



DERECHO Y TIC. VERTIENTES ACTUALES

EVELYN TÉLLEZ CARVAJAL
Coordinadora



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE INVESTIGACIONES JURÍDICAS
INFOTEC, CENTRO DE INVESTIGACIONES E INNOVACIÓN
EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, CONACYT

DERECHO Y TIC.
VERTIENTES ACTUALES

INSTITUTO DE INVESTIGACIONES JURÍDICAS
Serie DOCTRINA JURÍDICA, núm. 751

COORDINACIÓN EDITORIAL

Lic. Raúl Márquez Romero
Secretario Técnico

Lic. Wendy Vanesa Rocha Cacho
Jefa del Departamento de Publicaciones

Irma Martínez Hidalgo
Formación en computadora

Arturo de Jesús Flores Ávalos
Elaboración de portada

DERECHO Y TIC. VERTIENTES ACTUALES

EVELYN TÉLLEZ CARVAJAL

Coordinadora



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE INVESTIGACIONES JURÍDICAS
INFOTEC, CENTRO DE INVESTIGACIÓN E INNOVACIÓN
EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
CONACYT
México, 2016

Primera edición: 6 de enero de 2016

DR © 2016. Universidad Nacional Autónoma de México

INSTITUTO DE INVESTIGACIONES JURÍDICAS

Circuito Maestro Mario de la Cueva s/n
Ciudad de la Investigación en Humanidades
Ciudad Universitaria, 04510 México, D. F.

Impreso y hecho en México

ISBN 978-607-02-7410-7

CONTENIDO

Prólogo	IX
Alberto NAVA GARCÉS	
Introducción	XIII
Evelyn TÉLLEZ CARVAJAL	
Abreviaturas	XIX
La integración de México a la Sociedad de la Información	1
Miguel CASILLAS	
Alberto RAMÍREZ-MARTINELL	
Moisés CARVAJAL	
Karla VALENCIA	
Los sujetos de las SIC	33
Federico César LEFRANC WEEGAN	
Género y TIC. Por una Sociedad de la Información con perspectiva de género.....	49
Alejandro de la GARZA REYES	
Evelyn TÉLLEZ CARVAJAL	
Tecnologías de Información y Comunicación (TIC), protección de datos y derechos humanos en la jurisprudencia del Tribunal Europeo de Derechos Humanos	79
Florian HUBER	

El ejercicio de los derechos ARCO ante el flujo transfronterizo de información biométrica	117
Vanesa DÍAZ	
TIC. Globalización y política pública en el Estado contemporáneo . .	139
Gonzalo FARRERA BRAVO	
Daniela MARTÍNEZ SALINAS	
Justicia electrónica: en busca de la interoperabilidad	161
Myrna Elia GARCÍA BARRERA	
La protección de los datos digitales. Una lectura de la tensión del <i>habeas data</i> en el contexto del cambio de las relaciones sociales que supone Internet	183
Frey Alexander PRADA V.	
Carolina VELANDIA H.	
Algunos aspectos de la propiedad intelectual en el entorno digital . . .	215
Carlos Alberto ORTIZ LÓPEZ	
El derecho de autor en Internet y las responsabilidades de los proveedores de servicios de Internet	235
Jonathan Gabriel GARZÓN GALVÁN	
Bitcoin: problemas reales	265
Cristina GÓMEZ RODRÍGUEZ	
La transposición del Convenio de Budapest sobre la ciberdelincuencia en la legislación francesa en la práctica	299
Cynthia SOLÍS	
Vincent LEMOINE	
De los autores	315

Derecho y TIC. Vertientes actuales, editado por el Instituto de Investigaciones Jurídicas de la UNAM, se terminó de imprimir el 6 de enero de 2016 en los talleres de Impresión Comunicación Gráfica, S. A. de C. V., Manuel Ávila Camacho 689, col. Sta. Ma. Atzahuacán, delegación Iztapalapa, 09500 México, D. F. Se utilizó tipo *Baskerville* en 9, 10 y 11 puntos. En esta edición se empleó papel cultural 70 x 95 de 50 kilos para los interiores y cartulina couché de 250 gramos para los forros; consta de 500 ejemplares (impresión *offset*).

PRÓLOGO

Las nuevas tecnologías de la información y las comunicaciones traen un paso galopante en la historia reciente. Mientras unos investigadores acometen en sus estudios algunas de sus aristas, en algún lugar del mundo aparece un nuevo prodigio de la técnica para mejorar o desarrollar las nuevas herramientas del efímero futuro que les sigue.

En la disyuntiva de entender a la tecnología como objeto de regulación o permitir que ésta suceda, ajena al control del Estado, aparecen distintos profesionales que explican cómo ha cambiado la forma y el nivel de vida de personas, así como la regulación ingente que inunda la red, sin siquiera poder abarcar un sector de ella de modo tajante, puntual, atinado.

En este mapa sin brújula, distintos teóricos de diferentes latitudes nos ponen al día con una vasta y novedosa bibliografía. Tratar el tema de las tecnologías nos acerca más al pensamiento de Heráclito, pues en cada ocasión que metemos la mano al río, ni es la misma mano, ni son las mismas aguas.

¿Cómo enfrentar este fenómeno para no hacer una fotografía de lo efímero?

Los distintos autores que participan en la obra se sujetaron a principios inamovibles, se acercaron a los temas desde la perspectiva que no cambia, que forja principios y que da soluciones desde el ámbito general.

La visión de los nuevos artilugios, y si éstos le dan la característica al sujeto o a la era en que ocurre, propicia la reflexión sobre quién sirve a quién, ¿la tecnología al sujeto o el sujeto es esclavo del cambio tecnológico?

Un libro como el que ahora invitamos a su lectura nos ofrece, en un solo volumen, provechosas enseñanzas y reflexiones que le dan una dimensión pocas veces vista a un tema que ha transformado la cotidianidad.

De la explicación del sujeto en esta nueva era, pasamos a las distintas aristas de un mundo virtual perseguido por los formalismos de la regulación tradicional. En ese ámbito podemos encontrar la visión de los profesionales que le han dedicado más de una década de estudio a los progresos tecnológicos y a sus soluciones normativas, lo cual equivale a tomar un rayo por las manos.

La memoria de ese cada vez más lejano Convenio de Budapest contra la cibercriminalidad (2001) que no ha terminado de cuajar, así como la aparición de figuras virtuales como el pago con una moneda que no ha sido emitida por un banco estatal, son parte de los temas frontera que aparecen en las páginas de este libro, que ofrece al lector un valor agregado: llenarlo de posibilidades.

Al abordar el tema de los derechos humanos en un libro de este calado, es impresionante el número y la clase de criterios con los que se ilustra el tema para entender ese nuevo vínculo entre la protección de datos, los derechos humanos y las tecnologías de información y comunicación, una cuestión que hace veinte años no era tratada en las aulas ni siquiera de manera referencial. Es claro que las nuevas tecnologías han dado paso a la creación de nuevos institutos, como en su momento ocurrió con el tema de los derechos humanos, así como las cuestiones de género, cuyo tratamiento ha cambiado la óptica de los operadores de justicia y de algunas instituciones, pero en la que resalta la necesidad de seguir transformando el contexto en el que hombres y mujeres se desenvuelven bajo estas nuevas circunstancias tendentes a la equidad. En el cuerpo del libro encontramos el siguiente párrafo:

La capacidad técnica del ser humano parece ser una de sus características esenciales, nacemos con esta cualidad pero no nos determina. Por eso en este artículo se cuestiona la expresión nativo digital, como si denotara una especie distinta de seres humanos, es decir, como si los determinara. Esa pretensión es falaz. Lo que hace una expresión así, es separar, discriminando y etiquetando a partir de la posesión de aparatos. Aquí recordamos que ni Steve Jobs, ni Stephen Wozniak, ni Bill Gates han sido nativos digitales, e invitamos al lector a sacar las consecuencias.

Con esa apertura al debate, sabemos que lo mejor de su trabajo no vino de los pequeños talleres que formaron en un principio, sino en su visión de cómo deberían funcionar los aparatos y los programas que han transformado a la sociedad y que, aun sin quererlo, dividieron a la gente por sus habilidades para adaptarse a los cambios. Un ejemplo: el mp3 y los distintos reproductores de música digital ya eran una realidad cuando al imaginativo Jobs se le ocurrió transformar el mercado con ese dispositivo llamado *Ipod*. Es evidente que esta invitación a la lectura, la hago con los ojos maravillados de un migrante digital.

La brecha generacional dada por la tecnología no pretende discriminar a los sujetos, sino entenderlos desde sus habilidades y tener en cuenta que son partícipes de un contexto diferente. Trabajos como este, ayudan a cerrar esa

PRÓLOGO

XI

brecha y a abrir nuevos debates, lo cual celebro y hago mis mejores votos para que este libro salga al encuentro de distintos lectores para su provecho y desarrollo de las ideas que aquí, con gran tino, ha reunido la maestra Evelyn Téllez Carvajal.

Alberto E. NAVA GARCÉS*
Otoño de 2014

* Profesor e investigador de INFOTEC.

INTRODUCCIÓN

La obra que el lector tiene en sus manos es producto de una serie de doce artículos inéditos escritos por autores de diversos países, todos especialistas en cada una de las materias que se tratan. Conscientes de la importancia que tienen hoy en día los progresos en materia de Tecnologías de la Información y Comunicación (TIC), así como su relación con diversas áreas como la educación, la propiedad intelectual, el gobierno, la justicia, los derechos humanos, la ciberdelincuencia, etcétera, hemos participado en la elaboración de este libro colectivo, cuya finalidad, como su título lo advierte, es brindar un panorama actual de las diversas vertientes en las que se relaciona el derecho con las TIC.

En el primer apartado el lector tiene la obra realizada por Casillas, Ramírez-Martinell, Carvajal y Valencia, todos ellos profesores de la Universidad Veracruzana, quienes entregan un trabajo titulado: “La integración de México a la Sociedad de la Información”. Decidimos iniciar esta obra con esta contribución pues es necesario no perder de vista que el uso de las TIC se inserta como un fenómeno globalizador, por ello es necesario reconocer cuál es el desarrollo y el impacto que tienen las TIC en la sociedad en el contexto mexicano.

En su obra los autores se remiten a diversos indicadores sobre la integración de los mexicanos al acceso a Internet, así como a diversos dispositivos tecnológicos en un periodo comprendido de 2001 a 2011. En este periodo se puede observar cómo ciertas regiones del país se han incorporado a esta llamada Sociedad de la Información, pero, al mismo tiempo, los autores señalan la marcada diferencia que hay entre los distintos estados que integran la República mexicana en cuanto a la integración y desarrollo de estas TIC. Esto ocasiona que la llamada brecha digital sea cada vez más amplia y agranda las diferencias en oportunidades para los ciudadanos que no tienen el mismo acceso a ellas.

Una vez entendido el contexto en que se sitúan los profesores de la Universidad Veracruzana, el trabajo presentado por el doctor Lefranc Weegan, “Los Sujetos de las SIC”, segundo artículo de la obra, establece una realidad en la que nos encontramos inmersos todos los individuos en relación

con la llamada Sociedad de la Información. El doctor Lefranc cuestiona el concepto de Sociedad de la Información y Conocimiento (SIC), frente al de Sociedad de la Información y Comunicación.

A lo largo de su contribución el autor nos pone frente a preguntas que nos llevan a un análisis minucioso y concientizado sobre el significado de conceptos como soberanía, nativo digital, brecha digital, sociedad digital en el contexto de la SIC.

Con diversos cuestionamientos se invita a la reflexión sobre la importancia que se le da a las TIC y la relevancia que en realidad tienen en la vida de los ciudadanos, en donde las TIC son tanto una herramienta útil a la vida diaria como un riesgo a la misma.

En su contribución el doctor Lefranc señala la necesidad de observar en su justa dimensión el progreso y el uso de las TIC en nuestra vida cotidiana y dejar de verlas como una panacea que resolverá los problemas de la sociedad.

El tercer artículo, del maestro De la Garza y la maestra Téllez, propone la inclusión de una perspectiva de género en la Sociedad de la Información ya que consideran que las TIC pueden ser una herramienta que beneficie al cambio de paradigmas sobre los roles de la mujer en la sociedad actual.

Al igual que el doctor Lefranc, consideramos a las TIC en un contexto real y no ideal, siendo críticos sobre los objetivos que se pudieran alcanzar a través del uso adecuado de las TIC en beneficio de los derechos humanos, su difusión pero, sobre todo, su práctica y respeto.

Para los autores de este artículo es necesario reconstruir el rol de las mujeres y permitir su empoderamiento a través de la oportunidad que brinda la Sociedad de la Información, y cumplir así con los tratados internacionales de derechos humanos y los Objetivos del Milenio, cuyo fin último es erradicar la pobreza y lograr un desarrollo integral de toda la comunidad internacional que permita gozar de los estándares de vida digna para todos.

El cuarto artículo se refiere a las “Tecnologías de la Información y Comunicación (TIC), protección de datos y derechos humanos en la jurisprudencia del Tribunal Europeo de Derechos Humanos”, un análisis que el profesor Huber, con una amplia experiencia en la materia, elaboró *ex profeso* para permitirnos observar el lugar en el que se encuentra la ponderación de derechos en el contexto europeo y así evaluar nuestra situación.

En el artículo el profesor Huber pone de manifiesto los fundamentos normativos de la protección de datos antes de entrar al análisis de las sentencias del Tribunal Europeo de Derechos Humanos. El trabajo permite apreciar la manera en que los jueces europeos ponderan diversos derechos humanos junto a la protección de datos, un ejercicio que es muy incipiente en nuestro país.

Como quinta contribución, y relacionado con el artículo anterior, el lector se encuentra con el artículo de la maestra Díaz que se titula: “El ejercicio de los derechos ARCO ante el flujo transfronterizo de información biométrica”. En su artículo la autora explica la trascendencia e importancia de un adecuado manejo, recolección, utilización y transferencia de los datos biométricos sobre todo si esa transferencia de información se da más allá de las fronteras.

Al ser los datos biométricos todas aquellas características fisiológicas y morfológicas que identifican a los individuos como seres únicos, su protección debe situarse en los estándares más altos. La autora explica, a través de la experiencia de los sistemas biométricos regionales existentes, como son en Europa, el Sistema de Información de Schengen (SIS) y EURODAC, y, en el foro Asia-Pacífico de Cooperación Económica (APEC), la Tarjeta de Viajes de Negocios de APEC, cómo se aplican al flujo transfronterizo de datos. Un aporte que debe interesarnos.

La autora hace un análisis sobre las diferencias normativas en cuanto al tratamiento de los derechos ARCO según el ordenamiento jurídico de que se trate, identificando importantes lagunas legales al respecto que son urgentes de solucionar para dar pleno cumplimiento a los denominados derechos ARCO.

Como sexta contribución se encuentra el artículo “TIC: Globalización y política pública en el Estado contemporáneo” del maestro Farrera Bravo y Daniela Martínez, quienes comparten su experiencia en el área de gobernanza y TIC.

Los autores parten de la idea de que los Estados de América Latina se han visto en la necesidad de incluir las TIC en la administración pública. Así se han creado nuevas formas de comunicación entre los ciudadanos y el gobierno tratando de aprovechar al máximo el uso de las TIC. Sin embargo, los autores ponen de manifiesto las desigualdades a lo largo y ancho del territorio en cuanto al acceso de las TIC, lo que impide que el gobierno digital sea una realidad en este contexto; a lo anterior se unen cuestiones relativas a la educación en torno a las TIC y el costo-beneficio de implementar estas nuevas tecnologías en la administración pública federal.

Los autores también hacen un análisis del *e-gobierno* desde el Poder Judicial, Legislativo y Ejecutivo, para concluir en las virtudes y ventajas que ha representado la experiencia del *e-gobierno* en nuestro país.

En el séptimo trabajo, “Justicia electrónica. En búsqueda de la interoperabilidad”, la doctora García Barrera sostiene la necesidad de conseguir que los sistemas y aplicaciones informáticas que actualmente se manejan en las diversas instituciones públicas puedan establecer una comunicación

entre ellas, es decir, sean interoperables para poder contribuir a agilizar los trámites y reducir los tiempos de atención al ciudadano haciendo énfasis en la administración de justicia.

La autora indica que es necesario que el gobierno transite del documento en papel al documento digital pues el *e-gobierno* no sólo se refiere a poder consultar información a través de las plataformas y páginas gubernamentales, sino que tiene que existir la posibilidad de realizar trámites por medio de estas mismas plataformas de manera segura y rápida. Así las cosas, la propuesta de la autora va más allá, pues sugiere una transición al Estado de derecho más dinámico y transparente en el que, gracias al *e-gobierno*, el ciudadano pueda establecer una comunicación más directa con sus gobernantes.

Finalmente, la doctora Myrna García expone la importancia que ha tenido y tendrá la informática jurídica decisoria que se basa en el principio de que las TIC faciliten la información adecuada al jurista para ayudarle a tomar decisiones correctas.

El octavo trabajo, “La protección de los datos digitales. Una lectura de la tensión del *habeas data* en el contexto del cambio de las relaciones sociales que supone Internet”, de los profesores Prada V. y Velandia H., analiza la Sociedad de la Información desde la perspectiva propuesta por Niklas Luhmann, quien sostenía que la sociedad era comunicación.

Así, los autores dejan al descubierto que si bien es cierto que mucho de lo que conforma a la sociedad actual es la información, en la realidad, estas informaciones no se encuentran adecuadamente protegidas.

Los autores echan mano de la experiencia colombiana del *habeas data* para dejar en claro la falta de herramientas efectivas por parte del individuo para lograr que el Estado brinde la protección adecuada a sus datos, por lo que nos encontramos ante casos de abusos y violación a los derechos de los individuos por una inadecuada protección de la información.

En el noveno artículo, “Algunos aspectos de la propiedad intelectual en el entorno digital”, el profesor Ortiz López discurre sobre problemáticas que se derivan respecto a la propiedad intelectual a través del uso de las TIC. Si bien el autor explica que el derecho de propiedad intelectual no es nuevo, pues el derecho de autor, por ejemplo, es ampliamente reconocido por proteger exclusivamente la forma literaria o artística de las ideas descritas, ilustradas o incorporadas en obras, sí lo es el abuso que de ciertas obras se hace por medio de las nuevas tecnologías.

El profesor Ortiz resalta que el uso de las TIC se ha convertido en el principal reto de la protección de la propiedad intelectual debido a los nuevos usos y alcances de la masiva cultura de vulneración de estos derechos. El autor reafirma que los Estados han quedado rebasados en sus intentos por

regular la protección de la propiedad intelectual en Internet, toda vez que simplemente han creado pequeñas disposiciones que pretenden actualizar las normas ya existentes en la materia, sin entender la necesidad de hacer un alto en el camino y crear una norma completa, que permita visualizar cada uno de los aspectos del uso de creaciones en el ambiente analógico y digital, y que lo mismo debe hacerse respecto a las marcas y los nombres de dominio.

En el artículo décimo, el maestro Garzón Galván, al igual que el profesor Ortiz, presenta un trabajo en el que analiza una de las diversas aristas que representa la vulneración de derechos de propiedad intelectual en Internet.

En su contribución el maestro Garzón expone la situación que enfrentan los proveedores de servicios de Internet ante estas prácticas violatorias de los derechos de propiedad intelectual.

Haciendo uso de experiencias en casos similares, el profesor Garzón presenta algunas oportunidades para el caso mexicano y menciona los aportes de Estados Unidos, Europa y América Latina.

Desde la perspectiva que se presenta en el artículo, la solución a la vulneración de derechos de propiedad intelectual presenta la complejidad de tener que analizarse a la luz de otros derechos que pudieran verse vulnerados al querer proteger los derechos de los autores de obras, tales como la libertad de expresión, la privacidad de las personas, el derecho a la inviolabilidad de las comunicaciones privadas y, por otro lado, al tratar de dar soluciones a la problemática no caer en excesos de imponer cargas tecnológicamente inviables o altamente costosas a los proveedores de servicios de Internet, por mencionar algunos.

En el undécimo artículo “Bitcoin: Problemas reales”, la licenciada Cristina Gómez Rodríguez explica cómo entender el *software* que se ha utilizado como medio de pago por bienes y servicios en la red, lo que ha llevado a la mala interpretación de reconocerlo como “dinero virtual” o “moneda digital” y a una reflexión sobre su normatividad.

En su contribución la autora nos muestra la problemática en diversas áreas del derecho que se ven impactadas por esta unidad de cambio. La licenciada Gómez no sólo hace el análisis del origen y actualidad de la denominada *Bitcoin* sino que también nos da su opinión respecto a su futuro.

Finalmente, el doceavo artículo, a cargo de los profesores Solís y Lemoine, proporciona una versión fresca sobre “La transposición del Convenio de Budapest sobre la ciberdelincuencia en la legislación francesa en la práctica. Lecciones para México en el marco de su posible adhesión al mismo”.

Las nuevas tecnologías y su ambivalencia en cuanto a beneficios y perjuicios para la sociedad, es una constante en la obra, y este trabajo no es la

excepción pues se refiere a la comisión de delitos a través de estas nuevas tecnologías y como la comunidad internacional, pendiente de las posibles soluciones, no deja de observar las violaciones a otros derechos que pudieran verse en juego.

Los diferentes actores en materia de procedimiento penal en materia de TIC, como magistrados y policías, pueden realizar la interceptación de información, intervención de equipos y sistemas de cómputo e inclusive violar la correspondencia electrónica en aras de abatir la ciberdelincuencia.

La experiencia francesa en el caso permite a México ser cauto en la conveniencia o no de suscribir este tipo de instrumentos internacionales, por lo que la propuesta de los profesores es significativamente útil para nuestro país.

Por todo lo anterior y recordando que la palabra vertiente hace referencia al antiguo participio activo del latín *verter*, que se refiere a un declive o lugar por donde corre el agua, se presentan estos doce artículos, que son como ese afluente que corre vertiginoso a través de montañas y valles, pues son aguas que corren tempestuosas, y ya sea desde cimas, picos y crestas o tierras bajas, pero su paso deja huella que erosiona, de acuerdo con su altura y desnivel.

Esta es la manera en que consideramos al derecho y las TIC, como esos pensamientos que surgen y corren entre terrenos fértiles que causan modificaciones en su entorno aun sin quererlo. Son puntos de vista y opiniones de diversos expertos en las distintas áreas que hemos presentado y que ponemos a consideración del lector, para que sea él quien juzgue la pertinencia y utilidad de su contenido.

Agradezco infinitamente al INFOTEC por todas las facilidades y apoyos para la realización de la presente obra, en especial mi reconocimiento a todos y cada uno de los autores que me confiaron sus escritos para llevarlos a ver la luz en esta obra colectiva.

