claras. Después de todo, ya no se espía al enemigo, sino a cualquiera, en cualquier lugar, en cualquier momento, en caso de que haya interés en hacerlo, o con el poder del *big data*, con tal de que haya poder de procesamiento para ello.

Hoy, basta con escanear internet y las redes sociales para descubrir secretos industriales, por ejemplo. Muchas veces eso no configura un acto de espionaje, pues este supone que el incidente sólo ocurre cuando la información está protegida, de la misma forma en que no es posible el crimen de invasión si la puerta está abierta. Si las personas publican todo, incluso sobre su rutina, horario, trayectos, proyectos, trabajo e incluso contenidos sobre otras personas, basta que alguien esté observando para descubrir esas informaciones.

Ciertamente, lo que cambió fue que acabó el glamur. De una navegación en Facebook al uso de un *sniffer* para buscar datos en una máquina ajena, banalizamos no sólo el espionaje, sino la propia información. El mejor combate al espionaje hoy involucra a la educación en seguridad de la información. Claro, se hace esencial celebrar un tratado internacional entre los países de la arena político-económica mundial actual para que sean definidas las nuevas reglas del juego. Desde el fin de la URSS y la caída del Muro de Berlín, no reestablecemos esas reglas. Ahora que todo el mundo juega contra todo el mundo, ¡el que caiga en la red es pescado!

DE LA INTERCEPTACIÓN TELEMÁTICA

Rafael Mott Farah

La constitución federal, en su artículo 5º, inciso XII, garantiza el secreto de los datos de comunicación, sean las comunicaciones por correspondencia, las comunicaciones telegráficas, las de datos o las comunicaciones telefónicas, permitiendo la ruptura de tal secreto – por medio de la Interceptación – sólo en algunas de estas hipótesis y con el cumplimiento de algunos requisitos.

Sobre el significado de interceptación, esta es la valiosa lección del maestro Araújo de Castro[96]:

> *"Interceptar es interrumpir el curso original, impedir el paso, siendo que en la ley tiene el sentido de captar la comunicación, conocer su contenido. Interceptar es tener contacto con el valor de la comunicación, no impidiendo que ella llegue a su destinatario."*

De tal suerte, prevé el art. 5º, XII de la Constitución Federal de Brasil, que "es inviolable el secreto de la correspondencia y de las comunicaciones telegráficas, de datos y de las comunicaciones telefónicas, salvo, en el último caso, por orden judicial, en las hipótesis y forma que la ley establezca para fines de investigación criminal o instrucción procesal penal".

Así, a pesar de entender que la excepción constitucional expresa se refiere sólo al último caso – comunicaciones telefónicas –, Alexandre de Moraes[97]

[96] ARAÚJO DE CASTRO, Carla Rodrigues. Crimes de Informática e seus aspectos processuais. Río de Janeiro: Lúmen Júris, 2001. p. 111 y 112.

[97] MORAES, Alexandre de. Direito Constitucional, Ed. Atlas. 28º ed., p. 59-60.

plantea que "ninguna libertad individual es absoluta, siendo posible, respetados ciertos parámetros, la interceptación de las correspondencias y comunicaciones telegráficas y de datos siempre que las libertades públicas estén siendo utilizadas como instrumento de salvaguarda de prácticas ilícitas".

Además, sobre el secreto de los datos informáticos, Alexandre de Moraes nos trae una preciosa lección:

> *"El precepto que garantiza el secreto de datos engloba el uso de informaciones derivadas de la informática. Esa nueva garantía, necesaria a causa de la existencia de una nueva forma de almacenamiento y transmisión de informaciones, debe coadunarse con las garantías de intimidad, honra y dignidad humanas, de forma que se impidan interceptaciones o divulgaciones por medios ilícitos".*

De la Interceptación Telemática

Es de suma importancia mencionar la discusión doctrinaria que comprende la posibilidad o no de la interceptación telemática, siendo verdad que la esencia principal de la discusión se deriva de la hermenéutica de la redacción constitucional, más específicamente sobre la expresión "(...) salvo, en el último caso, por orden judicial (...)".