Evelyn TÉLLEZ CARVAJAL
Otño, Ciudad de México, 2014

ABREVIATURAS

ACC	Autoridad Común de Control de Schengen
ACTA	Acuerdo Comercial Antifalsificación
ADPIC	Acuerdos de los Derechos de Propiedad Intelectual relacionados con el Comercio
AFIS	Sistema Automatizado de Identificación de Huellas Dactilares por sus siglas en inglés
APEC	Cooperación Económica de Asia-Pacífico
APF	Administración Pública Federal
Apps	Aplicaciones
ARCO	Acceso, Rectificación, Cancelación y Oposición
CCF	Código Civil Federal
CCTV	Circuito cerrado de televisión
CEDH	Convención Europea de Derechos Humanos
CEPOL	Colegio Europeo de Policía
CONAPO	Consejo Nacional de Población
CPCNL	Código de Procedimientos Civiles del Estado de Nuevo León
CPPNL	Código Procesal Penal del Estado de Nuevo León
DESC	Derechos económicos, sociales y culturales
DMCA	<i>Digital Millennium Copyright Act</i>
DNS	Servicio de Nombres de Dominio por sus siglas en inglés
EEE	Espacio Económico Europeo
HADOPI	Ley de Difusión y Protección de la Creación en Internet (Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet)
IMPI	Instituto Mexicano de la Propiedad Industrial
INEGI	Instituto Nacional de Estadística y Geografía
IANA	<i>Internet Assigned Numbers Authority</i>
ISO	<i>International Standard Organization</i>
ISP	<i>Internet Service Provider</i>
ITESM	Instituto Tecnológico de Estudios Superiores de Monterrey

ITU	<i>International Telecommunication Union</i>
LFDA	Ley Federal de Derechos de Autor
OACI	Organización de Aviación Civil Internacional
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OMC	Organización Mundial del Comercio
OMPI	Organización Mundial de la Propiedad Intelectual
ONU	Organización de Naciones Unidas
NSFNET o NSF	<i>National Science Foundation</i>
P2P	Entre pares, entre iguales
PPD	Principios de protección de datos
PSI	Proveedor de Servicios de Internet
SEPD	Supervisor Europeo de Protección de Datos Personales
SIS	Sistema de Información de Schengen
TEDH	Tribunal Europeo de Derechos Humanos
TIC	Tecnologías de Información y Comunicación
TLCAN	Tratado de Libre Comercio de América del Norte
TODA	Tratado de la OMPI sobre Derecho de Autor
TOIEF	Tratado de la OMPI sobre Interpretaciones o Ejecuciones de Fonogramas
TPP	Acuerdo Estratégico Trans-Pacífico de Asociación Económica
UE	Unión Europea

LA INTEGRACIÓN DE MÉXICO A LA SOCIEDAD DE LA INFORMACIÓN

Miguel CASILLAS*
Alberto RAMÍREZ-MARTINELL**
Moisés CARVAJAL***
Karla VALENCIA****

SUMARIO: I. *Introducción*. II. *México ante la sociedad de la información*. III. *Acceso a Internet*. IV. *Telefonía móvil*. V. *El desarrollo desigual en México*. VI. *Conclusiones*. VII. *Bibliografía*.

I. INTRODUCCIÓN

Estudiosos de las sociedades modernas¹ hablan de civilizaciones habilitadas por nuevos esquemas económicos, por movilizaciones sociales, y por relaciones entre empresas, instituciones y grupos sociales cuya lógica de comunicación se explica por el entendimiento de una sociedad interconectada de escala global y cuya dinámica empresarial, social y política está orientada hacia la habilitación de la provisión e intercambio de servicios y productos

* Doctor en sociología por la Escuela de Altos Estudios en Ciencias Sociales de París, investigador titular del Instituto de Investigaciones en Educación de la Universidad Veracruzana.

** Doctor en tecnología educativa por la Universidad de Lancaster, Inglaterra, investigador titular del Instituto de Investigaciones en Educación de la Universidad Veracruzana.

*** Licenciado en pedagogía por la Universidad Veracruzana, estudiante de la maestría en Educación virtual de la misma casa de estudios.

**** Maestra en desarrollo regional por el Colegio de Veracruz, técnico académico en el Instituto de Investigaciones en Educación de la Universidad Veracruzana.

¹ Castells, Manuel, *The Rise of the Network Society*, Oxford, Blackwell, 1996; Toffler, Alvin, *La tercera ola*, Bogotá, Edinal, 1981, y Simone, Raffaele, *La tercera fase: formas de saber que estamos perdiendo*, México, Taurus, 2001.

intangibles. Para abordar la evolución de las sociedades, Alvin Toffler² propone una discusión en torno de una serie de olas de cambio sin fronteras claras que chocan y se traslapan entre sí. La primera oleada de cambio a la que se refiere el autor estadounidense corresponde a las civilizaciones basadas en la agricultura y que tenían una cultura y una organización ligadas y limitadas a las propiedades de la tierra. La segunda ola –la de las civilizaciones industriales– poseía características que dividieron a las clases productoras de las consumidoras y que potenciaron la importancia de las ciudades y del empleo en las fábricas. Finalmente, con la decadencia del industrialismo, Toffler asevera que surge una nueva civilización –u ola–, en la que la producción masiva se diversifica, los productores –actores principales de la segunda ola– se asumen a su vez como consumidores (*prosumidores*) de productos y servicios; la generación y distribución de la información se vuelve esencial. Por su parte, el sociólogo español, Manuel Castells identifica tres revoluciones en la economía mundial: la agrícola; la industrial –con dos etapas: la caracterizada por la sustitución de herramientas por máquinas (la máquina de vapor, la hiladora de varios husos) y la basada en el uso de “electricidad, el motor de combustión interna, la química basada en la ciencia, la fusión de acero eficiente y el comienzo de las tecnologías de la comunicación”–;³ y la “revolución tecnológica centrada en torno a las tecnologías de información y comunicación basada en la electrónica, la microelectrónica, los ordenadores y las telecomunicaciones”,⁴ que potencian la existencia de una sociedad red, que a diferencia de las sociedades propias de las otras dos revoluciones, entendía a la información como producto, como materia prima y como el combustible que la echaba a andar. Finalmente, la visión de Simone⁵ en torno a la evolución de las civilizaciones se relaciona con la concepción de “la escritura como medio de conservación del saber”.⁶ Para el lingüista italiano esta evolución también está compuesta por tres fases pero para él son relativas a la formación y conservación del conocimiento: una que parte del invento de los signos escritos como soporte estable para la documentación de sucesos; otra que tiene sentido a partir de la invención de la imprenta y el advenimiento del libro, y una tercera fase en la que el conocimiento circula de formas audiovisuales. Las visiones de evolución estructurada, escalonada y paulatina de Toffler, Castells y Simo-

² Toffler, Alvin, *La tercera ola*, *op. cit.*, nota 1.

³ Castells, Manuel, *The Rise of the Network Society*, *op. cit.*, nota 1.

⁴ *Ibidem*, p. 70.

⁵ Simone, Raffaele, *La tercera fase: formas de saber que estamos perdiendo*, *op. cit.*, nota 1.

⁶ *Ibidem*, p. 11.

ne delinear una sociedad posindustrial, en red y audiovisual, que otros han referido como aldea global;⁷ sociedad informacional;⁸ o sociedad del conocimiento.⁹ En todos los casos refiriéndose a una sociedad donde la información juega un papel preponderante y de carácter global donde las naciones participan simultáneamente en movimientos sociales, culturales y empresariales. Para el estudio que presentamos en este capítulo hemos decidido utilizar la denominación de sociedad de la información para referirnos a una sociedad moderna en la que “la globalización y la informacionalización parecen relacionarse estructuralmente con el funcionamiento en red y la flexibilidad”¹⁰ facilitando el flujo de la información en aquellos que están conectados a la red.

La sociedad de la información representa una evolución social, en la que la visión económica y cultural está cambiando el foco de su atención principal de los procesos industriales de producción a la generación, distribución y procesamiento electrónico de la información. La sociedad de la información es entonces una sociedad posindustrial que se caracteriza por estar conectada y por brindar conectividad a los individuos, por lo que el análisis de ciertos indicadores de conectividad –como el número de usuarios que poseen una computadora, que están conectados a Internet o que disponen de acceso a telefonía móvil– nos permitirán caracterizar a las sociedades que participen cultural, empresarial, social y políticamente en la sociedad –global– de la información.

Sin embargo, los procesos globalizadores son en sí un motivo de marginación social en los que al describir a la sociedad de la cima globalizada¹¹ se hace *de facto* una abyección. Es decir “que cada vez que actualizamos los lenguajes y las metas, en ánimo de lograr mayor y mejor inclusión, también cambiamos los términos para su consecución o las consecuencias de fallar en ello”.¹² Al describir qué es la sociedad de la información y quiénes forman parte de ella –aun cuando no se haga de manera explícita– se describe

⁷ McLuhan, Marshall, *The Gutenberg Galaxy. Making of Typographic Man*, Londres, Routledge and Kegan Paul, 1962.

⁸ Castells, Manuel, *The Rise of the Network Society*, *op. cit.*, nota 1.

⁹ UNESCO, “Toward Knowledge societies”, *UNESCO World Report*, Francia. UNESCO Publishing, disponible en <http://unesdoc.unesco.org/0014/001418/1418#e.pdf>, última fecha de consulta el 12 de mayo de 2014.

¹⁰ Castells, Manuel, *The Rise of the Network Society*, *op. cit.*, nota 1, p. 263.

¹¹ Bauman, Zygmund, *Globalization: The Human Consequences*, Nueva York, Columbia University Press, 1998, p. 9.

¹² Lizarazo Arias, Diego y Andión Gamboa, Mauricio, *Símbolos digitales. Representaciones de las TIC en la comunidad escolar*, México, Siglo XXI, 2013.

a aquellos que no forman parte de las elites extraterritoriales, institucionales, cultas, adineradas, móviles o globales. “Internet y la Red no son para todos, y difícilmente serán algún día de uso universal”.¹³

Esto se debe a que la evolución de Internet no se ha dado de manera homogénea ni en una escala global. Su desarrollo y expansión a nivel mundial ha sido desigual. Si bien Internet surgió en un momento determinado, en sus inicios, su alcance geográfico fue restringido. En 1969, todavía bajo el nombre y modelo de Arpanet, su alcance se limitó al oeste de Estados Unidos¹⁴ para 1973 –después de una expansión nacional– se logró –a través de una conexión satelital– establecer contacto con el Reino Unido y con Noruega;¹⁵ pero no fue sino hasta finales de los años ochenta que Internet se volvió global, y es precisamente en esas fechas cuando el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM), campus Monterrey, se enlazó por primera vez a la red de la *National Science Foundation* (NSFNET), sucesor de Arpanet y antecesor del actual Internet¹⁶ (NIC, 2011). Esta fecha es importante ya que nos permite ubicar el momento en el que la incorporación a la sociedad de la información era factible para México. Es decir, aun cuando Internet, en forma de Arpanet ve la luz en 1969, no fue hasta el “1 de febrero de 1989”,¹⁷ cuando se abre la posibilidad para que México se conecte por primera vez a Internet.¹⁸

La historia de Internet en México tiene cerca de 25 años, lo cual nos permite recordar y hacer evidente que éste es un fenómeno muy reciente cuya evolución no ha sido homogénea ni al interior ni al exterior de sus bordes geográficos. El carácter desigual de esta evolución sugiere la existencia de brechas entre regiones de México y entre países; esto nos permite poner en duda la existencia global de una sociedad de la información y cuestionar

¹³ Bauman, Zygmund, *Globalization: The Human Consequences*, *op. cit.*, nota 11, p. 72.

¹⁴ Véase el mapa de Arpanet en 1969, disponible en <http://mercury.lcs.mit.edu/~jnc/tech/jpg/G69Dec.jpg>, última fecha de consulta el 14 de mayo de 2014.

¹⁵ Véase el mapa correspondiente, disponible en <http://mercury.lcs.mit.edu/~jnc/tech/jpg/G73Sep.jpg>, última fecha de consulta el 20 de junio de 2014.

¹⁶ NIC, “Nuestra historia”, en el sitio de *Network Information Center, México, S.C.*, disponible en <http://www.nicmexico.mx/es/NicMx.Historia>, última fecha de consulta el 2 de junio de 2014.

¹⁷ *Idem.*

¹⁸ Información obtenida de una recopilación de mapas del Grupo de Arquitectura Avanzada de Redes del Laboratorio de Inteligencia Artificial y Ciencias de la Computación perteneciente al Instituto Tecnológico de Massachusetts, <http://mercury.lcs.mit.edu/~jnc/tech/arpageo.html>, que fue utilizada –entre otras fuentes– por VOX en su publicación “40 mapas que explican a Internet”, <http://www.vox.com/a/internet-maps>, última fecha de consulta el 21 de junio de 2014.

los esfuerzos del Estado para impulsar o direccionar la incorporación de las Tecnologías de Información y Comunicación (en adelante TIC) en nuestra sociedad.

Para la elaboración de este texto exploramos diversas fuentes. Las principales, más confiables y sistemáticas, nos permitieron construir las series históricas del periodo comprendido entre 2000 y 2011. Estas fuentes son el Instituto Nacional de Estadística y Geografía (en adelante INEGI) y el Banco Mundial. Del INEGI revisamos los indicadores de “Usuarios de Internet¹⁹ y Telefonía móvil:²⁰ Datos Internacionales de 2000 a 2011” y el módulo de “Disponibilidad y Uso de Tecnologías de la Información 2013”.²¹ Es pertinente mencionar que el INEGI se apoyó en el Consejo Nacional de Población (Conapo), Select, *International Telecommunication Union* (ITU) y en los conteos de población y vivienda que el INEGI mismo realiza, para elaborar estos reportes de datos estadísticos.²² Del Banco Mundial hemos revisado el número de habitantes por país, que son usuarios de Internet por

¹⁹ INEGI, “Usuarios de Internet por cada 100 habitantes por países seleccionados, 2000 a 2011”, disponible en <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tnf142&s=est&c=19452>, última fecha de consulta el 13 de octubre de 2013.

²⁰ INEGI, “Suscriptores de telefonía móvil por cada 100 habitantes por países seleccionados, 2000 a 2011”, disponible en <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tnf146&s=est&c=19453>, última fecha de consulta el 13 de octubre de 2013.

²¹ INEGI, “Disponibilidad y uso de tecnologías de la información en los hogares”, disponible en <http://www3.inegi.org.mx/est/contenidos/proyectos/encuestas/hogares/modulos/endutih/default.aspx>, última fecha de consulta el 13 de octubre de 2013.

²² Para el acceso a Internet internacional se basa en: ITU y para México 2001, 2002 y a partir de 2004: INEGI. Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares. La cifra por cada 100 habitantes es una estimación del Conapo y del INEGI, con base en las Proyecciones de Población 2000-2051 y Proyecciones de Población 2005-2050 del Conapo, y para México 2000 y 2003: Cofetel, Dirección de Tarifas e Integración Estadística, con base en información de Select. La cifra por cada 100 habitantes es estimación del Conapo y del INEGI, con base en los resultados definitivos del II Censo de Población y Vivienda 2005.

Para suscripciones a telefonía móvil internacionales: ITU y para México Cofetel, Dirección de Información de Estadística de Mercados.

Para datos nacionales sobre tecnologías de información y comunicaciones (2001 a 2013) se consideró: INEGI: Módulo sobre disponibilidad y uso de tecnologías de la información en los hogares y el INEGI: Censo de Población y Vivienda 2010, Tabulados del Cuestionario Básico, 2010.

Es pertinente recalcar que para los datos nacionales se considera: el total de viviendas particulares habitadas que no incluye viviendas móviles, refugios y locales no construidos para habitación debido a que no se captaron características de estas clases de vivienda. Asimismo, excluye las viviendas sin información de ocupantes, así como en las cifras de 2013 están conciliadas conforme las proyecciones demográficas del Conapo de abril de 2013. En su oportunidad se presentarán los correspondientes ajustes para años previos.

cada 100 habitantes en los periodos 2000-2013,²³ suscriptores de servicio fijo de banda ancha por cada 100 habitantes²⁴ y los indicadores de desarrollo de México.

Adicionalmente, hemos considerado una serie de mapas y estadísticas que tienen un carácter más informal y de divulgación –por el formato de su publicación– compilados por Vox en su artículo *40 Maps that Explain the Internet*²⁵ y elaboradas por el colectivo internacional *We Are Social* en su publicación sobre estadísticas mundiales de digitalización *Global Digital Statistics 2014*.²⁶

De esta manera, pretendemos establecer –desde una serie de datos estadísticos confiables– un contexto propicio para un entendimiento informado sobre la incorporación de México a la sociedad de la información a partir de los indicadores de acceso a computadora, a Internet y disposición de telefonía móvil desde dos perspectivas: la global y la regional.

II. MÉXICO ANTE LA SOCIEDAD DE LA INFORMACIÓN

La incorporación de México en la sociedad de la información y la apropiación de las TIC por parte de sus habitantes no son hechos naturales que hayan ocurrido por sí solos. Tampoco es una cuestión que debiéramos dejar a las fuerzas libres del mercado. Nosotros lo entendemos como un bien público en el que el Estado tiene responsabilidad de intervenir para favorecer y promover la expansión de las TIC, de manera tal que, como país de manera integral (que implica a los sectores y regiones más desprotegidos), nos podamos incorporar plenamente a la sociedad de la información. Para esta integración no sólo hay que resolver la situación de acceso a la infraestructura tecnológica y a los servicios digitales adecuados, sino también generar las condiciones de apropiación de las TIC para todos los ciudadanos. Para el caso de México, el uso de las TIC ha iniciado relativamente tarde y su desarrollo se ha dado con profunda desigualdad. En esta materia, las bre-

²³ Worldbank (s. f.), “Internet users (per 100 people)”, disponible en <http://data.worldbank.org/indicador/IT.NET.USER.P2>, última fecha de consulta el 24 de junio de 2014.

²⁴ Worldbank (s. f.), “Indicators”. disponible en <http://data.worldbank.org/indicador>, última fecha de consulta el 24 de junio de 2014.

²⁵ Vox (s.f.), “40 maps that explain the Internet”, disponible en <http://www.vox.com/a/internet-maps>, última fecha de consulta el 24 de junio de 2014.

²⁶ We are social, “Social, Digital & Mobile in 2014”, disponible en <http://wearesocial.sg/blog/2014/01/social-digital-mobile-2014>, última fecha de consulta el 24 de junio de 2014.

chas entre México y la mayoría de los países del mundo se amplían condenándonos a una situación de rezago que implica falta de competitividad en un entorno global. Pero eso no es todo, al interior del territorio nacional los contrastes son tan grandes que es posible identificar regiones tan conectadas como el primer mundo, y otras con una situación similar a la de los países más desprotegidos del orbe.

Identificar a 1989 como el año de la potencial llegada de Internet a México, es una afirmación que debemos tomar con mucho cuidado, pues en ese entonces su cobertura era tan pequeña que resultaba, incluso, elitista. Según los datos del Banco Mundial que hemos revisado,²⁷ en el año 2000 solamente cinco mexicanos de cada 100 tenían acceso a la red, mientras que en 2012 ya se había incrementado a 38 personas por cada 100. El crecimiento también se puede ver por el número de dominios .mx, que partieron en 1992 de 45 (40 académicos y cinco comerciales), alcanzando 30 mil dominios en 2000, para llegar, en 2008, a 250 mil dominios .mx.²⁸

Los gobiernos y sus planes y programas nacionales son determinantes para el desarrollo de los países. Tenemos el caso de Brasil y de otros países de América, Europa o Asia, cuyos gobiernos han promovido políticas y fuertes inversiones dando lugar a un alto desarrollo de las TIC. Asimismo, han definido estrategias de educación, conectividad, equipamiento y distribución, que favorecen el despliegue de la sociedad de la información, mientras que en México iniciamos tarde, vamos evolucionando con lentitud y el desarrollo al interior del país es muy desigual. Esta retrasada, lenta y desigual incorporación de México a la sociedad de la información, no sólo es un problema para el presente y el grado de competitividad que tenemos como nación a nivel global, sino que además compromete el futuro del país, y perpetúa su situación de dependencia y de rezago tecnológico frente a otras naciones.

En el siguiente apartado presentamos dos cuadros de datos internacionales en los que mostramos las proporciones de acceso a Internet y la disposición de telefonía móvil por cada 100 usuarios. El objetivo de ambos casos es poner en relación con otros países la evolución, desarrollo, condiciones y posibles proyecciones de incorporación de nuestro país.

²⁷ Referidos con anterioridad disponibles en <http://data.worldbank.org/indicator/IT.NET.USER.P2?page=2>.

²⁸ NIC, "Nuestra historia", en el sitio de *Network Information Center, México, S.C., op. cit.*, nota 16.

III. ACCESO A INTERNET

En el cuadro sobre Usuarios de Internet por cada 100 habitantes podemos encontrar datos reveladores. En primer lugar resultan evidentes las condiciones de desigualdad con que los países van expandiendo el uso de Internet. Hagamos una breve consideración por continentes. En América destaca que Estados Unidos y Canadá ya tenían incorporada casi a la mitad de su población en el año 2000. Y al finalizar el periodo, en 2011, lograron incorporar a más de tres cuartas partes de su población. En cuanto al número de usuarios de Internet, estos dos países tienen una situación de ventaja muy fuerte con el resto de países del subcontinente. Entre los países de América Latina la evolución ha sido muy diversa, hay países que se han transformado muy rápido y otros que avanzan con lentitud; entre los primeros destacan Brasil, Argentina, Chile, Uruguay y Venezuela, que, teniendo una base muy pequeña en 2000, diez años después llevan a la mitad de su población a ser usuarios de Internet. México y Perú, por el contrario, son ejemplo de países con un lento desarrollo, pues habiendo iniciado el siglo en una situación semejante a los otros países de América Latina, al terminar la década apenas estaban incorporando a una tercera parte de su población. En relación con sus competidores, podemos observar que México llega tarde a la incorporación masiva de Internet y que, además, va con retraso en su evolución. Su situación de desventaja es grave, pues la mayoría de los países de América han iniciado con fuerza su inclusión a la sociedad de la información y en México el rezago es grande; mientras que en los países de América del Norte ocho de cada 10 personas tienen acceso a Internet, en México solamente tres de cada 10 acceden a la red.

Este ritmo aletargado y tardío no lo podemos atribuir en abstracto a la condición de país en desarrollo, puesto que Brasil, por ejemplo, que es un país con casi el doble de la población de México y cuyo territorio es notablemente más extenso (17 millones de kilómetros cuadrados comparados con los casi 2 millones de kilómetros cuadrados de México), en el año 2000 partió de una base de 2.87 por cada 100 habitantes y en 2011 había incorporado cerca del 45% de su población. El esfuerzo de ese país es notable y seguramente está asociado no sólo a la expansión global de Internet, sino al desarrollo económico. En la década de estudio, en Brasil cerca de 30 millones de personas salieron de la pobreza extrema y es probable que un buen porcentaje de ellos se haya vuelto usuarios de Internet. Los brasileños han

invertido en conectividad; han distribuido equipos de cómputo, asignado créditos y fomentado la educación, de tal manera que el uso de Internet se ha incrementado considerablemente. Internet no se desarrolla por sí solo, su expansión es producto del desarrollo social. Evidentemente, en la sociedad de la información, los países más tecnologizados tienen condiciones de producir más y de manera más eficiente. La situación de rezago no es una fatalidad, sino que resulta de los proyectos políticos nacionales, donde el esfuerzo de los gobiernos es fundamental.²⁹

La condición de rezago tecnológico no sólo nos explica la situación económica y social contemporánea, sino que anticipa las condiciones de la competencia futura entre las naciones. Considerando el índice de crecimiento de Canadá, China y México, podríamos suponer si las cosas siguen como van, Canadá que partió en el año 2000 de 51.3% y llega en 2011 al 83%, en el año 2016 conectaría al 100% de sus habitantes a Internet; China podría cubrir al 100% de sus habitantes en 16 años; mientras que para México la misma proyección indicaría que la cobertura del 100% no se lograría sino hasta el año 2040.

El desarrollo de la economía contemporánea es global y la competencia por incorporarse a la sociedad de la información es despiadada. En la mayoría de los países del mundo se fomenta que el uso de Internet sea más extendido y claramente se pueden detectar esfuerzos nacionales muy importantes. En Europa destacan Holanda y Suecia que superan el 90%, Francia, Alemania, Inglaterra y otros están alrededor del 80%, e Italia, que es de los bajos, tiene cubierta la mitad de la población.

El caso de Rusia llama la atención, pues además de ser un país inmenso con millones de habitantes, el número de sus usuarios de Internet pasó del 2% al 50% en diez años. Este mismo esfuerzo se observa en Asia, donde destacan los casos de Corea, Japón, Australia y Nueva Zelanda con participaciones alrededor del 80%, Singapur con 75% y Malasia –que sería un país con desarrollo bajo– llega a cubrir al 61% de su población. El caso más relevante de este continente es de otro gigante, China, que pasó de tener incorporado al 1.78% de su población en el año 2000, al 38.3% en 2011; este país no sólo incrementó el tamaño de su población, sino que incorporaron cerca de 520 millones de personas como usuarios de Internet en un plazo relativamente corto. Cabe mencionar que, a pesar de este avance, China sigue teniendo una posición de frágil ganancia, lo cual se explica por las convicciones políticas del régimen chino que supone que el

²⁹ Castells, Manuel, *The Power of Identity (The Information Age: Economy, Society and Culture)*, vol. I, Oxford, Blackwell, 1997.

Cuadro 1. Usuarios de Internet por cada 100 habitantes por países seleccionados en el mundo, 2000 a 2011

<i>Países seleccionados</i>	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Holanda	44	49	61	64	69	81	84	86	87	90	91	92
Suecia	46	52	71	79	84	85	88	82	90	91	90	91
Nueva Zelanda	47	53	59	61	62	63	69	70	72	80	83	86
Corea	45	57	59	66	73	74	78	79	81	82	84	84
Canadá	51	60	62	64	66	72	72	73	77	80	80	83
Alemania	30	32	49	56	65	69	72	75	78	79	82	83
UK	27	33	56	65	66	70	69	75	78	78	78	82
Francia	14	26	30	36	39	43	47	66	71	72	80	80
Japón	30	39	47	48	62	67	69	74	75	78	78	80
Australia	47	53	ND	ND	ND	63	66	69	72	74	76	79
EUA	43	49	59	62	65	68	69	75	74	71	74	78
Singapur	36	42	47	54	62	61	59	68	69	69	71	75
España	14	18	20	40	44	48	50	55	60	62	66	68
Malasia	21	27	32	35	42	49	52	56	56	56	56	61
Italia	23	27	28	29	33	35	38	41	45	49	54	57
Chile	17	19	22	25	28	31	35	36	37	39	45	54
Uruguay	11	11	11	16	17	20	29	34	39	42	46	51
Rusia	2	3	4	8	13	15	18	25	27	29	43	49
Argentina	7	10	11	12	16	18	21	26	28	34	40	48

Brasil	3	5	9	13	19	21	28	31	34	39	41	45
Panamá	7	7	9	10	11	11	17	22	34	39	40	43
Colombia	2	3	5	7	9	11	15	22	26	30	37	40
Venezuela	3	5	5	8	8	13	15	21	26	33	37	40
China	2	3	5	6	7	9	11	16	23	29	34	38
Perú	3	8	9	12	14	17	21	25	31	31	35	37
México	5	7	10	12	12	16	18	20	21	25	30	34

FUENTE: ITU.

Para México 2000 y 2003: Cofetel, Dirección de Tarifas e Integración Estadística, con base en información de Select. La cifra por cada 100 habitantes es estimación del Conapo e INEGI, con base en los resultados definitivos del II Censo de Población y Vivienda 2005. Para México 2001, 2002 y a partir de 2004, INEGI, Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares. La cifra por cada 100 habitantes es estimación del Conapo y del INEGI, con base en las Proyecciones de Población 2000-2051 y Proyecciones de Población 2005-2050 del Conapo.

Fecha de actualización: lunes 22 de octubre de 2013.

uso de Internet puede ser un atentado a la estructura y cohesión ideológica del país, por lo que la existencia de controles, límites y filtros de acceso no son inusuales.

La diferencia de los países más aventajados del cuadro 1 con respecto al avance de México en el periodo estudiado es importante. En todos ellos se han dado pasos efectivos para incorporar a sus ciudadanos a la sociedad de la información con respecto al indicador de acceso a Internet. Si se observa el ritmo de crecimiento mostrado en la última década podemos afirmar que la situación de desventaja de México hacia el futuro va a continuar y probablemente se profundizará.

IV. TELEFONÍA MÓVIL

La telefonía móvil no sólo ha venido a revolucionar las comunicaciones entre las personas, sino que los actuales teléfonos inteligentes o *smartphones* posibilitan el acceso a Internet y, por tanto, pueden ser utilizados no sólo para desarrollar conferencias telefónicas entre personas, sino como recursos de información y transmisión de datos, como cámara fotográfica o como grabadora. “La expansión de las funcionalidades del dispositivo móvil desde la comunicación interpersonal en la movilidad hacia el concepto de centro multimedia de acceso móvil a Internet impone una revisión de los paradigmas de la comunicación social urbana”.³⁰ Los dispositivos móviles son cada día más versátiles y capaces de brindar servicios personalizados y relevantes para sus portadores en función del acceso a la información y a las aplicaciones (*apps*) que se hayan descargado e instalado en el teléfono inteligente.

Los teléfonos móviles se han vuelto un producto de masas, objetos populares entre personas de todas las edades y condiciones sociales, recursos de trabajo casi indispensables para la gente de hoy, símbolos de distinción que diferencian a sus propietarios y poseedores. Hay millones de teléfonos móviles circulando por el mundo, que brindan servicios telefónicos, de mensajería, de transferencia de información y datos, pero que también generan toneladas de basura y contaminación asociada con su producción y desecho.³¹

³⁰ Igarza, Roberto, *Burbujas de ocio: nuevas formas de consumo cultural*, Buenos Aires, La Crujía Ediciones, 2009, p. 21.

³¹ Véase Pánico, Francesco *et al.*, “Una visión integral de las TIC desde la sustentabilidad humana: retos y oportunidades para la universidad del siglo XXI”, en Ramírez-Martinell, Alberto y Casillas, Miguel Ángel (comps.), *Háblame de TIC: tecnología en la educación superior*, Argentina, Brujas, 2014.

El uso de teléfonos móviles es un indicador importante para considerar la incursión en la sociedad de la información. Las estadísticas mostradas en el cuadro 2: Suscripciones a telefonía móvil en el mundo por cada 100 habitantes, representan el número de teléfonos celulares que hay en cada centenar de habitantes, pero en los casos donde el número de celulares excede a 100, la proporción no necesariamente implica que todas las personas tiene acceso a un teléfono móvil, más bien lo que se puede interpretar es que algunas personas tienen más de un celular y otras no cuentan con teléfono móvil alguno. Para México —que no es la excepción— el valor de 84, entonces, no necesariamente representa que 84 de cada 100 personas tienen un teléfono móvil, ya que en estos datos podríamos encontrar a aquellos sin teléfono y a otros con más de un teléfono.

En la actualidad el uso de estos aparatos se ha extendido en todas las naciones de manera muy amplia. Podríamos incluso decir que el teléfono móvil es el dispositivo de la década. Sin embargo, hay diferencias muy importantes que se relacionan con los efectos de las políticas públicas y las iniciativas gubernamentales. Como reflejo de las diferencias en el desarrollo económico y social, podemos identificar un primer grupo de países —primordialmente europeos— que en el año 2000 ya habían logrado extender el uso de la telefonía móvil a un 75% de sus ciudadanos y que prácticamente universalizan su uso (cubren al 100% de sus habitantes) en el año 2006, destacan Italia, Inglaterra y Suecia. Un segundo grupo de países está conformado por aquellos como Alemania y España que en el año 2000 tenían una participación cercana al 50% y que universalizaron la telefonía móvil a mediados de la década. Corea, Japón y Australia iniciaron la década de un modo semejante y en el año 2011 apenas habían incorporado al 80%.

Por lo que respecta a la evolución de China y de Rusia, encontramos similitudes. A principios del siglo XXI el número de suscriptores a la telefonía móvil era muy bajo, 2% y 6% respectivamente. Rusia superó el 100% en 2006 y China ha logrado incorporar al final del periodo a 70% de los habitantes. Puede parecer una proporción todavía baja, pero en China el incremento representó que mil millones de personas tuvieran acceso a esta tecnología. Si bien el incremento porcentual de China es bajo, esto se debe a su numerosa población.

Por su parte, en el año 2000 la enorme mayoría de los países de América Latina tenían bajos porcentajes de participación y en 2011 lograron universalizar el uso de los dispositivos móviles. A contrapelo de todas estas tendencias internacionales, la evolución de México en cuanto al uso de teléfonos móviles es lenta y supera apenas al 80% de los habitantes.

Cuadro 2. Suscripciones a telefonía móvil en el mundo por cada 100 habitantes, 2000 a 2011

<i>Países seleccionados</i>	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Panamá	14	16	17	22	40	54	66	90	115	175	189	204
Rusia	2	5	12	25	51	83	105	119	139	161	166	179
Italia	74	90	94	98	108	122	136	151	151	146	150	152
Singapur	70	75	82	88	96	103	109	129	134	139	145	149
Uruguay	12	16	15	15	18	35	70	90	105	122	132	141
Argentina	18	18	17	21	35	57	81	103	117	131	133	135
Alemania	59	68	72	79	86	96	104	117	128	127	127	132
UK	74	78	83	91	100	109	116	121	125	130	131	131
Chile	22	33	40	46	57	65	76	84	88	97	116	130
Malasia	22	31	37	44	57	75	73	86	101	108	119	127
Brasil	13	16	19	26	36	46	53	64	79	90	104	123
Holanda	68	76	75	82	91	97	106	117	125	122	115	119
Suecia	72	81	89	99	98	101	106	110	108	112	116	119
España	60	73	81	89	90	98	104	109	110	112	112	114
Perú	5	7	9	11	15	20	33	55	74	86	100	110
Nueva Zelanda	40	59	62	65	74	85	91	100	108	109	108	109
Corea	58	63	70	72	78	82	85	93	96	100	105	109
Australia	45	57	65	72	82	90	95	101	103	101	101	108
EUA	39	45	49	55	63	69	77	82	86	89	90	106

Francia	49	62	65	69	74	79	84	90	93	95	101	105
Japón	53	59	64	69	72	76	79	85	87	92	97	103
Colombia	6	8	11	15	25	51	68	77	92	92	96	98
Venezuela	22	26	26	27	32	47	69	86	98	99	96	98
México	14	22	25	29	36	45	53	63	70	77	81	84
Canadá	28	34	38	42	47	53	57	61	66	71	71	75
China	7	11	16	21	26	30	35	41	48	56	64	73

FUENTE: ITU. Para México Cofetel. Dirección de Información de Estadística de Mercados.
Fecha de actualización: lunes 22 de octubre de 2013.

Paradójicamente, mientras que en México tiene su sede una de las más importantes compañías mundiales de telefonía y su propietario es el hombre más rico del planeta, nuestro país vive una marcada condición de rezago frente a la mayoría de las naciones del mundo en cuanto a la expansión y uso de la telefonía móvil. No sólo llegamos tarde comparativamente con otros países, sino que hemos evolucionado con tremenda lentitud. Si los teléfonos móviles son un recurso de comunicación cada día más habitual, en México los flujos aún están restringidos a un grupo y las telecomunicaciones no tienen una capacidad que tienda a ser universal para todos los ciudadanos de este país. Si los móviles son una herramienta para las nuevas formas del trabajo, en nuestro país todavía hay miles de personas que no disponen de esos recursos y eso les imposibilita incorporarse productivamente a la nueva economía. Si los teléfonos móviles más nuevos y desarrollados –también los más caros y exclusivos– son instrumentos de transferencia de datos y de información, miles de mexicanos están quedando al margen de su uso, ubicándose en clara situación de desventaja social frente a los trabajadores y ciudadanos de otras naciones.

El desarrollo reciente de México observado en la última década nos permite comprobar la insuficiencia de las acciones públicas, la ausencia de planes y políticas de desarrollo tecnológico eficientes y la ausencia de incentivos económicos para favorecer el uso de las TIC. No hay una estrategia nacional con metas claras ni ha habido acciones que tuvieran continuidad. En la comparación internacional observamos como todas las naciones evolucionan positivamente, incrementando el número de usuarios de Internet y de telefonía móvil, mientras que en México esta evolución es aletargada y carente de un plan de desarrollo inclusivo.

La evolución de las TIC entre los países no ha sido homogénea. Está marcada por el tipo de configuración económica-social³² que los distingue como desarrollados y subdesarrollados. En efecto, al inicio del siglo XXI parecía determinante que la sociedad de la información se desplegaría de modo muy diferenciado y se concentraría entre los países del primer mundo. Sin embargo, lo que observamos en su primera década es como muchas de las naciones más pobres y atrasadas se pusieron manos a la obra para promover la incorporación de las TIC entre sus ciudadanos y lograron –en el 2011– cerrar la brecha con las naciones más desarrolladas. Desafortunadamente éste no es el caso de México.

³² Elías, Norbert, *La sociedad cortesana*, México, Fondo de Cultura Económica, 1982, y Zabludovsky Kuper, Gina, *Norbert Elías y los problemas actuales de la sociología* (s. 1.), España, Fondo de Cultura Económica, 2007.

V. EL DESARROLLO DESIGUAL EN MÉXICO

Una foto de la situación de México en la actualidad puede ser suficiente para observar el desigual desarrollo de las TIC en nuestro país y reconocer las diferencias que distinguen a las entidades federativas y a sus ciudadanos. El crecimiento desigual es expresión del desarrollo regional y de la desigual distribución de las oportunidades sociales. También es expresión del fracaso de las políticas federales, que han sido incapaces de formular un desarrollo con equidad.

Según los datos del INEGI, en 2013 en México había un 46.7% de habitantes que disponían de una computadora y 43.5% eran usuarios de Internet. Este promedio nacional –de por sí bajo en la comparación internacional– esconde profundas diferencias entre las entidades federativas del país. Hay entidades como el Distrito Federal, Nuevo León, Jalisco, Colima y Coahuila que superan el promedio y tienen indicadores semejantes a los del primer mundo: el Distrito Federal, por ejemplo, tiene 63% de usuarios de computadora y 60.5% de usuarios de Internet, mientras que en el extremo contrario, tenemos a entidades como Chiapas, Guerrero, Oaxaca o Veracruz, que se encuentran por abajo del promedio nacional y con indicadores parecidos a los países más atrasados del planeta. En Chiapas sólo hay un 26.4% de usuarios de computadoras y 24% de usuarios de Internet. Las diferencias interregionales son muy fuertes. Verdaderas brechas diferencian las oportunidades sociales de los habitantes de unas y otras regiones del país y dan lugar a un desarrollo muy desigual.

Otra vez, como en el caso de la comparabilidad internacional, al interior de nuestro país estas enormes diferencias en términos de la expansión en el uso de las TIC, hacen que la competencia estructurada en el marco de la sociedad de la información sea muy desigual e inequitativa. El epítome de la sociedad de la información es un usuario conectado a Internet. Para lograr conectar a los habitantes de un país, es necesario resolver la cuestión del acceso al dispositivo y a la red. En un país como México, donde no todos tienen acceso a equipos y redes públicas, la posición de dispositivos conectados a Internet es entonces el boleto de entrada a la sociedad de la información.

Ahora bien, se podría pensar que las personas que no tienen computadora o acceso a Internet es porque no les interesa o porque consideran que no es útil, pero los datos del INEGI nos muestran que la principal razón por la que una persona no tiene computadora es principalmente la falta de recursos económicos. Esta razón se mantiene en el tiempo, pues en 2001 así

respondió el 66% de la población y en 2013 así lo siguió haciendo el 61%. En resumen, eran y siguen siendo razones económicas las que alejan a las personas de la posesión de equipos de cómputo, y a pesar de que en México los precios de las computadoras han bajado notoriamente y que han surgido en estos años computadoras de bajo costo –laptops de \$12 000 pesos mexicanos que pueden ser sustituidas por pequeñas laptops o *netbooks* de \$3 500–, la falta de recursos económicos de los ciudadanos sigue siendo la razón principal para determinar quién sí y quién no tiene oportunidad de adquirir una computadora.

Sobre el acceso a Internet, las cosas son semejantes. Aun cuando la razón principal que separa a las personas de una conexión a Internet, es igualmente económica, hay un cambio importante en las percepciones de la población. En 2000, el 26% desconocía su utilidad, mientras que hoy sólo 2% la desconoce. Hay una percepción general de que Internet es útil y a la población le interesa; es decir, cada día le interesa a más personas y la necesitan, pero no tienen recursos para conseguir acceso a la red. A partir de esto podemos decir que en México poseer una computadora –con acceso a Internet– todavía representa un lujo. Por ende, no podemos afirmar que México en su totalidad está conectado y que participa en la sociedad de la información.

El acceso a Internet juega un papel importante en la expansión de las TIC, y los datos recientes sugieren que la computadora e Internet han dejado de ser obligaciones o herramientas escolares y laborales, para incorporarse al hogar. El acceso tiende a diversificarse en muchos espacios sociales. En 2001 el acceso se daba principalmente en la escuela (41%), en el hogar (42%) y en el trabajo (30%). En 2013 el acceso a Internet en el hogar se ha incrementado hasta un 59%, mientras que en el trabajo y la escuela disminuyen a 22% y a 21% respectivamente. Esto implica que Internet se salió de los contextos escolares y laborales para meterse a los hogares y a sitios públicos permitiendo a las personas acceder a la red con fines distintos a los que se podían utilizar en los contextos formales. Los sitios públicos con acceso a Internet –como café Internet, parques públicos– tuvieron un incremento de 16% en 2001 a 33% en 2013.

Los usos de la computadora e Internet evolucionaron en este periodo. Como era de esperarse los usos (primordialmente de procesador de texto y hoja de cálculo) escolares y laborales bajaron relativamente, de un 59% a 49%, para apoyo escolar y de 38% a 28%, para apoyo en el trabajo. En el rubro de entretenimiento, hubo un incremento de 37% a 45%, pero el cambio más relevante se dio en lo que respecta a comunicación mediada por computadora que en 2001 parte de 22% para llegar a 58% en el año 2013.

El uso actual predominante de la computadora es para satisfacer necesidades de comunicación. La computadora está dejando de tener un uso (exclusivo) académico y laboral, y se expande como objeto cultural proveedor de opciones recreativas, de entretenimiento y diversión, que podrían incluir el consumo de música, videos, películas, videojuegos y procuración de redes sociales.

Este cambio de paradigma de los usos de las computadoras se observa también en el uso de los programas informáticos. En 2001 la prioridad era usar procesadores de texto (69%), seguido de las hojas de cálculo (39%) y el manejo de base de datos y lenguaje de programación (39%). En ese momento —y con sólo un 5% de usuarios conectados a Internet— la comunicación se situaba en un lugar no muy favorable con un 14%. Pero en 2013 la situación cambió. Los programas de comunicación se colocaron como los más comunes entre los usuarios con un 49%, y todos los programas de “oficina” perdieron su popularidad (procesador de texto tiene 33%, las hojas de cálculo 10% y los programas de manejo de base de datos y lenguaje de programación 17%). Con esto podemos observar que México ha incrementado sus indicadores en materia de comunicación. Los mexicanos están más comunicados que antes. Internet, la telefonía móvil y la computadora indican que vamos hacia una sociedad —más que de la información— de la comunicación.

Asimismo, podríamos decir que en el año 2000 había una brecha entre personas según su nivel académico, es decir, la escolaridad era un factor que determinaba el acceso y el uso de computadoras. La computadora inicia el periodo de análisis siendo una herramienta en educación superior, situación que cambia en 2013 pues ahora se ha diversificado el tipo de usuarios entre personas con muy diferentes escolaridades. En 2000, el grupo de los usuarios que tenía licenciatura era el sector prioritario con un 30%. En 2013 esto cambió, en todos los niveles escolares se empieza a usar la computadora en proporciones similares. De 2001 a 2004 hay un crecimiento de 13% a 21% en el nivel primaria, quizá debido a la puesta en marcha de Enciclomedia.

En el mismo sentido que la escolaridad, cada vez es más acentuada la diversificación etaria de los agentes sociales que utilizan las TIC. Destaca cómo los niños y los grupos de mayor edad incrementan su participación porcentual, rompiendo el mito de que las TIC son un asunto exclusivamente juvenil. En el cuadro 5, podemos observar que en 2001 el grupo de edad que más utilizaba las computadoras era el de 18 a 24, que coincide con la edad promedio de los estudiantes de licenciatura, que representaba al grupo de usuarios con más disposiciones para utilizar dichas herramientas. También podemos ver que en 2011 los niños de 6 a 11 años, usuarios de tecno-

Cuadro 3. Usuarios de computadora en México por tipo de uso por cada 100 habitantes

<i>Tipo de uso</i>	2001	2002	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Comunicarse	22	7	7	21	23	24	31	36	44	49	49	58
Apoyo escolar	60	55	53	60	59	60	57	53	53	52	52	50
Entretenimiento	38	13	16	31	31	28	29	40	38	40	40	47
Apoyar/realizar trabajo	38	33	31	34	32	30	32	30	32	29	30	28
Otro uso	2	1	2	2	2	2	2	2	2	3	2	2

FUENTE: INEGI. Módulo sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares.
 Fecha de actualización: miércoles 27 de noviembre de 2013.

Cuadro 4. Usuarios de computadora según el nivel de escolaridad

<i>Nivel de escolaridad</i>	2001	2002	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Usuarios de computadora	100	100	100	100	100	100	100	100	100	100	100	100
Primaria	13.3	15.3	21	20.4	22.4	23.6	21.5	21.3	21.8	22.3	22.4	22.1
Secundaria	26	25.9	25.5	22.8	22.4	22	22.5	24.5	23.4	24.5	24.3	24.1
Preparatoria	28	27.7	23.6	27.6	27.8	25.3	25.7	26.8	27.7	27.4	27.2	27.7
Licenciatura	30.1	28.8	25.8	25.3	22.8	24.5	25.6	23.4	22.8	21.9	22.2	21.8
Posgrado	1.8	1.3	2.3	2.1	2.3	2.2	2.3	2	1.7	1.6	1.8	2
Otro / No especificado	0.7	1.1	1.8	1.9	2.2	2.4	2.3	2	2.5	2.4	2.1	2.3

FUENTE: INEGI. Módulo sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares.
 Fecha de actualización: miércoles 27 de noviembre de 2013.

logía digital, se duplicaron y que los adultos mayores de 45 años pasaron de 9% a 12%, lo que sugiere que el uso de computadoras —quizás por su entrada al hogar y diversificación de uso— se amplió ligeramente a grupos etarios que al inicio de la década no hacían uso de ellas.