Como alecciona el Profesor Marco Antônio de Barros[98] "si de un lado es imposible ignorar la veda constitucional y la superioridad del contenido de tal norma, de otro, es necesario encontrar una salida jurídica válida para impedir que la inviolabilidad del secreto de datos no se convierta en un serio estorbo para el buen desempeño de las actividades relacionadas con el descubrimiento de la verdad en el proceso penal".

[98] BARROS, Marco Antônio de. A Busca da Verdade no Processo Penal, 3. ed., atual. y ampl., São Paulo: ED. RT, p. 172.

Además, de acuerdo con el renombrado jurista, "durante muchos años, parte de la doctrina defendió que sólo puede haber autorización judicial para interceptación de comunicación telefónica, siendo inadmisible, por inconstitucional tal determinación para la interceptación de la correspondencia, telegrafía y de datos".

Liderada por Fernando da Costa Tourinho Filho[99], otra corriente doctrinaria pasó a sustentar que el inciso XII del art. 5º de la Constitución Federal, al tratar sobre el tema, habría hecho referencia a sólo dos hipótesis de inviolabilidad, pues la aposición de la coma entre las expresiones "comunicaciones telegráficas" y "datos" revelaría la existencia de dos casos distintos de inviolabilidad. De un lado la correspondencia (física) y las comunicaciones telegráficas y del otro los datos y las comunicaciones telefónicas.

Así, de acuerdo con Marco Antônio de Barros[100], cuando el texto legal plantea "salvo en el último caso", también estaría comprendida la posibilidad de autorizarse judicialmente la interceptación de la transmisión de datos por tercera persona. De esta forma, con apoyo en la Ley 9.296/1996, no habría impedimento a la ruptura del secreto de datos, siempre que sea autorizada judicialmente, para fines de persecución o investigación penal.

Siguiendo la misma línea de raciocinio del renombrado Procurador de Justicia, la protección del secreto de datos encuentra los mismos límites que la protección al secreto de la comunicación telefónica.

No obstante, ninguna de las dos corrientes logró establecer un fin al conflicto existente en la doctrina entre la garantía individual de manutención del secreto de datos contra el interés público, que se

[99] TOURINHO FILHO, Fernando da Costa. Processo Penal, 25. São Paulo: Saraiva, 3. ed., p. 232.

[100] BARROS, Marco Antônio de. A Busca da Verdade no Processo Penal, 3. ed., atual. y ampl., São Paulo: Ed. RT, p. 172.

encuentra traducido en la investigación criminal o en la instrucción procesal penal.

Ante lo expuesto, sobrevino además una tercera corriente doctrinaria, liderada por Tércio Sampaio Ferraz Junior[101], según el cual, entre los cuatro medios de comunicación mencionados en la Carta Magna, solamente en el telefónico es que se configura la instantaneidad, he aquí que este sólo es "mientras ocurre", no dejando vestigios de su contenido cuando termina, posibilitando, a posteriori, sólo la obtención del contenido de la comunicación y no la comunicación en sí.

Además, de la argumentación del doctrinador Tércio Sampaio de Arruda, se extrae que la Constitución no habría hecho ninguna reserva a las otras modalidades de comunicación porque se vislumbra la posibilidad de obtención de pruebas en base a los vestigios dejados por ellas. Y concluye, afirmando que es técnicamente posible al constituyente no permitir, en absoluto, la interferencia de terceros en el flujo comunicativo, lo que no induce, necesariamente, a que no se pueda tener acceso, posteriormente, a la identificación de los sujetos y al relato de los mensajes publicados siempre que el interés público así lo exija.

En síntesis, concluye Tércio Sampaio que lo que nuestra Carta Magna veda es la interceptación de la correspondencia electrónica, pero no la autorización judicial para su búsqueda, en momento posterior a que ocurra.