Las diferencias sociales y regionales son tan grandes en nuestro país que es difícil hablar de una plena incorporación a la sociedad de la información. Los estados del norte y el Distrito Federal guardan profundas diferencias con los estados que se encuentran al sur del país. México es un país de enormes desigualdades sociales y de grandes contrastes. Cuando analizamos lo que sucede al interior del país, las diferencias son dramáticas, y el promedio nacional de acceso a computadoras no representa la realidad del país. En los estados como Baja California, Baja California Sur, Nuevo León, Sonora, Jalisco y el Distrito Federal la disponibilidad de computadoras es de más del 57%, mientras que en estados como Chiapas, Oaxaca y Guerrero el indicador no supera al 33% de disponibilidad entre sus viviendas. Si vemos los índices de desarrollo humano, de modernidad política y de educación, la geografía es básicamente la misma. Podemos entonces concluir que el despliegue de la sociedad de la información depende de factores estructurales que definen el subdesarrollo a nivel regional.

Si observamos la disponibilidad de teléfonos móviles, nuevamente son los estados del sur, los más pobres y de mayor concentración de población indígena (Chiapas, Guerrero y Oaxaca) los menos favorecidos. Cuando el promedio nacional es de un 65%, el promedio de estos estados es inferior a 44%; el contraste con los estados del norte es mayor, pues Sonora, Baja California y Baja California Sur superan el 80% de disponibilidad de teléfono móvil. Quintana Roo es una excepción en este contraste norte-sur, pues también supera el 80% de usuarios de telefonía móvil, debido a que es una entidad con un fuerte desarrollo turístico internacional y un amplio desarrollo de las comunicaciones.

En cuanto a usuarios por computadora, el promedio nacional es 46%, pero con una desviación estándar inmenso. El Distrito Federal alcanza un 63% mientras que Chiapas apenas tiene el 26%. Es decir, que mientras que en el Distrito Federal más de la mitad de la población utiliza una computadora, en Chiapas esta proporción apenas llega a la cuarta parte de la población. Y aun así debemos hacer notar que el Distrito Federal no llega a los estándares de países desarrollados como Canadá, Estados Unidos, Japón o Francia.

En lo que respecta a los índices de posesión de computadora y conexión a Internet las diferencias son todavía de mayor tamaño. En México hay zonas donde la sociedad de la información es imposible. El esfuerzo que de-

Cuadro 5. Usuarios de computadora según su grupo de edad

<i>Grupos de edad</i>	2001	2002	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
	100	100	100	100	100	100	100	100	100	100	100	100
6 a 11	4.7	3.8	5.4	6.3	7.1	7.7	7.3	8	9.7	11.4	11.5	11.7
12 a 17	26.7	23.6	25.5	27.6	28.3	29.2	28.6	29.1	26.5	25.6	24.2	23.6
18 a 24	29.1	30.3	26.1	26.2	26.1	23.9	24.8	23	23	21.5	20.6	20.9
25 a 34	18.3	22.2	21.4	18.2	18.2	17.1	16.6	17.2	17.3	17.5	19.4	18.1
35 a 44	12	11.1	13.2	11.5	9.9	12.1	11.6	12.8	12.3	12.5	12.1	13.2
45 a 54	6.1	6.5	5.9	7.2	7.2	6.6	7.7	6.5	7.4	7.7	7.6	8.1
55 años y más	3	2.3	2.4	2.9	3.1	3.4	3.5	3.4	3.8	3.9	4.7	4.3

FUENTE: INEGI, Módulo sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares.
 Fecha de actualización: miércoles 27 de noviembre de 2013.

bemos realizar como país para incorporar a todas las entidades federativas con proporciones altas de usuarios de las TIC es enorme y no será resultado del azar, sino de políticas efectivas que tengan como propósito un desarrollo más igualitario en el país.

Para hacer evidentes estas diferencias, hemos propuesto un indicador nacional de incorporación a la Sociedad de la información (iSi) construido a partir de la sumatoria directa del número de personas en cada 100 usuarios en los tres rubros que presentamos en este texto: Usuarios de computadora, Usuarios de Internet, Usuarios de telefonía móvil.

El valor máximo esperado de este índice es de 300 (100 por cada uno de los tres rubros); y la media nacional es de 156. A partir de ahí podemos observar tres grupos de estados con condiciones distintas de participación en la sociedad de la información. Los que se encuentran por arriba de la media nacional y que prácticamente tienen cubierto en los tres rubros al menos al 50% de su población son: Coahuila con 177; Chihuahua con 179; Colima con 183; Jalisco con 184; Quintana Roo con 185; Nuevo León con 190, Baja California Sur con 198; Sonora y el Distrito Federal con 200; y Baja California con 204. Los que oscilan alrededor de la media nacional son Durango con 145, Guanajuato con 147; Campeche con 148; Yucatán con 149; Querétaro con 155; México, Nayarit y Morelos con 160; Sinaloa con 172; Tamaulipas con 175 y Aguascalientes con 176. Y finalmente, los que se encuentran muy por debajo de 156 y que solamente en el rubro de telefonía móvil presentan –en algunos casos– valores superiores al 50%. Estos estados son: Chiapas con 91; Oaxaca con 103; Guerrero con 106; Michoacán con 126; Puebla con 127; San Luis Potosí con 128; Hidalgo con 129; Veracruz con 132; Tabasco con 134 y Tlaxcala con 137. Esta información se puede ver en el cuadro 6.

VI. CONCLUSIONES

La primera comprobación que debemos señalar en una perspectiva comparada a nivel global es que México ingresó tarde a la sociedad de la información, que ha evolucionado con lentitud y que su desarrollo actual es muy inferior a todos los países desarrollados, y es inferior a la mayoría de los países de América Latina y otros con desarrollos económicos semejantes. Esta situación de atraso y de lento desarrollo no es resultado de la casualidad, ni una fatalidad natural sino de la carencia de planes nacionales inclusivos y contundentes. Lo que observamos con la comparación internacional es que hay países que han hecho esfuerzos importantes y diseñado políticas

Cuadro 6. Indicador nacional de incorporación a la Sociedad de la información (iSi)

<i>Entidad federativa</i>	<i>Usuarios por computadora</i>	<i>Usuarios de Internet</i>	<i>Usuarios de telefonía móvil</i>	<i>MiSi</i>
Baja California	60	58	86	204
Distrito Federal	63	61	77	200
Sonora	60	57	83	200
Baja California Sur	56	55	88	198
Nuevo León	57	55	78	190
Quintana Roo	53	51	80	185
Jalisco	55	52	77	184
Colima	55	51	77	183
Chihuahua	54	49	77	179
Coahuila de Zaragoza	53	49	75	177
Aguascalientes	54	51	72	176
Tamaulipas	51	48	76	175
Sinaloa	50	46	77	172
Morelos	48	46	66	160
Nayarit	48	44	68	160
México	48	45	67	160
Estados Unidos Mexicanos	47	44	66	156
Querétaro	43	41	71	155
Yucatán	42	39	68	149

Campeche	44	40	65	148
Guanajuato	44	41	62	147
Durango	44	38	64	145
Tlaxcala	43	39	56	137
Tabasco	36	34	65	134
Veracruz de Ignacio de la Llave	39	35	58	132
Hidalgo	39	36	54	129
San Luis Potosí	38	34	56	128
Puebla	41	37	49	127
Michoacán de Ocampo	35	30	61	126
Guerrero	33	31	43	106
Oaxaca	34	29	40	103
Chiapas	26	24	41	91

FUENTE: INEGI, Módulo sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares.
Fecha de actualización: miércoles 27 de noviembre de 2013.

eficientes para favorecer la incorporación de las TIC y el incremento en el número de los ciudadanos que las utilizan.

Las diferencias entre los países eran muy fuertes al inicio del siglo XXI, sin embargo, a lo largo de su primera década observamos como la enorme mayoría de las naciones logran expandir el número de usuarios de computadoras, de teléfonos móviles y de Internet. Se trata de estrategias nacionales para incorporarse plenamente a la sociedad de la información y competir con ventaja en la economía global.

Si miramos hacia el interior del país, las diferencias son muy profundas. Los promedios nacionales opacan las grandes brechas que distinguen a los estados. Observamos fuertes contrastes entre las entidades más desarrolladas en sus economías y con los mejores índices de desarrollo humano y las entidades con fuerte población indígena, escaso desarrollo económico y fuerte marginalidad. Estas oposiciones se expresan claramente entre el norte y el sur del país. Evidentemente, dada la estructura centralista de la nación, el Distrito Federal es la entidad con más alto desarrollo en materia de TIC. Una aparente coincidencia nos permite distinguir entre las entidades con mayor desarrollo de TIC y aquellas en las que predomina el atraso: en las primeras han ocurrido procesos de modernización política (alternancia en el gobierno estatal, transición democrática, etcétera) mientras que en las segundas sigue sin darse la alternancia política y la transición a la democracia no acaba de realizarse.

La sociedad de la información implica un uso intensivo de los medios electrónicos. Las computadoras, los teléfonos móviles y su conexión a Internet son recursos imprescindibles para la nueva economía global. La mayoría de las naciones lo han comprendido y sus gobiernos han emprendido acciones para ampliar la cobertura y la utilización de las TIC. México, como muchos otros países, llegó con atraso relativo a su incorporación pero a diferencia de la gran mayoría, su evolución y desarrollo reciente ha sido lento y muy desigual hacia su interior. En efecto, mientras que muchas naciones iniciaron el siglo XXI en una situación semejante a la de México, después de una década, han sido mucho más activas y han puesto en práctica políticas inclusivas exitosas. China, Rusia, Brasil y otras naciones han incorporado a millones de nuevos usuarios de TIC en la última década; México, por su parte, tiene un lento crecimiento que nos condena a una situación de desventaja en la competencia global.

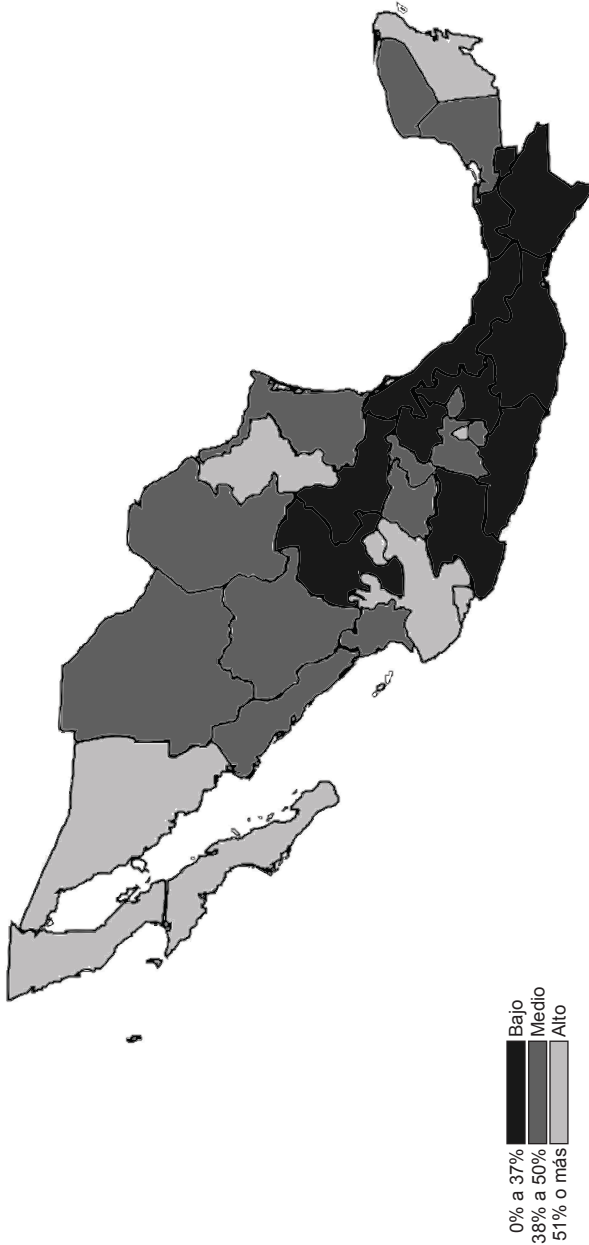
A pesar de que comparativamente con otras naciones México ha evolucionado lentamente y con retraso, podemos observar una franca expansión en el uso de las computadoras, los teléfonos móviles y la conexión a Internet. Cada día se incorporan nuevos usuarios y la cultura digital se instala

progresivamente entre las prácticas cotidianas de los mexicanos. Durante el periodo que estudiamos no sólo se ha incrementado el número de usuarios, sino que también se ha transformado el sentido con que se utilizan estas tecnologías. En la revisión que hemos realizado podemos identificar algunos rasgos del cambio que ha ocurrido en la última década en el sentido del uso de las TIC. Primero, los criterios de uso que predominaban en el año 2000 eran los relativos a la productividad, uso de correo electrónico, *chat* y educación. Al final del periodo hay una mayor diversificación de uso. Ahora los criterios de utilización incluyen a los anteriores y se han extendido principalmente en cuestiones de comunicación, recreativas y lúdicas. En este mismo sentido, podemos ver como la computadora dejó de ser una herramienta estrictamente educativa, académica, formal y laboral, para volverse una cuestión mucho más diversa que al final de la década potenció aspectos propios de una ciudadanía en un entorno digital, al llevar a la comunicación medida por dispositivos digitales a niveles de participación ciudadana, denuncia, infoactivismo y comunicación.

Un segundo rasgo concierne al tipo de usuarios, pues ha dejado de ser cierto que es un asunto exclusivo de jóvenes. Durante el periodo no sólo aumenta el número de usuarios entre todos los grupos etarios, sino que se duplica la participación porcentual de los niños y crece significativamente el de los mayores de 55 años. De acuerdo con lo anterior, podemos observar que la computadora se popularizó hacia los niveles extremos y hacia todos los estratos sociales, no necesariamente los de más alto capital escolar. Tecnológicamente hablando durante el periodo ocurrió un cambio muy significativo en términos del acceso a Internet por línea telefónica dedicada. Mientras que en 2001 la línea telefónica dedicada cubría casi la totalidad (95%) de la forma de conexión a Internet, en 2013 sólo el 3% de los que tienen acceso a la red lo hacen a través de ese medio. Hoy predominan las conexiones asociadas a los servicios telefónicos y de televisión por cable en paquetes de telefonía, acceso a Internet y televisión por cable. La banda ancha, y las conexiones inalámbricas se han expandido dentro y fuera del hogar y la tendencia apunta a la apertura de zonas de wi-fi gratuito.

En relación con la incorporación de las TIC, el esquema internacional se repite al interior de la república. Somos un país muy desigual y las diferencias en términos económicos, de desarrollo humano, de educación y de modernidad política son muy profundas entre los estados, tenemos entidades federativas muy desarrolladas y otras sumamente subdesarrolladas. Hablamos de un país de enormes desigualdades tecnológicas en todos los niveles geográficos. A nivel nacional existen brechas que tienen una extensión grave, pues algunos estados han logrado índices de desarrollo cercanos

Mapa 1. Usuarios de Internet por entidad federativa, 2013



FUENTE: INEGI. Módulo sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares.
Fecha de actualización: miércoles 27 de noviembre de 2013.

a los de los países del primer mundo mientras que otros tienen a la enorme mayoría de su población desconectada y fuera de la cultura digital. El mapa 1 ilustra esta situación.

Como puede observarse, son muy diferentes las oportunidades que tienen los ciudadanos mexicanos para incorporarse a la sociedad de la información. El problema es grave y debe ser un asunto de interés público y objeto de políticas específicas que permitan crecer más a los que más lo necesitan. Si no se entiende que el desarrollo nacional implica que todos estos estados pintados de rojo tienen que transitar y evolucionar más rápido para ser estados más modernos, más desarrollados, más económicamente potentes, si no hay ese proyecto nacional que nos impulse de manera igualitaria, el desarrollo se seguirá fomentando de un modo desigual donde los estados que más tienen seguirán teniendo más y aquellos más pobres seguirán condenados a la marginalidad y la pobreza. En términos de la competencia global, podríamos plantear la conjetura de que en México se están desarrollando regiones con mayores posibilidades de participar en la nueva economía y que otras están en riesgo de quedar excluidas, lo que al final terminará afectando a la nación entera.

Para que nuestro país alcance un nivel de desarrollo tecnológico como el de los países desarrollados debe plantearse en principio la superación de las brechas que oponen a las regiones y estados entre sí. Esto no podrá realizarse si las cosas siguen el curso que llevan; la simple reproducción de las estrategias seguirá produciendo desigualdad social. Es imprescindible un cambio de rumbo y éste debe comprometer al Estado para que se diseñen políticas de dotación, fomento y conectividad capaces de permitir que las regiones más desfavorecidas alcancen a las más desarrolladas y conjuntamente avancemos como país para estar en mejores condiciones de competir a escala global y de incorporarnos plenamente a la sociedad de la información.

VII. BIBLIOGRAFÍA

- BAUMAN, Zygmund, *Globalization: The Human Consequences*, Nueva York, Columbia University Press, 1998.
- CASTELLS, Manuel, *The Rise of the Network Society*, The Information Age: Economy, Society, and Culture, vol. I, Oxford, Blackwell Publishers, 1996.
- , *The Power of Identity*, The Information Age: Economy, Society and Culture, vol. II, Oxford, Blackwell Publishers, 1997.
- ELIAS, Norbert, *La sociedad cortesana*, México, Fondo de Cultura Económica, 1982.

- IGARZA, Roberto, *Burbujas de ocio: nuevas formas de consumo cultural*, Buenos Aires, La Crujía Ediciones, 2009.
- INEGI, *Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares*, México, 2001.
- , *Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares*, México, 2002.
- , *Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares*, México, 2004.
- , *Usuarios de Internet por cada 100 habitantes por países seleccionados, 2000 a 2011*, 2012, recuperado el 13 de octubre de 2013, <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tnf142&s=est&c=19452>.
- , *Suscriptores de telefonía móvil por cada 100 habitantes por países seleccionados, 2000 a 2011*, 2012, Recuperado el 13 de octubre de 2013, <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tnf146&s=est&c=19453>.
- , *Disponibilidad y Uso de Tecnologías de la Información en los Hogares*, 2013, Recuperado el 13 de octubre de 2013, <http://www.inegi.org.mx/est/contenidos/proyectos/encuestas/hogares/modulos/endutih/default.aspx>.
- , *Módulo sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares*, 2013, recuperado el 27 de noviembre de 2013.
- ZABLUDOSKY KUPER, Gina, *Norbert Elias y los problemas actuales de la sociología*, México, Fondo de Cultura Económica, 2007.
- LIZARAZO, Diego y ANDIÓN, Mauricio, *Símbolos digitales. Representaciones de las TIC en la comunidad escolar*, México, Siglo XXI, 2013.
- MCLUHAN, Marshall, *The Gutenberg Galaxy. The Making of Typographic Man*, Londres, Routledge and Kegan Paul, 1962.
- NIC, “Nuestra historia”, recuperado el 2 de junio de 2014 del sitio de Network Information Center, México, S.C., 2011, <http://www.nicmexico.mx/es/NicMx.Historia>
- PÁNICO, Francesco *et al.*, *Una visión integral de las TIC desde la sustentabilidad humana: retos y oportunidades para la universidad del siglo XXI*, en RAMÍREZ-MARTINELL, Alberto y CASILLAS, Miguel (comps.), *Háblame de TIC: Tecnología digital en la educación superior*, Córdoba, Argentina, Brujas, 2014.
- SIMONE, Raffaele, *La tercera fase: formas de saber que estamos perdiendo*, México, Taurus, 2001.
- TOFFLER, Alvin, *La tercera ola*, Ediciones Nacionales, Círculo de Lectores, Colombia, Edinal, 1981.

- UNESCO, “Toward knowledge societies”, *UNESCO World Report*, Francia, UNESCO Publishing, 2005, recuperado el 12 de mayo de 2014, <http://unesdoc.unesco.org/images/0014/001418/141843e.pdf>.
- WORLD BANK. (s.f). *Internet users (per 100 people)*, recuperado el 24 de junio de 2014, <http://data.worldbank.org/indicator/IT.NET.USER.P2>.
- , “Indicators”. Recuperado el 24 de junio de 2014, <http://data.worldbank.org/indicator>.
- VOX (s.f). “40 Maps that Explain the Internet”, recuperado el 24 de junio de 2014, <http://www.vox.com/a/internet-maps>.
- WE ARE SOCIAL, “Social, Digital & Mobile in 2014”, recuperado el 24 de junio de 2014, <http://wearesocial.sg/blog/2014/01/social-digital-mobile-2014/>.

AGRADECIMIENTOS

Los autores de este texto quieren agradecer a los integrantes del Seminario Recursos y Medios Digitales para la Educación de la maestría en Educación Virtual de la Universidad Veracruzana, con quienes reflexionamos y discutimos el tema, doctora Denise Hernández y Hernández; maestras Ana Teresa Morales Rodríguez, Karla Paola Martínez Ramila y Verónica Ortiz Mena; licenciados José Luis Aguilar Trejo, César Augusto Borromeo García, Jonathan Martínez Ladrón de Guevara, así como a Brenda Leñero, y especialmente a Monserrat Rodríguez, quien nos apoyó en las cuestiones editoriales de este documento.

LOS SUJETOS DE LA SIC*

Federico César LEFRANC WEEGAN**

SUMARIO: I. *Un don*. II. *El nativo digital, un sujeto epistemológico de la sociedad digital posmoderna*. III. *Navegantes*. IV. *Fénix*. V. *Los costos no visibles*. VI. *Conclusiones*. VII. *Bibliografía*.

Si seguimos la historia del derecho, veremos que costó muchos esfuerzos que se reconocieran los mismos derechos a todas las personas, y que éstos, fueran reconocidos en las Constituciones de cada país. Fue igualmente difícil que cada Estado se asumiera como protector y promotor de los derechos humanos, en los llamados Estados constitucionales de derecho.¹ En ese modelo el Estado es el garante de los derechos, y a México esa concepción amplia del ser humano portador de derechos, llegó apenas en 2011. Sin embargo, con el desarrollo de la Sociedad de la Información y del Conocimiento—hoy también interpretada como Sociedad de la Información y de la Comunicación— esta perspectiva se transforma vertiginosamente.

Sobre las siglas SIC conviene hacer la siguiente observación. La UNESCO, por ejemplo, tiene una oficina para la información y la comunicación, y en general, hoy estos dos términos se vinculan complementándose entre ellos.² De manera que las siglas SIC, que tradicionalmente se han venido leyendo como relacionadas con la información y el conocimiento, ahora, en la segunda década del siglo XXI, me parece que han ajustado su significado, a otras siglas paradigmáticas como son las de las TIC, relacionando comunicación e información.

* Sociedad de la Información y el Conocimiento.

** Profesor investigador de tiempo completo adscrito a INFOTEC.

¹ Zagrebelsky, Gustavo, *El Estado dúctil*, Madrid, Trotta, 2002.

² *Cfr.* <http://www.unesco.org/new/es/office-in-montevideo/comunicacion-e-informacion/acceso-al-conocimiento/las-tic-y-la-sociedad-del-conocimiento/>, consultado el 3 de mayo de 2014.

La influencia de las amplias concepciones del derecho privado, o cuando menos de sus manifestaciones como *lex mercatorum*, en el ámbito del ciberespacio, se revela en la conceptualización del sujeto como consumidor, un poco distinto de aquel portador de derechos fundamentales. Ello significa que se destacan de dicho sujeto, ya no sus cualidades racionales, lúdicas o espirituales, sino una de sus funciones en relación con los objetos del mercado.³ ¿Qué consecuencias se pueden prever? Ese es el motivo de esta reflexión.

En la Sociedad de la Información y del Conocimiento la complejidad de las relaciones de poder ya no permite que se les identifique con el concepto de soberanía. En ese sentido han sido desbordados los análisis filosóficos del poder, identificados con la modernidad, y que van desde Hobbes hasta Austin.⁴ Ahora el núcleo real del poder no siempre se ve representado en sus referentes jurídicos e institucionales y, por lo mismo, se ha afectado el concepto de seguridad jurídica que resultaba clave para la modernidad.⁵ ¿Quién es el soberano en la Sociedad de la Información y del Conocimiento?

El derecho es el esqueleto de la justicia, así que la justicia camina como camina el derecho y no se puede despegar de él. Siendo de esta manera, la justicia es un poco ajena a la unicidad de la persona, lo que no deja de ser paradójico si consideramos que una de sus definiciones más conocidas la concibe como dar a cada uno lo que le corresponde.⁶ Pero podemos preguntarnos, de qué manera dará a cada uno, aunque sea a uno, lo que merece en la Sociedad de la Información, si en realidad es un poco ajena a todos.

Primera pregunta: ¿Es el lector un ilegal en la Sociedad de la Información y del Conocimiento? Ya sé que dirán, no, no, no, mi computadora y mis programas, todos mis programas son originales, y el IP está a mi nombre. Pero mi pregunta no está dirigida a esos aspectos.

¿Las interacciones en la Sociedad de la Información afectan o no lo más profundo de nuestro ser? ¿De qué forma? ¿Somos conscientes de ello? ⁷

Las Tecnologías de la Información han transformado nuestras vidas, y nos hemos rendido ante ellas. Para el derecho, para la política, para la re-

³ Weingarten, Celia, *Derechos en expectativa del consumidor*, Buenos Aires, Astrea, 2004.

⁴ Hobbes, Thomas, *Leviatán*, Barcelona, Altaya, 1994.

⁵ García, Alicia, *La gobernanza del miedo*, Barcelona, Proteus, 2013.

⁶ Gómez, Guido, *Diccionario de etimología*, México, Fondo de Cultura Económica, 2009, voz: justicia.

⁷ Basta aludir a las siglas FOMO, “fear of missing out”, que alude a la sensación del internauta de estarse perdiendo algo cuando está desconectado. Vázquez, Karelia, “La memoria digital”, *El País semanal*, núm. 1965, 25 de mayo de 2014.

creación y para la mera convivencia esto significa nuevos retos, grandes y desconocidos retos. ¿Suena bien hablar de la Sociedad de la Información y del Conocimiento? Largo nombre. Protagonistas de la Sociedad de la Información y del Conocimiento. ¿De qué queremos hablar, si las dos expresiones son difusas?

Por cierto, la abreviatura de esta sociedad también es un poco ambigua, SIC, antes entre paréntesis y con minúsculas (*sic*) que significa “así” en latín, se usaba en textos escritos para llamar la atención sobre la palabra siguiente, que podría ser incorrecta aunque hubiera sido transcrita literalmente. Para saber quiénes son los protagonistas de esta sociedad, debemos de considerar lo siguiente.

La evolución de los pactos, desde la carta magna entre los súbditos y el rey, donde está presente la razón divina, los pactos del mundo moderno, entre los súbditos y el Estado sustentados en la razón de Estado,⁸ hasta llegar al último gran pacto celebrado por la humanidad. El último gran pacto de la humanidad tuvo su origen en una vivencia atroz, la Segunda Guerra Mundial, y se sintetiza en la obligación actual de los Estados de reconocer, proteger y promover la dignidad humana.⁹ Los pactos pueden ser explícitos o tácitos, escritos o verbales, más o menos solemnes, deseados o indeseados, pero los pactos están presentes en el siglo XXI, contribuyendo a conformar el imaginario colectivo. Todos estos pactos han tenido sus protagonistas, ¿quién de todos ellos es usted?

Ahora, en el inicio del siglo XXI, este último gran pacto parece haber empezado su declive, una vez que se ha manifestado en los hechos la imposibilidad de consolidar un Estado de bienestar generalizado.¹⁰

¿Necesita un pacto la Sociedad de la Información y del Conocimiento?, o ¿Puede funcionar sin él? ¿Entre quiénes se celebraría un pacto así?

¿El pacto en la Sociedad de la Información seguiría siendo inspirado en la dignidad humana?

Los fenómenos se parecen a los que suceden en el mundo real, pero tienen sus propias características, menos exploradas, menos bajo nuestro control. En Internet se difunden las noticias más graves y las más alentadoras.

⁸ Meinecke, Friedrich, *La idea de la razón de Estado en la edad moderna*, Madrid, Centro de Estudios Políticos y Constitucionales, Madrid, 1997.

⁹ Lefranc, Federico, *Sobre la dignidad humana. Los tribunales, la filosofía y la experiencia atroz*, México, UBIJUS, 2011.

¹⁰ Hibou, Béatrice, *De la privatización de las economías a la privatización de los Estados*, México, Fondo de Cultura Económica, 2008.

I. UN DON

Celebremos la técnica porque con el primer gesto técnico apareció el ser humano: “Podría decirse que el día que se manifestó por primera vez en los antropoides un gesto técnico, aquel día nació el que hoy llamamos hombre”.¹¹

Las manifestaciones técnicas no definen al ser humano sino el momento histórico. La rueda, la máquina de vapor, las naves espaciales o la telefonía celular, no han transformado en realidad al ser humano.

Es decir, la capacidad técnica caracteriza al ser humano pero no lo determina; no somos los seres del espacio como no fuimos antes los autómatas mecánicos.

El atributo de crear mediante la orden es propio de los seres humanos: “se decide desde el comienzo en la *teknh* la historia del hombre”.¹²

Si el ser humano es la única esencia que puede hacer fuego, entonces una de las preguntas necesarias para completar esta perspectiva, será; ¿se puede verificar la eficacia de la orden que se emite con un clic? Porque sólo así sabemos si la idea de una justicia que pueda ser lograda en una Sociedad virtual tiene un verdadero sentido, o si es tan sólo que el imaginario ha consolidado ya, esta idea: “la técnica: no es dominio de la naturaleza, sino dominio de la relación entre naturaleza y humanidad”... “...ni el hombre debe dominar a la naturaleza ni la naturaleza al hombre”.¹³

¿Cómo desarrollar esa clase de conocimiento? Parece la pregunta urgente. Se puede crear una prótesis mecánica que beneficie a una persona lesionada, como se puede crear una prótesis bioelectrónica que con todos los medios actuales beneficie a quien lo necesite.

II. EL NATIVO DIGITAL, UN SUJETO EPISTEMOLÓGICO DE LA SOCIEDAD DIGITAL POSMODERNA

¿Qué es y para qué sirve un sujeto epistemológico? Un sujeto epistemológico si acaso sirve para dar coherencia a un discurso teórico específico y eso es suficiente. Un ejemplo paradigmático sería el “yo pienso” que permite dar coherencia a toda la filosofía pura kantiana.

¹¹ Galimberti, Umberto, *Los mitos de nuestro tiempo*, Barcelona, Debate, 2013, p. 231.

¹² Heidegger, Martin, *Meditación*, Buenos Aires, Biblos, 2006, p. 121.

¹³ Agamben, Giorgio, *Lo abierto. El hombre y el animal*, Valencia, Pre-textos, 2010, p. 105.

Un sujeto epistemológico es un sujeto que responde a determinada teoría del conocimiento, por ello es necesario poner al descubierto sus presupuestos, cuestionar la legitimidad de sus concreciones.

El sujeto epistemológico es uno para una corriente de pensamiento. Es un sujeto modelo. En el presente caso deberá ser un sujeto modelo congruente con el discurso de la globalización tecnificada, se le ha considerado como nativo digital.

Es preciso enfatizar que todo sujeto epistemológico oculta la desigualdad.¹⁴ Por necesidades formales, para que pueda cumplir su función debe eliminar toda singularidad que pudiera aparecer. Caemos fácilmente en la tentación de dividir entre los que comprenden el discurso y los que no lo comprenden, y nos engañamos un poco pensando que los únicos protagonistas de las SIC son los nativos digitales. Determinadas interpretaciones de una concepción formal y simplificada del yo, como unidad racional han evolucionado en formas tales que pueden ser utilizadas para legitimar que se establezcan entre los seres humanos parámetros de comparación, parámetros que simplifican la idea de persona y, con esa legitimación, pueden permitir también que, violentándolo, se compare a un ser humano concebido como *el otro* para saber si satisface los requisitos para ser asimilado en una comunidad que se pretende abstracta y atemporal, pero que en realidad no responde sino a una concepción de lo instantáneo y de lo global cargada de intereses no necesariamente humanísticos.¹⁵ Explica Jorge Alemán:

En el discurso capitalista, como en su día en los totalitarismos modernos, se encuentra de forma implícita el proyecto de producir un sujeto nuevo, sin legado histórico ni herencia simbólica. Este ‘sujeto capitalista’, tributario de nada que no sea colaborar con la voluntad acéfala que realiza, se caracteriza entonces por no tener en cuenta consecuencia alguna. Autopropulsándose desde sí, de un modo inmanente y conectado, en principio se presenta sin que se pueda pensar su exterior.¹⁶

¹⁴ Acerca de las implicaciones epistemológicas para la visión feminista, Posada, Luisa, *Razón y conocimiento en Kant. Sobre los sentidos de lo inteligible y lo sensible*, Madrid, Biblioteca Nueva, 2008, especialmente el Epílogo II, “Para una hermenéutica crítico-feminista”.

¹⁵ “En la edad de la burguesía triunfante, la Aufklärung abandonó sus aspiraciones humanistas y emancipadoras para postular la igualdad entre los hombres como categoría normativa, a partir de la cual se hacía imposible reconocer y respetar su diversidad cultural, ética o de género. Quienes no entran en esta norma –pronto simbolizada por la respetabilidad burguesa y la ética puritana– son excluidos y se transforman en marginales”. Enzo Traverso, *La historia desgarrada*, Barcelona, Herder, 2001, p. 149.

¹⁶ Alemán, Jorge, “La metamorfosis de la ciencia en técnica”, en Jorge Alemán *et al.*, *Los otros entre nosotros. Alteridad e inmigración*, Madrid, UAM, 2009, p. 201.

Pero en lugar de lo abstracto y lo atemporal, hoy tenemos lo instantáneo manifiesto en forma de nuevos binomios excluyentes; comunicado o incomunicado, actualizado u obsoleto, instantáneo, lento, global, local. Binomios donde el primero de los términos denota una cualidad y el segundo un defecto de modo que el sujeto modelo apreciado se ha concebido como un sujeto comunicado, actualizado, instantáneo y global.

Tratemos, entonces, del sujeto de un discurso específico. Del discurso de la globalización tecnificada. Es prudente sugerir desde ahora que el mismo término globalización no es neutral, basta con comparar la idea de globo con la idea de universo. El discurso globalizador parece haber sustituido a la noción de lo universal, que corresponde a la primera gran pretensión de los imperios y de las culturas, por la idea de lo global más modesta pero de ninguna manera inofensiva. Antes de seguir, abordaremos como referente primero al sujeto epistemológico del sistema kantiano.

¿Quién es un sujeto epistemológico? Es aquel que idealmente puede comprender el discurso que se le dirige. Escribe Safranski: “La globalización moderna es autorreferencial y, por lo que se refiere a las técnicas comunicativas, se realiza en tiempo real”.¹⁷

Cada persona una computadora es el lema y la premisa. Una premisa que puede ser caracterizada por la siguiente expresión de Safranski: “El Dios uno, que antaño garantizaba la conexión espiritual de la sociedad occidental, ha estallado en una pluralidad de pequeños dioses domésticos”.¹⁸ Oráculo y altar, simultáneamente la electrónica da forma a esos pequeños dioses domésticos. Que pequeños como son, no son menos exigentes. Dioses que todavía simulan la existencia de una conexión espiritual de la sociedad occidental.

No terminamos de transitar del sujeto cognoscente al sujeto ético como hubieran esperado los filósofos ilustrados, sino que pasamos al sujeto de la comunicación en tiempo real, habituado a una pluralidad de lenguajes con los que sustituye al conocimiento narrativo.¹⁹ En este tránsito, algo no estuvo previsto, como no es previsible ninguna transformación fundamental. ¿Tiene alguna ventaja comprobada ser nativo digital? Veamos.

Steve Jobs hoy tendría 59 años, Stephen Wozniak 64 años, Bill Gates 58 años, no son nativos digitales habría que recapacitar en eso. Pero fueron ellos, entre otros, los que crearon todos esos entornos que caracterizan a la

¹⁷ Safranski, Rüdiger, *¿Cuánta globalización podemos soportar?*, p. 18.

¹⁸ *Ibidem*, p. 61.

¹⁹ Featherstone, Mike, *Cultura de consumo y posmodernismo*, Argentina, Amorrortu, 2000, especialmente el epígrafe “Modernidad-posmodernidad”.

llamada Sociedad de la Información y del Conocimiento, en la que se mueven esos protagonistas que se preguntan si ellos mismos son o no nativos digitales, sin saber que la expresión nativo digital, que les encanta, tiene una connotación terriblemente excluyente y potencialmente discriminadora.

III. NAVEGANTES

La metáfora de los navegantes aplica bien para los usuarios, cuando menos para las cuestiones políticas y jurídicas. Los navegantes navegan aun en ausencia de leyes. Un poco a la deriva, aceptando que no tienen el control total sobre su ruta.

Es claro que los navegantes de dicha sociedad no conforman una nación, ni un Estado, ni siquiera tienen garantizados sus derechos, o tienen muy pocos derechos garantizados, no tienen entonces una Constitución. Hasta ahora no se ha generado el equivalente a un modelo de Estado, para la Sociedad de la Información.

El riesgo siempre será quedarse en navegantes de habitación, como lo ha dicho, no sin amargura, Paul Virilio.²⁰

IV. FÉNIX

Aun si fuera casi destruida la Sociedad del Conocimiento siempre podría resurgir. Pero antes de destruirla tenemos la oportunidad de no cometer los mismos errores que hemos venido repitiendo en la sociedad real.

No seamos entonces aquel que replica la información sin mayor ejercicio crítico, aprovechemos que convivimos en la sociedad digital con aquellos que son capaces de iniciar grandes o pequeños movimientos humanitarios. Malala es un magnífico ejemplo de ello. ¿Qué promueve Malala?

Diferente es el caso del niño que juega y juega y juega hasta estar hiperestimulado ante la indiferencia de sus padres, que han optado por usar a la *tablet* como niñera.

Pero el mismo medio que sirve para formar redes de pornografía infantil, sirve para difundir la Alerta Amber. ¿Qué es la Alerta Amber? ¿Cuántos menores se han recuperado? ¿Qué es lo que se está proponiendo en otros espacios? Entre otras cosas. “El primer ministro británico anuncia que los

²⁰ Virilio, Paulo, *Ciudad pánico*, Argentina, Libros del Zorzal, 2006, p. 139.

internautas del país sólo podrán acceder a webs para adultos si lo solicitan expresamente”.²¹

Está vigente el caso de la chica acusada de distribuir pornografía infantil por tweetear una selfie desnuda. La policía, que es otra de las comunidades de sujetos presentes en la Sociedad de la Información, afirma que distribuir fotografías de naturaleza sexual de un menor de edad es una conducta tipificada. Por su parte, algunos padres de familia de la comunidad en la que habita esta chica insisten en que la acusación es una respuesta excesiva al problema y que, finalmente, la única afectada será ella. ¿Qué opina el lector? ¿Es excesiva la respuesta de la policía en ese caso?

Stephanie Williams-Ortery, una policía de Virginia, aseguró que cualquier persona que haya recibido o accedido a las fotografías de la chica y las haya enviado a alguien más, podría ser acusada también de distribución de pornografía infantil.

Más cerca, un joven mexicano que secuestraba usando las redes sociales es detenido. El sospechoso confesó que planeó y llevó a cabo cuatro secuestros cuyas víctimas contactaba a través de redes sociales en Internet.

En otro caso una mujer de 26 años fue secuestrada en Guadalajara por tres hombres, uno de los cuales la conoció a través de Facebook. Los sujetos decidieron secuestrar a la víctima debido a que en sus conversaciones en esa red social la víctima presumía una situación económica desahogada y afirmaba ser la encargada de varios puestos de tacos al vapor pertenecientes a su familia.

Ejemplos como los anteriores se pueden encontrar todos los días, por ello, en este contexto la fuente pierde relevancia. Parecen notas que aparecen un día y desaparecen al día siguiente, y que nos llevan a preguntar: ¿hemos conseguido ya que en la Sociedad de la Información y del Conocimiento se garanticen nuestros derechos? ¿Quién es en esa sociedad el garante de ellos?

Las premisas siguientes, identificadas por Fernando Miró, muestran una grave regresión en el discurso de los derechos que deben ser protegidos.

²¹ “La propuesta de Reino Unido es universalizar los filtros para menores que ya se incluyen en navegadores y buscadores –pero que cualquiera puede desactivar–, y extenderlos por defecto a todos los ordenadores del Reino Unido, tengan la edad que tengan sus propietarios”.

Cameron justificó su drástica propuesta como un paso contra “la corrosiva influencia de la pornografía en los niños” y con el fin de “proteger a nuestros menores y su inocencia”. Es la respuesta de su gobierno al creciente debate suscitado en el país a raíz de la muerte de dos niños cuyos asesinos consumían pornografía infantil”. “Porno, de entrada, no”, http://tecnologia.elpais.com/tecnologia/2013/07/22/actualidad/1374483421_185730.html, consulta del 22 de julio de 2013.

Miró estudia el caso de las víctimas en la Sociedad de la Información y del Conocimiento en los términos que siguen.

La víctima define el ámbito de riesgo al que puede acceder el agresor motivado, afirma el investigador. Es la víctima con su conducta, que consiste en actualizar o no las claves informáticas, contratar o no un sistema anti-virus, actualizar el *software* de su ordenador, etcétera, la que define el riesgo de victimización al que se somete.

También la víctima decide si descarga archivos aun ignorando su seguridad, así como las horas que pasa en Internet, elemento que todos los estudios consideran determinante: a mayor número de horas en Internet mayor riesgo de victimización.

Todo, en definitiva, confirma la hipótesis de que el ciberespacio convierte a la víctima en determinante esencial de su victimización por medio de las conductas peligrosas que ella realice, los lugares a los que acceda, el tiempo que pase, los bienes que “suba” al ciberespacio, así como los guardianes que elija para su protección, etcétera.²²

Hay que notar que el significado de estas premisas equivale a una práctica que esperábamos haber dejado atrás hace tiempo; la acusación que recae sobre la mujer ultrajada de haber provocado a su victimario.

En realidad todo esto revela la manera cómo, en materia de víctimas, la administración de Internet se escapa de los ámbitos definidos de la responsabilidad del Estado, es decir, Internet escapa del espacio público de responsabilidad para situarse en un territorio ambiguo.²³

Por favor, no caigamos en la tentación de culpabilizar a la víctima y en cambio aceptemos que alguien tiene que hacerse responsable de lo que sucede en la red. ¿Quién de los protagonistas es el responsable de nuestros derechos?

Sabe el lector, cuáles son sus derechos en la Sociedad de la Información y del Conocimiento. ¿Cuáles son los actos de autoridad en esa sociedad? ¿Cuáles son los derechos de un niño en Internet? ¿Quién vela por ellos?

En nuestro país tiene gran fuerza entre los abogados, refiriéndose a las autoridades, la idea de un mandamiento escrito por autoridad competente, debidamente fundado y motivado, hoy, además, respetuoso de los derechos humanos.

²² Miró, Fernando, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012, p. 266.

²³ El uso de infraestructura pública y de *software* privado es característico.

¿Quién es realmente la autoridad competente en Internet? ¿De verdad el Estado lo es? ¿Qué significa la idea de mandamiento escrito en un medio así? ¿Cuál sería la fundamentación y la motivación adecuadas en un espacio donde convergen universos distintos del derecho, no todos detectables?

Leo textualmente las cláusulas 15.1 y 16, del contrato de uso de una de las enormes compañías que usamos diariamente, sin siquiera preocuparnos por su contenido, que resulta contrario a las premisas recién mencionadas:

“15.1 ...Sin perjuicio de lo anterior, la compañía tendrá el derecho, discrecionalmente, de remover cualquiera de su material por cualquier razón (o sin razón) [así dice textualmente], incluyendo si éste viola las condiciones o cualquier legislación”.

“16. Retroalimentación. Usted no tiene obligación de proveer ideas a la compañía (retroalimentación). No obstante, si usted proporciona retroalimentación a la compañía, nosotros [la compañía] podemos usarla sin ninguna compensación para usted”.

Sobra hacer notar la perspectiva unilateral del “contrato”. ¿Dónde están allí la fundamentación y la motivación? ¿Dónde la presencia de la autoridad competente? ¿Quién es la autoridad competente?

¿Quiénes de los lectores asumen que pertenecen a la Sociedad de la Información? ¿Quién usa Internet? O quizás sería mejor preguntar ¿quién de los lectores no usa Internet? Probablemente la mayoría usamos o hemos usado, por ejemplo, Google, en alguna ocasión. Una pregunta: ¿cómo es el documento de identificación en la Sociedad de la Información y del Conocimiento? ¿No lo tiene usted? Ahora vuelvo a preguntar: ¿Es usted un ilegal en la Sociedad de la Información y del Conocimiento?

Porque los protagonistas de las diversas sociedades cargan consigo un documento de identificación oficial, un pasaporte, una credencial de elector, una cédula profesional, etcétera y si no lo llevan consigo en el momento en que una autoridad se los requiera fácilmente se les puede acusar de que son ilegales.

Pero además de no haberse establecido la necesidad de un documento de identificación para navegar por la red, la premisa en ella es inversa, nos cuidamos mucho de no ser claramente identificados.

Cada lector seguramente confesó ser integrante de la Sociedad de la Información ¿Usa Adobe para intercambiar documentos? Y en serio, ¿ha leído la licencia de uso de Google, o la licencia de uso de Adobe?

Si tenemos un problema de tal gravedad que ponga en juego la seguridad de nuestros bienes, o nuestra tranquilidad personal, y en el que se haya usado como medio para facilitar su comisión, una plataforma, una interfaz,

popular o desconocida, ¿a quién debemos reclamar? ¿Ante quién debemos presentar nuestra reclamación? Y en el muy remoto caso de que recibamos respuesta, si la respuesta no nos satisface ¿Ante quién interponemos el recurso correspondiente? ¿Y cuál recurso, si es que lo hay?