Sin embargo, un punto que debe ser tenido en consideración es el principio inherente a las pruebas cuando estas se tratan de pruebas digitales. Tal principio es llamado "orden de volatilidad de los datos informáticos".

[101] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de Dados: o direito à privacidade e os limites à função fiscalizadora do Estado, disponible en [http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/28]. Acceso en 27.08.2015.

La volatilidad de las informaciones digitales no está relacionada solamente a la alteración no autorizada de los datos, sino que posee una condición más sutil, generalmente presente en el comportamiento de los propios sistemas (operativos o no) que pueden ejecutar alteraciones en las informaciones sin la acción humana. De esta manera, ¿cómo garantizar que el contenido de un mensaje escrito y enviado por Fulano a Mengano no haya sido alterado por una persona (o sistema) en su computadora, en la computadora de Mengano o en el tránsito de uno al otro?

Obviamente, existen métodos de evitar la modificación de un archivo a través de autenticaciones vía *Hash* y otras técnicas, aún así, imagine que Mengano no quiere que nadie tenga acceso a las informaciones proporcionadas por Fulano. Basta que aquel borre un archivo, un e-mail o un mensaje instantáneo y con simplemente apretar un botón las informaciones se perderán, figurando en los sistemas tan sólo que ocurrió el intercambio de mensajes, pero sin el contenido de estos.

Ante todo lo expuesto, en esta discusión, me sitúo en el papel de los que aceptan la interceptación telemática, ya que muchas veces la comunicación es hecha a través de programas que utilizan el sistema VoIP, *voice over IP*, los cuales permiten el intercambio de mensajes de voz y video[102], utilizando ambos sistemas (telefónico y telemático).

En el contexto antes expuesto, en caso de que aceptásemos la imposibilidad de la interceptación telemática, imposible sería la interceptación en comunicación que utiliza la tecnología VoIP, teniendo en cuenta el principio del "*in dubio pro reo*" y la prohibición de la analogía "*in malam partem"*, principalmente.

En ese ámbito, hay una contradicción de gran parte de la doctrina que no acepta la interceptación telemática, pero afirma que ninguna libertad

[102] Como ejemplo podemos citar "Skype", "MSN", entre otros. Hoy en día, hasta Facebook permite la comunicación por videoconferencia entre los usuarios.

individual puede servir de instrumento de salvaguarda de prácticas ilícitas.

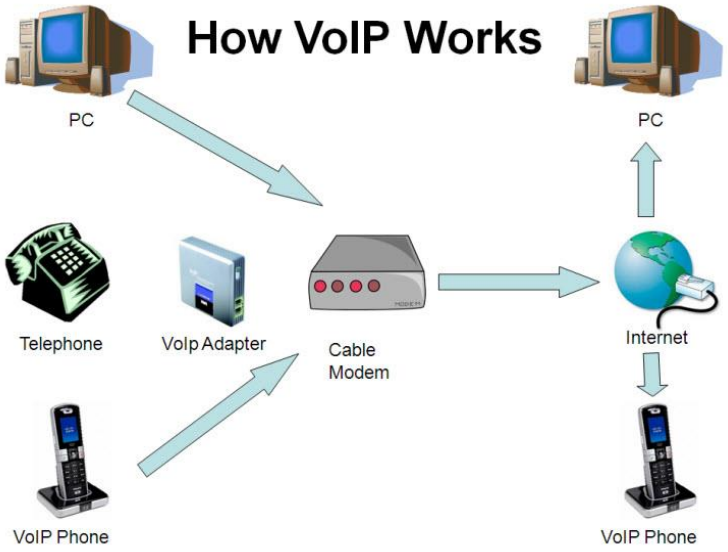
Pues bien, negándose la posibilidad de la interceptación telemática, se está protegiendo al malhechor que se vale de los medios tecnológicos más avanzados para la práctica de ilícitos e imposibilitando al Estado que prosiga con la debida persecución penal, frustrando así su *jus puniendi*.