¿Hay en esa sociedad virtual, vocación de pactar y por tanto de identificarnos, o deberemos de permanecer encerrados en nosotros mismos? La red da para todos.

Pero por ahora debemos tener claro que los pactos en la Sociedad de la Información y del Conocimiento no son pactos democráticos, porque no son entre sujetos iguales, y no son pactos entre iguales porque sus protagonistas ni siquiera están identificados, digamos que son virtuales e instantáneos. Si quisiéramos conceptualizar esta relación usando las viejas categorías diríamos que más que el derecho público, prevalece en el ciberespacio la *lex mercatoria* y que quienes gobiernan son soberanos particulares alejados de sus súbditos.

La consecuencia más dolorosa de este estado de cosas, es el sacrificio voluntario de la autonomía del individuo. ¿Qué es lo primero que hace usted, lector, cuando acaba de aterrizar el avión?

V. LOS COSTOS NO VISIBLES

Los sujetos que pagan el costo de la SIC son menos visibles, son los protagonistas olvidados del progreso. Recordemos lo siguiente. En el desarrollo de Europa alrededor del siglo XVI, fueron fundamentales las minas de oro y de plata de América, de lo que poco se habla es de los cientos de miles de trabajadores indígenas que murieron como consecuencia de las inhumanas condiciones de trabajo.

El costo de la Revolución industrial lo pagaron los obreros de las minas de carbón, aunque poco pensemos en ellos cuando usamos un automóvil.

Lo mismo sucede hoy con la revolución electrónica, ninguna de las decenas de veces diarias en que usamos el celular recordamos lejanamente las minas de coltán y la deshumanización que implican.

Este olvido es un rasgo que se asoma con características novedosas, es la instrumentalización cada vez más impúdica del derecho. Derecho *ad hoc*, a la altura de la circunstancia que se pretende justificar y contrario al concepto de práctica política emanado de la Revolución francesa y a partir del cual una generación se hace responsable del destino de las generaciones que la han de suceder. ¿Estamos hoy asumiendo nuestra responsabilidad con los sujetos de la próxima generación?

Las características anteriores se han exacerbado con el fenómeno que hoy identificamos como globalización.

La globalización no se debe solamente a la revolución de las técnicas de telecomunicaciones. Se debe también, y sobre todo, a cambios en el plano de las técnicas de producción, que han permitido poner a trabajar por salarios irrisorios a las inmensas reservas de mano de obra del sudeste y del este asiático, y de algunos otros países, entre ellos, algunos países de Latinoamérica.²⁴

Estos ejemplos pueden ser confrontados uno a uno con las características que han adoptado rápidamente en la sociedad digital en la que el costo humano se oculta para promover únicamente los beneficios. Al momento de la Segunda Guerra Mundial, a la vez que desvelaba el derrumbe de los grandes ideales de la modernidad, se anticipaba lo que llegaría a ser un aparente desbordamiento del individuo por la técnica, ahora, imparable.

Ahora la pregunta es: ¿se expresa de alguna manera la dignidad humana frente a la técnica? Nos alerta Nils Christie: “En las sociedades modernas abundan los mecanismos –intencionales o no– que tienen como resultado que las demás personas ya no sean tan importantes como lo fueron alguna vez”.²⁵

Cuando hablamos de los sujetos en la Sociedad de la Información y del Conocimiento, conviene preguntarnos seriamente, cómo vamos a conciliar los estándares internacionales que rigen la red o la nube, y que provienen de la *lex mercatoria*, con los estándares internacionales en materia de protección de los derechos humanos, que son los que deberían proteger a dichos sujetos.

Quiero terminar este texto citando a Ramón González Ferriz, del periódico *El País*: “El utopismo tecnológico, como todo utopismo, va a acabar decepcionándonos. La política real, con sus miles de problemas pendientes, no va a hallar soluciones tanto en la tecnología como en la mejor y más justa organización de las instituciones”.

Corresponde entonces a los lectores hacerse cargo, y decidir si permanecen como meros usuarios de Internet, aunque sean usuarios avanzados, o construyen los cimientos de un pacto, necesariamente complejísimo, que en un futuro les permita constituirse como una real Sociedad de la Información, en la cual, la verdadera importancia radique en las personas que la constituyan y que sean capaces de ejercer en ella su soberanía.

²⁴ Castoriadis, Cornelius, *Una sociedad a la deriva*, Buenos Aires, Katz Editores, 2005, p. 313.

²⁵ Christie, Nils, *La industria del control del delito. ¿La nueva forma del holocausto?*, Buenos Aires, Editores del Puerto, 1993, p. 28.

Reitero, celebremos la técnica, porque con el primer gesto técnico apareció el ser humano, el sujeto.

Si alguna vez se pensó que los objetos deberían de ser hechos a la medida del individuo que los usa, hoy más que en ningún otro momento se pretende que los sujetos se estandaricen para adaptarse a los sofisticados objetos que se les ofrecen, y que, además, este proceso de estandarización sea permanente y siga aproximadamente los mismos ritmos.

De esta manera la idea de globalización que se nos ofrece es una idea pobre, muy pobre en verdad.

No hay que equivocarse, la crítica no es a la evolución de la tecnología, ni tampoco frente a sus posibilidades ni frente a sus usos. La crítica se dirige a la concepción epistemológica de su discurso, en el entendido de que esta concepción se puede articular entendiendo al sujeto como receptor pasivo de dicho discurso o reconstruyéndolo como protagonista del mismo.

Hay una confusión, la globalización no es grandiosa, es simplemente globalización. No dejará de llamar la atención que dos de los grandes filósofos de occidente, Kant y Spinoza, produjeran su obra desde espacios modestos, sin estar de por medio viajes globales portentosos. Era su mente la que tenía la ambición de abarcar el universo entero. Eran pensadores ambiciosos. La vida tan limitada, espacial y temporalmente limitada, llevó a estos pensadores a imaginar que la mente no tenía límites.

Paradójicamente, con todo y posmodernidad, la idea de globalización no ha hecho sino materializar la modesta idea de razón del positivismo decimonónico. Hoy, idealmente, cuando menos en el discurso, se pide al sujeto que entregue su mente y se le regresa a cambio muy poco. Se pide de él tan sólo que consuma tiempo aire o mega bytes, que se actualice y que no cuelgue.

Ese teléfono inteligente o esa *tablet*, a los que hemos vendido nuestra alma, no querrán devolvérnosla, a menos que seamos capaces de hacer valer nuestra autonomía. ¿Cómo podemos hacer valer nuestra autonomía en el espacio de la tecnología? Pondré un solo ejemplo.

La técnica es libertad, cuando la última sutura de una operación quirúrgica a distancia, guiada por la red, culmina con éxito el trasplante de un órgano vital. La técnica es libertad cuando recordamos que estamos frente a un medio, un medio muy complejo, pero tan sólo eso. Los fines debemos decidirlos nosotros. Es decir, nuestra libertad depende de que seamos capaces de hacer valer los fines de cada uno, como seres humanos, a través de la técnica, del arte, del deporte, o de la vida cotidiana.

VI. CONCLUSIONES

Las definiciones y los conceptos en la SIC son elaborados por unos pocos equipos de especialistas, en diversas ciencias. Sus conceptos no son neutrales ni obedecen estrictamente a un interés neutro (si esto fuera posible) en materia de conocimiento.

Sus definiciones y conceptos están orientados por una necesidad de mercado, es decir, que se difundirá aquello que más y mejor venda, no aquello que beneficie más a la humanidad en general.

Aun los estudiosos tienden a omitir los análisis críticos de una cultura pretendidamente soportada exclusivamente por las TIC

En ese contexto, la conceptualización del sujeto y de sus cualidades debe ser revisada, de lo contrario, se estarán reduciendo nuestras perspectivas acerca de quién es el ser humano, es decir, la concepción de quiénes son nuestros interlocutores.

Todo lo anterior impacta en la promoción y discusión de los valores más profundos del propio ser humano, pues se tiende a adoptar como valores, de manera poco reflexiva, las prácticas inmediatas promovidas por el uso de la tecnología, confundándose, por ejemplo, una noción descriptiva, de por sí difusa, como, “nativo digital” con un valor, “ser nativo digital es mejor”.

Es necesario igualmente ser claro que respecto de las TIC, la mayoría de sus promotores tienen el nivel de simples usuarios, es decir, no conocen a fondo ni el *hardware* ni el *software* que las soportan, por lo mismo no tienen la posibilidad de crear a partir de ellas, de allí la legitimidad de la expresión “navegantes de habitación”. Si se tuviera conciencia de esta limitación, probablemente no se sobrestimaría a los aparatos por sí mismos y se revisarían con una mirada más neutra los usos que hacemos de éstos.

Resulta necesario un diálogo abierto sobre la importancia de las redes sociales, en proyectos colectivos o de servicio a la sociedad. En relación con ello es imprescindible revisar la construcción de los nuevos discursos victimológicos dirigidos al medio que aquí se analiza, ya que es evidente un grave retroceso en dichos discursos que una vez más tienden a responsabilizar a las víctimas de aquello que puedan padecer, en lugar de generar conciencia acerca de que son quienes se benefician de los inmensos negocios alrededor de las TIC, quienes deben aportar los mecanismos que protejan adecuadamente a los usuarios.

Por último, hoy más que nunca considero importante que el lector, y usuario de las tecnologías, reflexione seria y profundamente en aquello que

pueda significar su propia dignidad frente a los aparatos y programas que dan vida al mundo digital.

VI. BIBLIOGRAFÍA

- AGAMBEN, Giorgio, *Lo abierto. El hombre y el animal*, Valencia, Pre-textos, 2010.
- ALEMÁN, Jorge, “La metamorfosis de la ciencia en técnica”, en ALEMÁN, Jorge et al., *Los otros entre nosotros. Alteridad e inmigración*, Madrid, UAM, 2009.
- CASTORIADIS, Cornelius, *Una sociedad a la deriva*, Buenos Aires, Katz Editores, 2005.
- CHRISTIE, Nils, *La industria del control del delito. ¿La nueva forma del holocausto?*, Buenos Aires, Editores del Puerto, 1993.
- ENZO, Traverso, *La historia desgarrada*, Barcelona, Herder, 2001.
- FEATHERSTONE, Mike, *Cultura de consumo y posmodernismo*, Argentina, Amorrortu, 2000.
- GALIMBERTI, Umberto, *Los mitos de nuestro tiempo*, Barcelona, Debate, 2013.
- GARCÍA, Alicia, *La gobernanza del miedo*, Barcelona, Proteus, 2013.
- GÓMEZ, Guido, *Diccionario de etimología*, México, Fondo de Cultura Económica, 2009.
- HEIDEGGER, Martin, *Meditación*, Buenos Aires, Biblos, 2006.
- HIBOU, Béatrice, *De la privatización de las economías a la privatización de los Estados*, México, Fondo de Cultura Económica, 2008.
- HOBBS, Thomas, *Leviatán*, Barcelona, Altaya, 1994.
- LEFRANC, Federico, *Sobre la dignidad humana. Los tribunales, la filosofía y la experiencia atroz*, México, UBIJUS, 2011.
- MEINECKE, Friedrich, *La idea de la razón de Estado en la edad moderna*, Madrid, Centro de Estudios Políticos y Constitucionales, Madrid, 1997.
- MIRÓ, Fernando, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012.
- POSADA, Luisa, *Razón y conocimiento en Kant. Sobre los sentidos de lo inteligible y lo sensible*, Madrid, Biblioteca Nueva, 2008.
- SAFRANSKI, Rüdiger, *¿Cuánta globalización podemos soportar?*
- VIRILIO, Paulo, *Ciudad pánico*, Argentina, Libros del Zorzal, 2006.
- WEINGARTEN, Celia, *Derechos en expectativa del consumidor*, Buenos Aires, Astrea, 2004.
- ZAGREBELSKY, Gustavo, *El Estado dúctil*, Madrid, Trotta, 2002.

GÉNERO Y TIC. POR UNA SOCIEDAD DE LA INFORMACIÓN CON PERSPECTIVA DE GÉNERO

Alejandro DE LA GARZA REYES*
Evelyn TÉLLEZ CARVAJAL**

La mente no tiene sexo.
Pouline DE LA BARRE

SUMARIO: I. *Introducción.* II. *Derechos humanos y Sociedad de la Información.* III. *La evolución de la perspectiva de género. Aspectos básicos.* IV. *La Sociedad de la Información y la equidad de género.* V. *Áreas de oportunidad para una Sociedad de la Información.* VI. *La inclusión de la perspectiva de género en la Cumbre Mundial de la Sociedad de la Información.* VII. *Conclusiones.* VIII. *Bibliografía.*

I. INTRODUCCIÓN

A lo largo de este breve estudio, se resalta la importancia de incluir la equidad de género en el uso de las Tecnologías de la Información y la Comunicación (TIC), pues sin esta inclusión no es posible abatir la llamada brecha digital de la que tanto se habla hoy en día.

La equidad de género, proponemos, debe ser entendida como la forma de concebir y vivir la vida procurando en todo momento el respeto a la dignidad de las mujeres, y de los hombres también, pues el feminismo y la equidad de género no se refieren exclusivamente a los derechos y protec-

* Titular del despacho jurídico De La Garza y Abogados, maestro en defensa y promoción de los derechos humanos, egresado de la Universidad Autónoma de la Ciudad de México, profesor de la Universidad del Valle de México, plantel Coyoacán.

** Maestra en derecho por la División de Estudios de Posgrado de la Facultad de Derecho de la UNAM, adscrita a INFOTEC como profesora investigadora de tiempo completo. Actualmente es doctoranda de la Universidad de Hamburgo en Alemania.

ción de la mujer, como mal apunta la definición proporcionada en diccionarios como el de la Real Academia Española:

Feminismo: (Del lat. *femina*, mujer, hembra, e -ismo).

1. m. Doctrina social favorable a la mujer, a quien concede capacidad y derechos reservados antes a los hombres.

2. m. Movimiento que exige para las mujeres iguales derechos que para los hombres.¹

Nuria Varela, en su obra *Feminismo para principiantes*, apunta que la base de toda doctrina feminista en sus diferentes modalidades: "...es precisamente la de establecer que las mujeres son actrices de su propia vida y el hombre ni es el modelo al que equipararse, ni es el neutro por el que se puede utilizar ...varón como sinónimo de persona".²

Ante la constante desigualdad en el empleo, desigualdad de oportunidades, discriminación por embarazo, acoso, violencia verbal y física, etcétera que han enfrentado las mujeres a lo largo de la historia, surge el feminismo desde el siglo XVIII "...que supone la toma de conciencia de las mujeres como grupo o colectivo humano, de la opresión, dominación y explotación de que han sido y son objeto por parte del colectivo de los varones en el seno del patriarcado bajo sus distintas fases históricas de modelo de producción...".³

El presente artículo se escribe tratando de evidenciar que un cambio en el modelo social que incluya a las mujeres brindando igualdad de oportunidades, condiciones y formas de trato en la red, puede lograr transformar el modelo patriarcal que se continúa viviendo diariamente en la otra realidad que no es virtual.

Actualmente aceptamos la idea de vivir en la llamada sociedad de la información mas no hemos logrado transitar hacia la sociedad del conocimiento que sería más incluyente. Sin embargo, no podemos negar que las tecnologías de la información y comunicación, de las que hoy echamos mano, han logrado cuestionar conceptos como el de la meritocracia⁴ en

¹ *Diccionario de la Lengua Española*, disponible en <http://lema.rae.es/drae/?val=feminismo>, última fecha de consulta el 16 de junio de 2014.

² Varela, Nuria, *Feminismo para principiantes*, Barcelona, No ficción, 2013, p. 17.

³ Sau, Victoria, *Diccionario ideológico feminista*, vol. I, Barcelona, Icaira, 2000, p. 121, cita por Nuria Varela, *ibidem*, p. 17.

⁴ "Meritocracia dentro de lo que es éxito empresarial o profesional coarta y limita las actuaciones", Carmen Castro, economista, en <http://singenerodudedas.com/blog/proyectos/genero-y-tics/>.

donde se reproducían patrones que hacían pensar que los hombres tenían mayor facilidad para dedicarse al trabajo en un modelo presencialista, pues la mujer “es más proclive a intentar equilibrar el trabajo con la familia... y ...por regla general las mujeres están menos dispuestas a quedarse horas extra en la oficina, viajar continuamente, no asistir a actividades del colegio [de sus hijos], salir con clientes por la noche o cambiar de residencia, sacrificando la vida de su familia y sus intereses personales en beneficio de su carrera profesional”.⁵

Hay que tomar en cuenta que la informática e Internet son herramientas que han permitido que tanto la forma de trabajo como las empresas evolucionen y dejen de regirse por un sistema jerárquico centralizado, dando paso al trabajo fuera de una oficina. La red de redes, como es conocida Internet, la incorporación de las mujeres en un modelo de producción no lineal y que les permite ser incluidas a nuevas áreas laborales a través del uso de las TIC, siendo esto un paso de suma importancia para la inclusión de las mujeres en el mundo laboral a nivel global.

Es necesario entender el rol que tienen las mujeres que se han ido incorporando en el uso de las TIC, así como también es fundamental conocer la manera en que lo hacen y si esta inserción atiende a los principios de equidad y justicia para el género femenino, pues de lo contrario estaremos reproduciendo el modelo que predomina en la actualidad sin haber entendido que los derechos humanos y la dignidad que pregonan son fundamentales en la democratización de la información, el aprendizaje participativo, el intercambio de información y la generación de conocimiento.

II. DERECHOS HUMANOS Y SOCIEDAD DE LA INFORMACIÓN

El concepto de derechos humanos ha sido estudiado por expertos en diversas materias como sociólogos, politólogos y abogados. El concepto parece que se puso de moda, ya que se habla de estos derechos tanto en foros políticos, culturales, económicos y hasta en charlas de café.

La literatura en derechos humanos y su significado es abundante. Hoy en día tenemos a la mano distintos expertos dando su opinión al respecto. Sin embargo, pese a lo robusto de los trabajos de diversos especialistas, aún no existe un consenso respecto a qué son y cuáles son los llamados derechos

⁵ Fisher, Helen, *El primer sexo. Las capacidades innatas de las mujeres y cómo están cambiando el mundo*, México, Taurus, 2006, p. 78.

humanos. Tampoco se ha llegado a un acuerdo sobre si los derechos humanos son en realidad universales o bien si son relativos.

La metodología en el estudio de los derechos humanos, dividiéndolos en generaciones, parece que ha generado aún mayor confusión, haciendo creer muchas veces que siguen una suerte de evolución de forma natural y que en la actualidad nos encontramos en una cuarta o quinta generación de los mismos.

Estos comentarios no son ociosos ya que al consultar diversos autores que basan su estudio en los derechos humanos, no es extraño que en sus contribuciones no veamos una sola una definición de lo que ellos entienden por derechos humanos. En el mejor de los casos hallaremos frases como: “Los derechos humanos son aquellos que son inherentes al ser humano”, en donde la referencia “son aquellos” no ayuda a la identificación de cuáles son, o qué hace a un derecho, precisamente, un derecho humano.

Así, tras recolectar diversas definiciones de derechos humanos, observamos concepciones distintas, como las que a continuación se exponen.

Luigi Ferrajoli los define como “[T]odos aquellos derechos que son adscritos universalmente a todos, en cuanto personas, o en cuanto ciudadano o en cuanto a capaces de actuar”.⁶

Esta definición, al añadir el concepto ciudadano por lo menos en el contexto normativo mexicano dejaría fuera a los menores de dieciocho años, por lo que entonces los derechos humanos no serían universales a la población mexicana.

Beuchot los define como “derechos radicados en la naturaleza humana, por eso fueron preconizados como derechos naturales, como señalando que con arreglo a dicha naturaleza se puede encontrar el bien de los hombres y de acuerdo con ella se establece un despliegue de derechos y deberes”.⁷

Esta definición nos pone ante la disyuntiva al tener que aclarar la diferencia entre derecho natural y derechos humanos ya que el derecho natural por definición es el intrínseco a la naturaleza humana.

Abelardo Villegas considera: “Estos derechos son principios filosóficos y no derecho positivo, por eso no pueden prever algunas situaciones que se presentan en diversas modalidades históricas”.⁸

⁶ Ferrajoli, Luigi, “Por una teoría de los derechos fundamentales”, en González Plascencia, Luis y Morales Sánchez, Julieta (coords.), *Derechos humanos. Actualidades y desafíos*, t. I, núm. 61, México, Fontamara, 2012, p. 13.

⁷ Beuchot, Mauricio, *Derechos humanos y filosofía*, 5a. ed., México, Fontamara, 2011, p. 59.

⁸ *Ibidem*, pp. 120 y 121.

La definición de Villegas, al considerar a los derechos humanos como “principios filosóficos” (es decir, como una proposición que es autoevidente) y separándolos del derecho positivo hace que para los abogados se diluya la defensa de los derechos en el ámbito jurídico al no encontrarse positivados, por lo menos principalmente para aquellos que se encuentran inmersos en un sistema del *civil law*, o del derecho romano.

Rafael E. Aguilera opina: “Los derechos humanos constituyen un conjunto de facultades e instituciones que, en cada momento histórico, han ido concretando las exigencias de la dignidad, igualdad y libertad humanas, exigencias fundamentales que forman parte de las sociedades democráticas desarrolladas”.⁹

Aquí la aportación nos plantea nuevas interrogantes ya que una facultad y una institución no son sinónimos de derecho. Así, por ejemplo, el derecho a la vida sería la facultad otorgada al individuo dependiendo de cada momento histórico lo que haría de este derecho humano un derecho totalmente relativizado a su contexto temporal y espacial.

Para los marxistas, según Panikkar, los derechos humanos son sólo derechos de clase.¹⁰ Y efectivamente, en muchos lugares del mundo no es poco común pensar “¿derechos humanos...? ¡ah, sí!, de esos derechos todavía no tenemos aquí”.

En esta pluralidad de ideas y aproximaciones hacia el concepto en comentario encontramos que los derechos humanos son tanto principios filosóficos como facultades, e instituciones e inclusive *Klassenrechte*. Por esta diversidad de opiniones es que decidimos referirnos a los derechos humanos desde una concepción jurídica, apartándonos de otros discursos, sean filosóficos o de otra índole pues, como menciona Laporta, “...hablar de “derechos” sólo tiene un significado comprensible cuando se hace en el marco del lenguaje normativo”.¹¹

Por ello, hemos elegido, para realizar el presente estudio de Género y TIC, el concepto de derechos humanos sugerido por el juez de la Corte Internacional de Justicia, Bruno Simma, quien durante el curso de la Academia Internacional de La Haya en 2007, se refirió a los derechos humanos

⁹ Aguilera Portales, Rafael Enrique, *Nuevas perspectivas y desafíos en la protección de los derechos humanos*, México, UNAM, Instituto de Investigaciones Jurídicas, 2011, p. XI.

¹⁰ En el original se lee: “For the Marxists, so-called Human Rights are merely “Klassenrechte”, “class rights”. Marx K., “Zur Judenfrage I”, p. 352, citado por Panikkar, R. en “Is the Notion of Human Rights a Western Concept?”, *Revista Diógenes*, vol. 75, núm. 30, 1982, p. 85.

¹¹ Laporta, Francisco, “El concepto de derechos humanos”, *Revista Diógenes*, p. 24.

como aquellos derechos reconocidos por el derecho internacional de derechos humanos.

Reconocemos que esta concepción podría desagradar a más de uno, sin embargo, la práctica demuestra que los llamados derechos humanos, son estos derechos consagrados en los instrumentos internacionales o regionales de derechos humanos que son reconocidos como “universales” por un gran número o, si se quiere, “la mayoría” de los Estados¹² que conforman las Naciones Unidas, pues fuera de éstos parece ser que los derechos humanos son sólo una invención.¹³

En realidad los derechos humanos resultan ser una simple invención cuando “(l)os derechos humanos precisan de tres cualidades entrelazadas: los derechos deben de ser *naturales* (inherentes a los seres humanos), *iguales* (los mismos para todos) y *universales* (válidos en todas partes)”,¹⁴ situación totalmente desproporcionada e irreal, pues, como evidencia Mauricio Beuchot, ningún concepto puede ser universal ya que siempre deberá ser interpretado a partir de los distintos *topoi*,¹⁵ también denominados cosmovisiones.

De esta manera permítasenos alejarnos de los debates filosóficos respecto al tema, por no ser objeto del presente análisis, y concentrarnos en la evolución de los derechos humanos contenidos en los instrumentos internacionales de derechos humanos hasta llegar a los derechos humanos en la sociedad de la información haciendo especial énfasis en la incorporación y reconocimiento de los derechos de grupos vulnerables, en particular los derechos de las mujeres.

Es nuestra intención dejar de manifiesto que si los derechos humanos contenidos en los instrumentos internacionales de derechos humanos no son debidamente incorporados en el derecho interno de los Estados que conforman la Sociedad Internacional y no se generan las políticas necesarias para garantizar la protección de los denominados derechos humanos a todos los individuos que se encuentran bajo su tutela “...al defender los derechos humanos estaremos defendiendo cosas inexistentes, que no pasan de ser altos ideales o meros buenos deseos”.¹⁶

¹² Se utiliza la mayoría de los Estados ya que hablar de las naciones civilizadas ya no es políticamente correcto.

¹³ Hunt, Lynn, *La invención de los derechos humanos*, trad. de Jordi Beltrán Ferrer, Barcelona, Tusquets, 2009.

¹⁴ *Idem*.

¹⁵ Beuchot, Mauricio, *Derechos humanos y filosofía*, *op. cit.*, nota 7.

¹⁶ *Ibidem*, p. 43.

1. *Primeros instrumentos internacionales de derechos humanos*

Los primeros instrumentos internacionales de derechos humanos que dieron pauta al actual sistema internacional de los derechos humanos fueron la Declaración Universal de los Derechos Humanos de 1948, el Pacto Internacional de Derechos Civiles y Políticos, y el Pacto Internacional de Derechos Económicos, Sociales, y Culturales.¹⁷

La Declaración Universal de los Derechos Humanos de 1948 por su naturaleza jurídica, fue un instrumento internacional no vinculante para los Estados. Conscientes de esta situación, los dos Pactos internacionales siguientes pretendieron dotar de obligatoriedad a la Declaración. Así, el Comité de Naciones Unidas encargado de redactar un instrumento único que recogiera los derechos contemplados por la Declaración de 1948 se encontró con la presión de dos grandes bloques políticos. Por un lado, se encontraba el bloque capitalista que apoyaba la creación de un Pacto Internacional de Derechos Civiles y Políticos y, por el otro, se encontraba el bloque socialista que impulsaba los derechos económicos, sociales y culturales (DESC) sobre los derechos civiles y políticos.¹⁸

Así, el Comité que había sido encargado de la confección de un tratado único se vio en la necesidad de separar los DESC de los derechos civiles y políticos, surgiendo dos pactos internacionales por separado. Por ello resulta incorrecto hablar de las generaciones de derechos humanos como una sucesión o evolución de ellos en el tiempo, pues tanto los derechos políticos y civiles y los DESC surgen en el mismo año de 1966.

2. *Otros tratados internacionales de derechos humanos*

Posterior a los pactos internacionales arriba mencionados, se dio una proliferación más o menos paulatina de distintos instrumentos internacionales de derechos humanos, siendo algunos de ellos ratificados por un gran número de Estados pero algunos otros no tan bien acogidos, como se ve a continuación.

¹⁷ Burgenthal, Thomas, "Human rights", en *Enciclopedia de Derecho Internacional Público*, <http://www.mpepil.com>, última fecha de consulta el 23 de febrero de 2014. Cassese, Antonio, *Human Rights in a Changing World*, Inglaterra, Polity Press, 1990.

¹⁸ *Idem*.

1. Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial, adoptada el 21 de diciembre de 1965 y en vigor el 4 de enero de 1969.¹⁹ Esta Convención, al día de hoy, cuenta con 177 Estados miembros.²⁰
2. Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer, adoptada el 18 de diciembre de 1979 y en vigor a partir del 3 de septiembre de 1981.²¹ Esta Convención, al día de hoy, cuenta con 188 Estados miembros.²²
3. Convención contra la Tortura y otros Tratos o Penas Cruelles, Inhumanos o Degradantes, adoptada el 10 de diciembre de 1984 y en vigor a partir del 26 de junio de 1987.²³ Esta Convención cuenta, al día de hoy, con 155 Estados miembros.²⁴
4. Convención sobre los Derechos del Niño, adoptada el 20 de noviembre de 1989 y en vigor desde el 2 de septiembre de 1989.²⁵ Esta Convención, es hasta el día de hoy la que cuenta con el mayor número de Estados miembros, 194.²⁶
5. Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores y sus Familias, adoptada el 18 de diciembre de 1990.²⁷ En vigor desde el 1 de julio de 2003. Esta Convención cuenta con tan solo 47 Estados miembros.²⁸

¹⁹ <http://www2.ohchr.org/spanish/law/cerd.htm>, última fecha de consulta el 30 de junio de 2014.

²⁰ http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-2&chapter=4&lang=en, última fecha de consulta el 30 de junio de 2014.

²¹ <http://www2.ohchr.org/spanish/law/cedaw.htm>, última fecha de consulta el 30 de junio de 2014.

²² http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-8&chapter=4&lang=en, última fecha de consulta el 30 de junio de 2014.

²³ <http://www2.ohchr.org/spanish/law/cat.htm>, última fecha de consulta el 30 de junio de 2014.

²⁴ http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-9&chapter=4&lang=en, última fecha de consulta el 30 de junio de 2014.

²⁵ <http://www2.ohchr.org/spanish/law/crc.htm>, última fecha de consulta el 30 de junio de 2014.

²⁶ http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&lang=en, última fecha de consulta el 30 de junio de 2014.

²⁷ <http://www2.ohchr.org/spanish/law/cmw.htm>, última fecha de consulta el 30 de junio de 2014.

²⁸ http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-13&chapter=4&lang=en, última fecha de acceso el 30 de junio de 2014.

6. Convención sobre los Derechos de las Personas con Discapacidad, adoptada en 2006.²⁹ En vigor desde el 3 de mayo de 2008, cuenta con 147 Estados miembros.³⁰
7. Convención Internacional para la Protección de todas las Personas contra las Desapariciones Forzadas, aprobada el 20 de diciembre de 2006.³¹ En vigor a partir del 23 de diciembre de 2010, cuenta con 143 Estados miembros.³²

Es pertinente señalar que las convenciones de derechos humanos cada vez se han vuelto más específicas en la materia que pretenden regular y, sin embargo, el entusiasmo que se percibió en un inicio entre los Estados para obligarse a velar por los “Derechos Humanos” a través de la ratificación de los instrumentos internacionales se ha visto mermado. Onna A. Hataway, en su artículo *Why do Countries Commit to Human Rights Treaties?*³³ (¿Por qué los Estados se comprometen con los tratados de derechos humanos?), deja de manifiesto que al parecer los Estados firman los convenios en la materia sólo por el hecho de evitar la crítica y rechazo que despertaría no hacerlo ante la comunidad internacional.

3. *¿Otras generaciones de derechos humanos?*

El estudio de los derechos humanos en generaciones ha creado confusión ya que las convenciones internacionales que se han celebrado en la materia no atienden a una evolución, pues no existe un paso gradual de uno a otro³⁴ sino más bien se han ido creando atendiendo a una especialización. Santiago Corcuera Cabezut afirma:

²⁹ <http://www.un.org/spanish/disabilities/default.asp?id=497>, última fecha de consulta el 30 de junio de 2014.

³⁰ https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-15&chapter=4&lang=en, última fecha de consulta el 30 de junio de 2014.

³¹ <http://www2.ohchr.org/spanish/law/disappearance-convention.htm>, última fecha de consulta el 30 de junio de 2014.

³² http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-16&chapter=4&lang=en, última fecha de consulta el 30 de junio de 2014.

³³ El artículo se puede consultar en: <http://jcr.sagepub.com/content/51/4/588.abstract>, última fecha de acceso el 23 de junio de 2014.

³⁴ Véase la definición de generación en el Diccionario de la RAE, <http://lema.rae.es/drae/?val=evoluci%C3%B3n>, última fecha de consulta el 14 de mayo de 2014.

La división en los derechos humanos en las llamadas ‘generaciones’ ha provocado mucho más daño que beneficio. Esta clasificación incurre en una multiplicidad de imprecisiones: que los derechos civiles y políticos son baratos y no cuestan al Estado; que los derechos económicos, sociales y culturales son caros; que los derechos civiles y políticos son exigibles y justicializables, mientras que los derechos económicos, sociales y culturales no lo son, que los derechos económicos, sociales y culturales son normas programáticas, por lo que prácticamente no son derechos; que los derechos civiles y políticos son individuales, mientras que los económicos, sociales y culturales son colectivos. Todas estas afirmaciones son, si no absolutamente, sí mayormente falsas. Y ahora hablar de una tercera generación en la que encontramos el derecho a la democracia, la paz y al desarrollo, por ejemplo, como derechos de los pueblos y no de los individuos, puede conducir al debilitamiento no solamente de estos derechos, sino a la de todos los demás.³⁵

Hoy en día se ha llegado a abusar del concepto de los derechos humanos, como lo deja de manifiesto en su artículo “Droit del hommisme”, Alain Pellet.³⁶ El profesor de derecho internacional de la Universidad de París X Nanterre menciona que hoy en día se diluyen los derechos humanos con el activismo férreo que provocan ciertos grupos defensores de los mismos al querer hacer creer las peculiaridades de los derechos humanos y tratar de hacer pasar por verdades jurídicas algo que sólo existe como una esperanza.³⁷

¿Es el caso de la equidad de género un “*droit de l’hommisme*”?, es decir, ¿estamos cayendo en un exceso al solicitar la inclusión de construcciones culturales distintas a las actuales que consideren e incorporen la identidad y diversidad genérica de las mujeres como una necesidad para abatir la brecha digital?

Los movimientos feministas podrían considerarse como un exceso en tratar de reivindicar a la mujer en su rol dentro de la sociedad, sin embargo, la realidad nos demuestra que es necesario dejar de hablar de un solo feminismo como aquella corriente de mujeres esquizofrénicas enemigas de los

³⁵ Corcuera Cabezut, Santiago, “Prólogo” de la obra de Servín Rodríguez, Christopher Alexis, *La Paz, ¿un objetivo de la Corte Penal Internacional?*, México, Porrúa, Universidad Veracruzana, 2013, p. XII.

³⁶ El original en francés se puede consultar en: <http://www.droits-fondamentaux.org/spip.php?article27>. En el original se lee: “il y a d’abord le fait de croire (ou de faire croire) qu’une technique juridique particulière est propre aux droits de l’homme alors qu’elle est bien connue en droit international général : c’est la recherche abusive du particularisme; à l’inverse, et cela est plus proche du “*wishful thinking*”, nos droits-de-l’hommes ont une certaine tendance à prendre leurs désirs pour des réalités et à tenir pour vérités juridiques des tendances encore balbutiantes ou, pire, qui n’existent que dans leurs espoirs”.

³⁷ Allain Pellet, en <http://www.droits-fondamentaux.org/spip.php?article27>.

hombres y comenzar a entender y plantear los feminismos; sí, feminismos en plural.

Esto de los feminismos en plural se explica entendiendo la evolución de los distintos movimientos y discursos políticos que se llevaron y se llevan a cabo para reivindicar la situación de las mujeres en la sociedad dependiendo del contexto histórico, pues estos movimientos han transitado por una diversidad de causalidades y por ello es incorrecto pensar que sólo existe un único movimiento feminista y que es el mismo que se plantea hoy en día en el contexto de la Sociedad de la Información. De acuerdo con la doctora Myrna García Barrera:

El término “sociedad de la información” se utilizó por primera vez en la reunión del Consejo Europeo de Bruselas en diciembre de 1993, en donde se elaboró el documento llamado *White Paper on Competitiveness, Growth and Employment*, estableciendo las bases para el desarrollo de las economías europeas y destacando la promoción en la utilización de las tecnologías, en la nueva sociedad de la información.³⁸

Es decir, que se hizo referencia a la Sociedad de la Información como el conjunto de individuos que utilizan las tecnologías. Una sociedad que a través de los avances de la ciencia y la tecnología tenía la capacidad de acceder a un volumen considerable de información en poco tiempo. Aunque para Wilma Arellano:

[El concepto] Sociedad de la Información fue introducido por el libro del sociólogo Daniel Bell [1973], el advenimiento de la sociedad posindustrial, y luego fue retomado por el estadounidense Thomas Friedman [2005] en su libro *La tierra es plana*, en donde realiza un análisis sobre cómo la sociedad ha ido evolucionando hacia un estudio donde el manejo, tratamiento y posesión de la información son cruciales para el desarrollo social, democrático y de las naciones en su conjunto.³⁹

En este caso, más que el uso de las tecnologías por parte de los individuos, se hace referencia a una sociedad que posee, maneja y trata la información que recibe, es por ello una sociedad informada.

Cualquiera que sea su origen lo cierto es que la sociedad en su evolución ha desarrollado avances tecnológicos que permiten una comunicación más

³⁸ García Barrera, Myrna Elia, *Derecho de las nuevas tecnologías*, México, UNAM, Instituto de Investigaciones Jurídicas, 2011, p. 1.

³⁹ Arellano Toledo, Wilma, *La Sociedad de la Información en Iberoamérica. Estudio multidisciplinar*, México, INFOTEC, 2010, p. 41.

ágil, que parece romper las distancias y por ello ahora el mundo está más conectado, es un mundo globalizado en donde igual los acontecimientos en un lugar del orbe se conocen y comunican en cualquier (o casi cualquier) parte del mundo, por ello el discurso universalizador inicial de 1948 de los derechos humanos parece volverse real pues las redes como Internet parecen hacerlo posible para esta llamada Sociedad de la Información.

Tenemos entonces que cuando se comenzaba a hablar de la Sociedad de la Información en 1973, hacía trece años ya que se había comenzado el diálogo de derechos humanos; por esas fechas, en 1979, se adoptaría y abriría a firma y ratificación la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer.⁴⁰ La sociedad evolucionaba y el discurso feminista también.

Las ideas en torno a la Sociedad de la Información y los derechos sobre la eliminación de todas las formas de discriminación contra la mujer, pese a que se gestaron en la misma década, siguen transitando por senderos distintos pues los feminismos no se han incorporado en el pensamiento de esta Sociedad de la Información, ya que no se nota esa inclusión de equidad de género en la integración de las mujeres en el desarrollo, utilización, aprovechamiento y apropiación de las TIC, dado el rezago de las mujeres en temas tan básicos como la educación, el trabajo y que se siguen reproduciendo los roles tradicionales que encasillan a las mujeres y refuerzan la brecha no sólo digital sino incluso entre derechos fundamentales.

Si bien es cierto que la Convención para la Eliminación de todas las Formas de Discriminación contra la Mujer, por su contexto, no especifica nada respecto a los derechos de las mujeres y la Sociedad de la Información, la Convención sí establece la necesidad de terminar con los estereotipos de roles entre hombres y mujeres en la sociedad, como los patrones culturales que definen el ámbito público como un mundo masculino y la esfera doméstica como el dominio de la mujer, por citar un ejemplo, pues en el preámbulo de esta Convención los Estados Parte se declaran: “Convencidos de que la máxima participación de la mujer, en igualdad de condiciones con el hombre, en todos los campos, es indispensable para el desarrollo pleno y completo de un país, el bienestar del mundo y la causa de la paz”.⁴¹

⁴⁰ Esta Convención entraría en vigor de conformidad con su artículo 27 hasta 1981, fecha en que se entregaría al Secretario General de las Naciones Unidas el vigésimo instrumento de ratificación. Al día de hoy 188 Estados son miembros siendo el último en adherirse a la Convención Qatar en 2009, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-8&chapter=4&lang=en.

⁴¹ Preámbulo de la Convención para la Eliminación de todas las Formas de Discriminación contra la Mujer, en <http://www.un.org/womenwatch/daw/cedaw/text/sconvention.htm>, última fecha de consulta el 3 de noviembre de 2014.

Así, una sociedad que se precie de ser respetuosa de los derechos humanos debe considerar la inclusión de la equidad de género en todos los ámbitos sociales, por lo que la Sociedad de la Información no queda exenta de ello, máxime si se precia de ser una sociedad comunicada, informada e incluyente.

III. LA EVOLUCIÓN DE LA PERSPECTIVA DE GÉNERO. ASPECTOS BÁSICOS

Hablar de género es hablar de feminismos en plural, es hablar de feminismo de la diferencia, de feminismo institucional, de ecofeminismo y ciberfeminismo.

La noción de género surge a partir de la idea de que lo “femenino” y lo “masculino” no son hechos naturales o biológicos, sino construcciones culturales. Por género se entiende, como decía Simone de Beauvoir, “lo que la humanidad ha hecho con la hembra humana”. Es decir, todas las normas, obligaciones, comportamientos, pensamientos, capacidades y hasta carácter que se han exigido que tuvieran las mujeres por ser biológicamente mujeres. Género no es sinónimo de sexo. Cuando hablamos de sexo nos referimos a la biología —a las diferencias físicas entre los cuerpos de las mujeres y de los hombres—, y hablar de género, a las normas y conductas asignadas a hombres y mujeres en función de su sexo.⁴²

Nunca como hoy la mujer se había identificado diferente, nunca como hoy la mujer ha decidido señalar las diferencias frente al género masculino y actuar en consecuencia a favor de una equidad de género. “El feminismo es un discurso político que se basa en la justicia. El feminismo es una teoría y práctica política articulada por mujeres que tras analizar la realidad en la que viven toman conciencia de las discriminaciones que sufren por la única razón de ser mujeres y deciden organizarse para acabar con ellas, para cambiar la sociedad”.⁴³

Los estudios de género ubican tres grandes momentos en la historia del feminismo. La Ilustración, las sufragistas y el feminismo radical.

⁴² Varela, Nuria, *Feminismo para principiantes*, *op. cit.*, nota 2, p. 181.

⁴³ *Ibidem*, p. 14.

1. *Feminismo en la Ilustración*

El feminismo nace en el siglo XVIII en la época de la Ilustración y la Revolución francesa, cuando mujeres como Olimpia de Gouges y Mary Wollstonecraft escribían sobre “Los derechos de la mujer y la ciudadana” (Francia, 1791), o la “Vindicación de los derechos de la mujer” (Inglaterra, 1792). En estos documentos ellas ponían de manifiesto la imagen positiva del cuerpo femenino, el derecho a la educación, el derecho al trabajo, los derechos matrimoniales, derechos sobre los hijos, la abolición de la prostitución, de los malos tratos y abusos en el matrimonio y la incorporación de las mujeres en la vida política, en particular el derecho al voto.⁴⁴

Fue Olimpia de Gouges quien levantó la voz al señalar que aquellos que habían luchado por los Derechos del Hombre y con quien ellas habían luchado hombro a hombro mentían cuando hablaban de principios universales como igualdad y libertad en un mundo donde aún era impensable que las mujeres estudiaran, trabajaran y participaran en la política. Por sus ideas Olimpia muere guillotizada en 1793.⁴⁵

Por su parte, Wollstonecraft señalaba la importancia de la educación de las mujeres, así como la independencia económica, la participación de las mujeres en la política, principalmente en ser representadas en el parlamento inglés. Mary Wollstonecraft, sin embargo, muere debido a negligencia médica durante el parto mucho antes de ver los efectos de sus ideales en la sociedad inglesa.⁴⁶

2. *Las sufragistas*

De acuerdo con Nuria Varela es el siglo XIX y principios del XX cuando mujeres como Emily W. Davison, Sarah y Angelina Grimké, Lucretia Mott y Elizabeth Candy Stanton, Alejandra Kollontai, Alicia Miyares, Emma Goldman y Simone de Beauvoir, tuvieron la visión de aprovechar los contextos históricos que les tocó vivir y de una manera, consciente o no, aprovecharon los discursos que soportaron los movimientos antiesclavistas, el marxismo y los derechos de los trabajadores logrando acarrear estos discursos reivindicatorios a la propia realidad que vivían las mujeres.

⁴⁴ *Ibidem*, pp. 23-31.

⁴⁵ *Ibidem*, pp. 21-34.

⁴⁶ *Ibidem*, pp. 21-42.

Cada una de estas mujeres destacó, ya sea por haber fundado sociedades femeninas,⁴⁷ escribir declaraciones exigiendo el derecho al voto⁴⁸ aun a costa de su propia vida,⁴⁹ difundir la lucha obrera,⁵⁰ o escribiendo libros reflexionando sobre el significado de la construcción del concepto “mujer”⁵¹ que se logró incluir el debate sobre ciertos derechos que posteriormente se otorgarían a las mujeres.⁵²

Es a principios del siglo XX que se logra no sólo el voto femenino en Estados Unidos (que posteriormente permearía el resto del mundo) sino una comprensión de los roles sociales construidos sobre las mujeres que se habían adoptado: “La heterodesignación ya que considera que las mujeres comparten una situación común: los varones les imponen que no asuman su existencia como sujetos, sino que se identifiquen con la proyección que en ellas hacen de sus deseos”.⁵³

3. *El feminismo radical*

Finalmente, el feminismo radical se da posterior a la Segunda Guerra Mundial pues cuando parecía que las mujeres, tras alcanzar su derecho al voto, la participación en la vida democrática de sus países, la misma situación las obligaba a la “domesticidad obligatoria”, es decir, ya no había motivos para salir a la calle y luchar por sus derechos pues los habían conquistado y con los avances en los electrodomésticos se facilitaba sus vidas, con las comidas enlatadas hasta tenían tiempo de sobra para atender sus casas, su apariencia y su familia.

Así, a pesar de participar en la vida laboral algunas de ellas eran nuevamente encasilladas en los roles de madre, ama de casa y amante esposa. Esta situación desencadenaba una “enfermedad” silenciosa, “síndrome de la fatiga crónica” que no era otra cosa que el tedio, la apatía, la depresión.

⁴⁷ Lucrecia Mott fundó la Sociedad Feminista contra la Esclavitud.

⁴⁸ Alicia Miyares escribió la “Declaración de Seneca Falls” por el derecho al voto.

⁴⁹ Emily W. Davison intentó detener el caballo del rey de Inglaterra durante el Derby Day para que escuchara la voz de las mujeres que reclamaban su derecho al voto, acto que le causaría la muerte y Emma Goldman, otra sufragista que exigía al Estado no sólo el voto sino la liberación, libertad, independencia y desarrollo de la mujer.