Interceptación en VoIP

Para una mejor comprensión de la posibilidad de la interceptación en VoIP, se hace necesario una mejor explicación sobre tal tecnología que suena extraño a los oídos, ya que, a pesar de estar muy presente en el diario de la Sociedad Digital, es poco discutida en el ámbito jurídico.

Como ya fue explicado, VoIP, sigla para *voice over IP*, es la tecnología o técnica de transformar la voz en el modo convencional en paquetes de datos para ser transmitida por una red de IP, internet o Intranet.

Para el uso del VoIP es necesario la existencia de una red de telecomunicaciones, móvil o fija, que dé soporte a ese conjunto de tecnologías, como demuestra la figura a continuación.



103

Como explica Patricia Peck Pinheiro "los tipos de comunicación de Voz sobre IP más tradicionales son: PC a PC, teléfono a teléfono y PC a teléfono (sea fijo o celular). Las PC's y teléfonos deben estar preparados para ese tipo de comunicación, con programas e interfaces específicos previamente instalados. El usuario individual puede utilizar Voz sobre IP (VoIP) para una conversación PC a PC vía Internet, sin necesidad de licencia. Normalmente son usados programas (gratuitos o no) existentes en el mercado que utilizan Internet como medio de transmisión de voz" [104].

Además, añade Patricia Peck Pinheiro que "VoIP viene a ser la entrega de la voz digitalmente en pequeños paquetes de comunicación en vez de los tradicionales protocolos de circuitos conmutados presentes en sistemas de *Public Switched Telephone Network* – PSTN, redes públicas de las operadoras de telefonía otorgadas por órgano competente"

[103] Disponible en [http://voipcommunicationreviews.com/wp-content/uploads/2013/12/voip-without-service-provider.jpg]. Acceso en 16.10.2014.

[104] PINHEIRO, Patrícia Peck. Direito Digital, São Paulo: Saraiva – 5° ed. p. 363.

La comunicación por voz vía internet (VoIP) no es otra cosa que una comunicación vía internet. Los datos salen de un lugar y son transportados, en paquetes, por el mismo camino o no, hacia otro, así como ocurre en la comunicación telemática tradicional, con la diferencia de que los datos no quedan almacenados, así como ocurre en la comunicación telefónica.

Por tanto, se trata de una modalidad de interceptación telemática que debe ser tratada como telefónica, debiendo tanto la jurisprudencia como la doctrina posicionarse urgentemente acerca del tema que gana más importancia cada día.

Del Crimen de Interceptación Ilegal

El artículo 10 de la Ley de Interceptaciones (9.296/1996) dispone que constituye crimen realizar interceptación de comunicaciones telefónicas, de informática o telemática, o violar el secreto de la Justicia, sin autorización judicial o con objetivos no autorizados en ley y decreta la pena legal de dos a cuatro años de reclusión, además de multa.

O sea, además de la Interceptación "clandestina" dar fruto sólo a pruebas ilícitas, su práctica también constituye crimen punible con pena de reclusión, además de multa.

Vale destacar otra medida adoptada por Brasil para aumentar aún más la efectividad de la garantía constitucional de la intimidad y de la vida privada. El 20 de noviembre de 2012 sobrevino la Ley 12.737[105], popularmente conocida como "Ley Carolina Dieckmann", la cual tipificó el crimen de invasión de dispositivo móvil ajeno. No bastase con esa evolución legislativa esperada hace mucho en nuestro Ordenamiento

[105] BRASIL. Lei 12.737/2012. Disponible en [http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm]. Acceso en 18.10.2014.

patrio, la referida ley incluye también un determinante para el crimen antes mencionado, en los siguientes términos:

> *"Art .154-A – §3º. Si de la invasión resulta la obtención de contenido de comunicaciones electrónicas privadas, secretos comerciales o industriales, informaciones secretas así definidas en ley o control remoto no autorizado del dispositivo invadido;*
> *Pena – reclusión de 6 (seis) meses a 2 (dos) años, y multa, si la conducta no constituye crimen más grave."*

De esta forma, se hace evidente la preocupación latente del legislador en la protección de los datos protegidos por el art. 5º, incs. X, XI y XII de la CF, ante las nuevas tecnologías que surgen con velocidad infinitamente superior a la producción legislativa.

Ante todo lo expuesto, concluimos que es posible la interceptación telemática, sea por la cuestión hermenéutica del art. 5º, XII de nuestra Carta Magna, sea por la cuestión de la imposibilidad de obtención de las informaciones de la comunicación *a posteriori* cuando esta sea hecha a través de la tecnología VoIP, sea por el hecho de que la garantía constitucional no puede servir de salvaguarda para que se cometan actos ilícitos, y en ese mismo sentido, es el entendimiento del Tribunal Supremo Federal al decidir que la "inviolabilidad del secreto epistolar no puede constituir instrumento de salvaguarda de práctica de ilícitos"[106], al juzgar un caso de interceptación de carta de un presidiario por la administración de la penitenciaría.

LA PRIVACIDAD EN LA ERA DE LA AUSENCIA DE PRIVACIDAD

Caroline Teófilo da Silva

[106] STF – 1° Turma, HC n.° 70.814-5/SP, Rel. Min. Celso de Mello, Diário da Justiça, Sección I, 24 jun., 1994, p. 16.650 – *RT* 709/418.

La creación de aplicaciones como Lulu y Tubby, además de generar mucha polémica, trajo nuevamente a colación la discusión sobre la privacidad y la libertad de expresión. En el caso del aplicativo Lulu, la herramienta permite que mujeres evalúen y comenten anónimamente sus percepciones sobre los hombres que poseen perfiles en Facebook y/o en Twitter, sin exigir autorizaciones de los evaluados, permitiendo que solo posteriormente sea solicitada la eliminación del perfil en la aplicación.

Tubby, por su parte, se dirige a hombres, para evaluar el comportamiento y el desempeño sexual de mujeres, que, según sus desarrolladores, fue hecho en represalia a Lulu. En Brasil, la aplicación fue prohibida por la justicia después de una acción en base a la Ley Maria da Penha (11.340/2006), por esta promover la violencia contra la mujer.

El derecho a la privacidad es mundialmente consagrado en el art. XII de la Declaración Universal de los Derechos Humanos[107] y, nacionalmente, en el art. 5°, X y XII[108] de la CF, no obstante, este aun es muchas veces puesto a prueba a causa de otro principio no menos importante, el derecho a la libertad de expresión.

Mientras el derecho a la privacidad protege a su detentor de exposiciones indeseadas de sus datos personales, sus informaciones, su intimidad, vida privada, honra e imagen, el derecho a la libertad de expresión le garantiza la posibilidad de manifestación del pensamiento, estipulado por el inc. IV,

[107] Art. XII - Nadie estará sujeto a la interferencia en su vida privada, en su familia, en su hogar o en su correspondencia, ni a ataque a su honra y reputación. Todo ser humano tiene derecho a la protección de la ley contra tales interferencias o ataques.

[108] Art. 5° (...)
X - son inviolables la intimidad, la vida privada, la honra y la imagen de las personas, asegurado el derecho a indemnización por el daño material o moral derivado de su violación (...)
XII - Es inviolable el secreto de la correspondencia y de las comunicaciones telegráficas, de datos y de las comunicaciones telefónicas, salvo, en el último caso, por orden judicial, en las hipótesis y en la forma que la ley establezca para fines de investigación criminal o instrucción procesal penal. (...).

art. 5° de la CF[109]. Aunque ambos sean analizados y compatibilizados judicialmente en el caso en concreto, son limitados, tanto por la propia Constitución Federal como por las demás legislaciones brasileñas.

Pero ¿es Facebook un ambiente que los usuarios pueden considerar como privativo? En sus políticas y términos de uso, la red social informa al usuario que, al agregar una aplicación a su línea de tiempo, como Lulu, Facebook le suministra las informaciones básicas del usuario, o sea, su identificación, informaciones públicas y la lista de amigos[110]. De esta forma, cuando el usuario crea su perfil, está de acuerdo con las condiciones del servicio ofrecidas por el prestador y acepta poner sus datos a disposición.

No obstante, los prestadores de servicios deben respetar los límites de la ética y de la proporcionalidad, además de la legislación nacional vigente, como preceptúan los arts. 186 y 187 del Código Civil:

"Art. 186. Aquel que, por acción u omisión voluntaria, negligencia o imprudencia, viole el derecho y cause daño a otro, aunque exclusivamente moral, comete un acto ilícito.

"Art. 187. También comete acto ilícito el titular de un derecho que, al ejercerlo, excede manifiestamente los límites impuestos por su fin económico o social, por la buena fe o por las buenas costumbres." (subrayado nuestro)

La utilización de los datos del usuario en aplicaciones para evaluación de las relaciones, sin su autorización específica, puede generar daños a la honra y a la privacidad del evaluado, limitando el derecho a la libertad de

[109] Art.5°, (...)
IV - es libre la manifestación del pensamiento, siendo vedado el anonimato.

[110] [https://www.facebook.com/about/privacy/your-info-on-other].

expresión, lo que generaría indemnización en el ámbito civil, de acuerdo con lo dispuesto en el Código Civil:

"Art. 21. La vida privada de la persona natural es inviolable, y el juez, a solicitud del interesado, adoptará las providencias necesarias para impedir o hacer cesar el acto contrario a esta norma."

En la esfera penal, por su parte, el responsable de la lesión podrá incurrir en los crímenes contra la honra – calumnia, injuria y difamación – y cuando son cometidos en presencia de varias personas, o por un medio que facilite la divulgación, por ejemplo, las redes sociales e internet, la pena de cada uno de los crímenes es aumentada en un tercio, como describe el art. 141, III del Código Penal[111].

Por eso, es importante siempre considerar, antes de la publicación, que las redes sociales amplían el alcance de las informaciones, y posibilitan el acceso irrestricto y en contextos diferentes de aquel en que inicialmente fue compartido. ¿Qué usuario imaginó que su comportamiento y sus actitudes presenciales serían evaluadas en una aplicación digital?

Además, la aplicación permite que la evaluación sea anónima, confrontando el inc. IV, art. 5° de la CF, que permite la libre manifestación del pensamiento, pero veda de manera expresa el anonimato.

Ante lo expuesto y de manera preventiva, se recomienda que el usuario de redes sociales y servicios digitales gratuitos esté atento a las políticas y a los términos de uso y que sólo proporcione informaciones si está de acuerdo con las condiciones descritas. Además, debe considerar qué contenidos y datos serán publicados, pues, como fue mencionado anteriormente, esos servicios almacenan las informaciones de registro y de comportamiento de los usuarios.

[111] Art. 141 - Las penas conminadas en este Capítulo aumentan en un tercio, si cualquiera de los crímenes es cometido:
III – en la presencia de varias personas, o por un medio que facilite la divulgación de la calumnia, de la difamación o de la injuria.

De igual forma, las configuraciones de los perfiles deben ser personalizadas, de modo que el usuario sea notificado siempre que se acceda a su cuenta desde otro dispositivo, por ejemplo, en Facebook, donde el usuario puede eliminar y verificar qué dispositivos están habilitados para acceso a su perfil.

Para que el público en general no tenga acceso a todos los contenidos proporcionados, las configuraciones de privacidad pueden ser alteradas o personalizadas de acuerdo con lo ofrecido por los servicios y del modo que mejor se adecue al usuario. También, en Facebook, el internauta puede activar la opción para analizar todas las publicaciones en que es etiquetado, además de escoger quién puede ver sus publicaciones y su línea de tiempo.

Con relación a las aplicaciones, Facebook habilita el campo para configuraciones de aplicaciones, y en caso de que el usuario no utilice ninguna aplicación, podrá desactivar esta opción y así ninguna de sus informaciones serán compartidas. No obstante, si posee aplicaciones, podrá editarlas, eliminarlas y escoger qué datos podrán ser tomados por otras personas al usar aplicaciones.

Resumiendo, los usuarios de servicios digitales gratuitos necesitan estar al corriente de cómo sus informaciones son utilizadas y almacenadas por los proveedores y adoptar medidas preventivas que puedan minimizar la exposición de sus informaciones. No obstante, si aun así se sintieran perjudicados, podrán accionar el poder judicial y proponer la acción pertinente, por ejemplo, la indagación instaurada por la Promotoría de Justicia de Defensa del Consumidor de Brasilia contra Lulu y Facebook, alegando ofensa a la honra y a la privacidad de los consumidores [112].

[112] [http://g1.globo.com/distrito-federal/noticia/2013/12/mp-do-df-instaura-inquerito-sobre-aplicativo-lulu-e-facebook.html]. Acceso en 03.12.2013.

Derecho digital 2.0

Directora Responsable
MARISA HARMS

Directora de Operaciones de Contenido
JULIANA MAYUMI O. ONO

Editores: Andréia Regina Schneider Nunes, Cristiane Gonzalez Basile de Faria, Diego Garcia Mendonça, Iviê A. M. Loureiro Gomes y Luciana Felix

Asistente Administrativa Editorial: Juliana Camilo Menezes

Producción Editorial
Coordinación
DANIEL CESAR LEAL DIAS DE CARVALHO

Analistas de Operaciones Editoriales: Aline Almeida da Silva, André Furtado de Oliveira, Damares Regina Felício, Danielle Rondon Castro de Morais, Flávia Campos Marcelino Martines, Gabriele Lais Sant'Anna dos Santos, Maria Eduarda Silva Rocha, Maurício Zednik Cassim y Thiago César Gonçalves de Souza

Calidad Editorial y Revisión
Coordinación
LUCIANA VAZ CAMEIRA

Analistas de Calidad Editorial: Carina Xavier Silva, Cinthia Santos Galarza, Daniela Medeiros Gonçalves Melo, Marcelo Ventura y Maria Angélica Leite

Analistas Editoriales: Daniele de Andrade Vintecinco y Mayara Crispim Freitas

Cubierta: Chrisley Figueiredo

Administración y Producción Gráfica
Coordinación
Caio Henrique Andrade

Analista Administrativa: Antonia Pereira
Asistente Administrativa: Francisca Lucélia Carvalho de Sena

Datos Internacionales de Catalogación en la Publicación (CIP)
(Cámara Brasileña del Libro, SP, Brasil)
Derecho digital 2.0
Patrícia Peck Pinheiro
Coordinadora
2da edición revisada, actualizada y ampliada
Sello –ebook

EDITORA REVISTA DOS TRIBUNAIS LTDA.
MARISA HARMS
Directora responsable
Rua do Bosque, 820 – Barra Funda
Tel. 11 3613-8400 – Fax 11 3613-8450
CEP 01136-000 – São Paulo, SP, Brasil

CENTRAL DE RELACIONES RT
(Atención, en días hábiles, de las 8 a las 17 horas)
Tel. 0800-702-2433

e-mail de atención al consumidor: sac@rt.com.br
Visite nuestro sitio: www.rt.com.br
Impreso en Brasil [08-2016] Profesional
Cierre de esta edición [00.07.2016]
ISBN 978-85-203-6918-0