⁵⁰ Kollontai, en Rusia, fundó el Círculo de Obreras.

⁵¹ Simone de Beauvoir, en Francia, escribió su libro *El segundo sexo*, identificando que la mujer no nace sino se hace a través de los roles sociales y que juegan una especie de papel secundario en la sociedad.

⁵² Varela, Nuria, *Feminismo para principiantes*, op. cit., nota 2, pp. 43-87.

⁵³ *Ibidem*, p. 85.

La norteamericana Betty Friedan escribiría sobre el debate de la mujer moderna, *La mística de la feminidad*, en 1963, que dejaría al descubierto que en el pasado las luchas feministas trataban de obtener los mismos derechos de los hombres cuando en realidad no era ese el fondo del asunto de género sino encontrar su propia naturaleza, la feminidad, crear y descubrir su propia identidad. Evidenciar la “discriminación” en razón del sexo, concepto hasta entonces no acuñado.⁵⁴

Empezarían entonces los movimientos en contra del acoso laboral, de la discriminación por razón de género, la libre movilidad, salir por las noches sabiendo que no serían asaltadas, violadas, ultrajadas.

Poco a poco las mujeres volvieron a conquistar espacios para los estudios de género, autoayuda, demandaron normas de salud femenina, salud ginecológica, centros para mujeres víctimas de abuso, violencia doméstica, políticas sexuales, libertad sexual, las mujeres negras, las mujeres indígenas, las mujeres como factor trascendental en el andamiaje económico, ecológico, cultural.

Las mujeres del tercer mundo lograron colar el tema ecológico, pues al ser ellas parte importante de la cosecha de las tierras para dar alimento a sus familias eran más conscientes del deterioro de los ecosistemas. Y así el discurso feminista pudo llegar a las Naciones Unidas cuando en 1975 se diera en México la Primera Conferencia Mundial de la ONU sobre la Mujer y seguiría la Conferencia Intermedia Mundial sobre la Mujer en Copenhague en 1980 y después Nairobi 1985, Pekín 1995, el discurso de equidad de género había permeado a la comunidad internacional y distintas organizaciones no gubernamentales se sumaban a las conferencias internacionales.

A partir de la década de los noventa y las conferencias auspiciadas por Naciones Unidas, el uso de las TIC se convirtió en algo común.

El cabildeo, las discusiones en listas electrónicas o en línea, los foros electrónicos, las publicaciones, los servicios de noticias, las radios feministas en línea, los sitios y portales web para dar a conocer las luchas por los derechos de las mujeres se convirtieron en instrumentos para el avance de las mujeres en su apropiación del ciberespacio.⁵⁵

Así es que los movimientos feministas fueron ganando terreno hasta el día de hoy que se puede conocer el concepto de ciberfeminismo.

⁵⁴ *Ibidem*, pp. 89-106.

⁵⁵ Sabanes Plou, Dafne, “Mujeres y nuevas tecnologías de la información y comunicación”, en *Tecnologías de la información y la comunicación, cuadernos internacionales de tecnología para el desarrollo humano*, vol. 9, núm. 1, 2011, España, Ingeniería sin Fronteras, Universidad de la Rioja, disponible en <http://dialnet.unirioja.es/servlet/articulo?codigo=3962256>.

Fue en Australia, en 1991, donde un grupo de artistas denominado VNS Matrix, acuñó el término de ciberfeminismo. Una de sus primeras acciones fue el diseño de un anti-video-juego desde la óptica feminista. Sus primeras instalaciones tenían formato electrónico, fotografía, sonido y video. Su propuesta consiste en utilizar la tecnología para la subversión irónica de los estereotipos culturales. Esta rama de ciberfeminismo pretende, por medio de las nuevas tecnologías, construir una identidad en el ciberespacio alejada de los mitos masculinos. ...El movimiento se consolidó en el Primer Encuentro Internacional Ciberfeminista, el 20 de septiembre de 1997 –organizado por OBN, colectivo liderado por la alemana Cornelia Sollfrank– en el seno de la Documenta X, una de las muestras internacionales de arte contemporáneo más relevantes celebrada en Kassel (Alemania). ...Desde su punto de vista, el ciberespacio es un mundo crucial para la lucha de género.

Una segunda rama se inició en el desarrollo de la perspectiva de género y el uso estratégico de las redes sociales electrónicas. Este ciberfeminismo social surgió en 1993 en la Asociación para el Progreso de las Comunicaciones donde se creó el grupo APC-mujeres con la intención de utilizar las nuevas tecnologías para el empoderamiento de las mujeres en el mundo.⁵⁶

El ciberfeminismo o tecnofeminismo contribuye a difundir las problemáticas que enfrentan las mujeres alrededor del globo. Las agencias noticiosas ya han modificado sus contenidos y han incluido en sus sitios web noticias relacionadas con las situaciones que enfrentan las mujeres y se promocionan: como el diario *El País*, de España, que indica claramente: “Este espacio nace para contar los cambios que está aportando la mujer a un mundo en transformación, para detectar desigualdades y para albergar debates bajo esta premisa clave: una sociedad desarrollada y libre no puede funcionar si no permite idénticas oportunidades a la mitad de la población”.⁵⁷

También se ha dado una proliferación de mujeres con una nueva profesión, conocidas como *bloggeras*, en áreas tan distintas pero que comparten el escribir e influenciar con su presencia la red.

Como ejemplo sirva mencionar algunas *bloggeras* de las cincuenta listadas en “NxE’s Fifty Most Influential’Female’Bloggers”,⁵⁸ como Lisa Stone, Elisa Camahort Page y Jory Des Jardins, que desde 2005 son organizadoras

⁵⁶ *Ibidem*, p. 128.

⁵⁷ Página web del diario español *El País*, disponible en <http://blogs.elpais.com/mujeres/>, última fecha de consulta el 30 de mayo de 2014.

⁵⁸ Colocado en la red por el administrador del blog North x East, el 10 de julio de 2008, disponible en <http://www.northeast.com/204/nxe/%e2%80%99s-fifty-most-influential-female-bloggers/>, última fecha de consulta el 29 de mayo de 2014.

de la Conferencia BlogHer, un medio para que las mujeres en el medio se conozcan y se apoyen mutuamente.

Gina Trapani, editora de Liferhacker, una compañía que desarrolla contenidos para Internet es también programadora independiente de red de códigos de extensión Firefox y sitios web. Escritora en las revistas *Scienza popolare*, *Wired* y *Laptop*.

Pamela Jones. Una de las voces más influyentes en aspectos legales alrededor del tema de acceso abierto y comunidad *software* libre. Es editora de *Groklaw*, en donde debate sobre eventos que afectan la comunidad en línea desde un aspecto legal pero sencillo.

En el contexto iberoamericano no se puede olvidar el caso de “la periodista española Judith Torrea, quien obtuvo ... el premio BOB-Reporteros Sin Fronteras por su blog ‘Ciudad Juárez, en la sombra del narcotráfico’, [al...] emplear Internet para denunciar el ‘poder de los cárteles de la droga’ en esa localidad mexicana fronteriza con EEUU, narrar la historia de las víctimas y criticar la extendida corrupción”.⁵⁹

O bien la comunidad Modenmujer, que fue desarrollada en 1992 por Beatriz Cavazos Siller, mexicana, que utilizó el correo electrónico para comunicarse con Yucatán, al sur del país, donde las organizaciones de mujeres se encontraban aisladas y con poco acceso a la información. Así, el uso del correo electrónico resultó un medio de comunicación poco costoso en comparación con el teléfono, el fax y el correo tradicional.⁶⁰

A pesar de todo lo anteriormente descrito, “según los datos estadísticos ...el porcentaje de mujeres bloggers o blogueras es bastante inferior al de hombres. Las bitacoreras suponen sólo el 19% de la blogósfera hispana según el informe de Bitácoras”.⁶¹

No podemos negar que las Tecnologías de la Información y Comunicación han ayudado a difundir el concepto y diálogo alrededor de la equidad de género; sin embargo, sabemos que aún queda mucho trabajo por hacer para reducir la brecha que existe entre hombres y mujeres en la apropiación

⁵⁹ Diario *El Mundo*, España, disponible en <http://www.elmundo.es/elmundo/2011/04/12/comunicacion/1302621417.html>, última fecha de consulta el 28 de mayo de 2014.

⁶⁰ *Cfr.* Sabanes Plou, Dafne, “Mujeres y nuevas tecnologías de la información y comunicación”, *op. cit.*, nota 55.

⁶¹ <http://ceslava.com/blog/quin-es-esa-bloguera/>, última consulta el 25 de junio de 2014. También se sugiere consultar <http://acceso-directo.com/las-mujeres-bloggers-ms-relevantes-de-habla-hispana/>, <http://www.soniablanca.es/2010/08/tesis-doctoral-del-blog-al-microblog-el-devenir-del-receptor-en-generador-y-emisor-de-contenidos-en-la-web-2-0-act-1/>, y <http://www.mujeresdeempresa.com/blog/index.php/sites-o-blogs-escritos-por-mujeres-en-espanol-2011/>, misma fecha de consulta.

ción de estos medios tecnológicos. Coincidimos con Nuria Varela cuando afirma que “[p]uesto que el feminismo está ausente en los medios de comunicación, en Internet se encuentra el mejor instrumento para comunicar y comunicarse”.⁶²

IV. LA SOCIEDAD DE LA INFORMACIÓN Y LA EQUIDAD DE GÉNERO

La Sociedad de la Información se caracteriza por el uso de las tecnologías para comunicarse de forma libre y global con la ventaja de no representar un costo excesivo como antaño lo serían las llamadas internacionales. Sin embargo, la velocidad a la que se puede compartir información hace que los individuos “naveguen” en un mar de información, muchas veces sin detenerse en la veracidad de la misma.

La información empodera a los individuos e Internet ha logrado dar voz a muchas mujeres. Tras un monitor el género desaparece, lo importante es la información y conocimientos que se comparten.

Las mujeres han entrado en el apropiamiento de las TIC no sin contratiempos, pues a pesar de que, como usuarias de las mismas, o como desarrolladoras, el medio no necesariamente ha dejado de ser considerado exclusivo de los hombres.

Nuevamente son el discurso y los roles sociales los que hacen que las mujeres no se consideren tecnófobas, o que se les considere más tendientes a las relaciones personales que a las virtuales y, en consecuencia, tengan una actitud pasiva hacia los avances tecnológicos. La inclusión de la perspectiva de género en todos los ámbitos, educativos, laborales, sociales, etcétera, es una obligación del Estado mexicano por ser parte de los tratados internacionales de derechos humanos y en particular de la Convención para la Eliminación de todas las Formas de Discriminación contra la Mujer, obligación que hasta el día de hoy no se cumple.

Las cifras indican que aún es mayoritario el número de internautas hombres que mujeres. Todavía las herramientas tecnológicas están más diseñadas hacia el género masculino. Hoy en día, son más hombres los que estudian ingenierías, sistemas en computación, en comparación con las mujeres.

Los trabajos ofertados en el área de las TIC parecen también estar más orientados hacia el género masculino. Sin embargo, las tendencias pueden cambiar:

⁶² Varela, Nuria, *op. cit.*, nota 2, p. 129.

¿Qué pasa en los países más avanzados tecnológicamente? Si nos guiamos por lo que está sucediendo en EE.UU. y por las previsiones, pronto habrá más mujeres internautas que hombres. En estos momentos las mujeres están liderando el crecimiento de nuevas conexiones a Internet en EE.UU., habiéndose triplicado su cifra en los últimos 30 meses hasta llegar al actual 49% de la población estadounidense con acceso a Internet. Las previsiones para finales de año o el año próximo en los países de mayor penetración como los EE.UU. y Escandinavia, indican que alrededor del 60% de los nuevos usuarios serán mujeres. ... Los hombres visitan las tiendas virtuales, las mujeres compran, dicen, en Cyberatlas. Las mujeres empresarias americanas lo tienen claro (Nua, Women Connect). Y las agencias de publicidad, también (Cyberatlas). Incluso hay agencias especializadas en insertar publicidad en sedes de mujeres, como es el caso de Her Agency. No hay duda de que las cosas están cambiando...⁶³

Pese a esta tendencia de las mujeres a incluirse en el uso de las TIC existe otra realidad en lo que toca a la educación de las mujeres y su incorporación en la educación en ciencias exactas. Las mujeres en México siguen representando una estadística baja en matrículas de carreras como la ingeniería.⁶⁴

En la mayoría de los países, la participación de las mujeres en la matrícula de las carreras de ciencias exactas o ingeniería es baja, semejándose a los guarismos de países como Estados Unidos (alrededor de 20%). A manera de ejemplo, comparado con el alto número de mujeres que continúa optando por los estudios en psicología, ciencias sociales, periodismo y educación, la Universidad Tecnológica Nacional de Argentina, con filiales en todo el país, sólo cuenta con 19.6% de alumnas mujeres, mientras que las carreras de ciencias exactas en todas las universidades nacionales apenas alcanzan en promedio 24% del alumnado femenino.

⁶³ Portal de noticias Africa on Line News, disponible en http://afrol.com/es/html/Categorias/Mujeres/especial_muj_internet.htm, última fecha de consulta el 8 de junio de 2014.

⁶⁴ “Al respecto, Pino Durán Escamilla, director de la Escuela Superior de Ingeniería y Arquitectura (ESIA), señala que de los 5 mil 549 inscritos en el campus Zacatenco, al menos 1 324 son mujeres que se forman como ingenieras civiles. En las especialidades más novedosas, como ingenierías en mecatrónica, telemática y biónica, sumaban 313 alumnas, de un total de 2 043 inscritos, mientras en ingeniería eléctrica concentraba a 136 mujeres; en mecánica se forman 323 y en aeronáutica 155, de un total de 1 547. En otro de los principales campos de desarrollo de la ingeniería, comunicaciones y electrónica, estaban inscritas 1 384 mujeres, de un total de 7 228 alumnos”. Tomado de la nota periodística “Mujeres en el Poli”, publicado en *La Jornada*, disponible en línea en <http://www.jornada.unam.mx/2013/02/14/politica/002n1pol>, última fecha de consulta el 3 de noviembre de 2014.

En el área de la investigación científica, la situación se repite. Mientras que en Uruguay el 56% de los investigadores son mujeres, en El Salvador llegan al 20%. En Argentina, Bolivia y Brasil el componente femenino es de alrededor del 49%, mientras que en Ecuador y Panamá la participación femenina llega al 30%. La mayoría de estas mujeres se ubica en el campo de las ciencias duras. Se observa, además, que a medida que se sube en la jerarquía dentro de los organismos para la investigación científica, el número de mujeres en puestos de decisión va disminuyendo y es prácticamente nula su presencia en los altos cargos de dirección de estos centros de investigación.⁶⁵

Todavía son pocas las mujeres en las áreas de estudio de tecnología e informática, electrónica y comunicaciones. “En Estados Unidos, las mujeres están poco representadas entre las personas que se gradúan en informática (34%) e ingeniería (21%). A nivel doctorado, las mujeres son sólo el 19% en informática y el 17% en ingeniería”.⁶⁶

Lo que también debe llamar la atención no sólo es el número de hombres y mujeres en uso de las TIC sino el tipo de uso que le dan unos y otras a las mismas.

La relación entre las mujeres y los saberes tecnológicos está cambiando, pero la presencia de alumnas en los estudios técnicos y científicos, y de investigadoras en estos campos, es mucho menor que la de los varones. Este es uno de los factores que hace necesaria la perspectiva de género para analizar el mundo de las Tecnologías de la Información y Comunicación (TIC).⁶⁷

Por ello se habla de distintas brechas digitales en cuanto al tema de género, como lo apuntan Susana Vázquez y Cecilia Castaño, quienes identifican tres tipos. La primera brecha digital de género se refiere al número de mujeres que tienen acceso a la tecnología, mientras que la segunda brecha se refiere al uso que se hace de esta tecnología. La tercera brecha digital de género se circunscribe al uso de los servicios menos avanzados de las Tecnologías de la Información y Comunicación.⁶⁸

⁶⁵ Sabanes Plou, Dafne, “Mujeres y nuevas Tecnologías de la Información y la Comunicación”, *op. cit.*, nota 55.

⁶⁶ Wajcman, Judy y Giraldo, Elida (trads.), “TIC e inequidad, ¿ganancias en red para las mujeres?”, *Educación y Pedagogía*, vol. 24, núm. 62, 2012, pp. 117-134, texto disponible en <http://dialnet.unirioja.es/servlet/articulo?codigo=4161068>, última fecha de consulta el 24 de julio de 2014. Algunas citas fueron omitidas.

⁶⁷ Sabanes Plou, Dafne, “Mujeres y nuevas tecnologías de la información y comunicación”, *op. cit.*, nota 55.

⁶⁸ Vázquez, Susana y Castaño, Cecilia, “La brecha digital del género: prácticas de e-inclusión y razones de la exclusión de las mujeres”, *Asparika*, investigación feminista,

V. ÁREAS DE OPORTUNIDAD PARA UNA SOCIEDAD DE LA INFORMACIÓN

El género es una construcción social, en este constructo social se han creado las obligaciones, capacidades, comportamientos, normas, etcétera, deseables y exigibles a las mujeres por su condición biológica, por ello en este trabajo se sostiene que la Sociedad de Información puede servir para deconstruir y construir una perspectiva de género que permita entender que, por ejemplo, las diferencias en salarios a trabajos iguales entre hombres y mujeres no es un problema biológico o natural sino un problema de cultura social y voluntad política respecto al rol de la mujer trabajadora.

...las diferencias biológicas hombre-mujer son deterministas, vienen dadas por la naturaleza, pero en cuanto que somos seres culturales, esa biología ya no determina nuestros comportamientos. ...Así, aquellos que claman para que todas las mujeres tengan como prioridad en su vida dedicarse a criar hijos y cuidar maridos, no parecen muy dispuestos a regalar sus automóviles para trasladarse en burro de una ciudad a otra. Tampoco renuncian a colgar sus encíclicas en Internet. El primer propósito de los estudios de género o de la teoría feminista es demostrar el prejuicio de que la biología determina lo “femenino”, mientras que lo cultural o humano es una creación masculina.⁶⁹

En el área educativa vemos un área de oportunidad pues se siguen repitiendo los modelos tradicionales de enseñanza. Es verdad que, como se apuntaba en el apartado II de este trabajo, las mujeres lograron a través de una lucha social la conquista del derecho a la educación, sin embargo, los modelos educativos a los que se incorporaron ya habían sido diseñados para y por los hombres.

A estas alturas deberíamos ya de saber que las experiencias de enseñanza-aprendizaje no son las mismas que deben de aplicarse en hombres que en mujeres. No es en vano que por ello la Comisión sobre Tecnología, Género y Educación Docente de la Fundación Educativa de la Asociación Americana de Mujeres Universitarias pusiera al descubierto que en la infancia:

...las niñas encuentran a los juegos de computación muy aburridos, repetitivos y violentos. Sus preferencias se vuelcan en las actividades y entreteni-

núm. 22, 2011, p. 3. Disponible en <http://dialnet.unirioja.es/servlet/articulo?codigo=4161068>, última fecha de consulta el 17 de junio de 2014.

⁶⁹ Varela, Nuria, *Feminismo para principiantes*, op. cit., nota 2, pp. 182 y 183.

mientos en los que haya simulación, interacción uso de estrategias. También demuestran interés por utilizar programas que las ayudan a resolver problemas concretos y crear comunidades de interés y amistad.

Los fabricantes de juegos de computación coinciden con este estudio en que las chicas se inclinan más “por juegos con relatos ricos, ambientados en mundos que pueden explorar a su propio ritmo”. También muestran interés por relacionarse con otras chicas de su edad, por lo cual las posibilidades de desarrollar *chats* o intercambios a través de *weblogs* las entusiasman. Los *weblogs* también las animan a escribir sus diarios íntimos o a crear guiones de relatos complejos.⁷⁰

Con todo esto aún se encuentra latente el reto de incluir la perspectiva de género en diversas áreas de la sociedad, como en la educación, el trabajo, la salud, por mencionar sólo algunas.

Las mujeres, pese a la desventaja de vivir en una sociedad con estereotipos y roles sociales, no han dejado de incursionar en las áreas que se consideraban exclusivas para los hombres.

Durante el V Foro Internacional de Software libre, que se realizó en Porto Alegre, Brasil, a comienzos de junio de 2004, se celebró el I Encuentro de Mujeres y Software Libre. Cabe señalar que en el Foro Internacional participaron 575 mujeres y la mayoría de ellas también estuvo en este primer encuentro donde se constató a partir de testimonios, ponencias, experiencias y demostraciones técnicas el nivel de preparación que están teniendo las mujeres en el desarrollo de *software* libre.

...Los perjuicios, el descrédito del trabajo de las mujeres técnicas que se percibe en las diferencias salariales con sus colegas varones, y la doble y triple jornada, al continuar enfrentando solas las demandas del hogar y la crianza de los hijos, son problemas que estas mujeres soportan día a día. Su deseo es que el espíritu de libertad, de posibilidades abiertas y de decisión sobre las soluciones a poner en práctica que reina en el mundo del *software* libre también sean posibles de aplicar en sus vidas cotidianas, exigiendo igualdad de oportunidades y equidad para acceder a ellas.⁷¹

Es una realidad que muchas mujeres siguen desarrollando trabajos considerados de bajo perfil en las diversas áreas de las TIC, como operadoras de teléfono, instaladoras y reparadoras de equipos de procesamiento de datos, así como operadoras de equipos de comunicaciones, pues no se les da la

⁷⁰ Sabanes Plou, Dafne, “Mujeres y nuevas tecnologías de la información y comunicación”, *op. cit.*, nota 55.

⁷¹ *Idem.*

oportunidad de incorporarse a trabajos que se consideran masculinos por excelencia, esto no es un problema de las TIC es una cuestión de educación y cultura, que desafortunadamente se produce y reproduce por medio de las TIC.⁷²

Las nuevas tecnologías efectivamente están creando una transformación social y, a pesar de que en un principio la mayoría de los usuarios de Internet eran hombres, la realidad ha cambiado. Este cambio no sólo es debido a los avances tecnológicos, también existen otras variables como las socioeconómicas, ya que las mujeres ahora tienen un mayor poder adquisitivo, mejores oportunidades de educación, mayor apertura en campos laborales y sociales en general, lo que logró que ellas pudieran desarrollar también habilidades técnicas.

El cambio de ideología que anteriormente permeaba en la mujer y aludía al “miedo digital”, hoy en día tiende a desaparecer, pues la automatización ha reducido la importancia del género respecto de la capacidad masculina y se ha reemplazado con las demandas de habilidades interpersonales, comunicativas, y de inteligencia.

Vivimos la era de la Sociedad de la Información, en la cual las TIC representan una gran oportunidad de cambio en viejos paradigmas respecto a los roles sociales que pretendieron dividir las oportunidades y derechos entre hombres y mujeres por razones de sexo. Hoy tenemos la oportunidad de dejar de reproducir ideas que vulneran los derechos de un grupo de la sociedad que representa la mitad de la población mundial. Tenemos la oportunidad de que sean las TIC una herramienta de enseñanza-aprendizaje respecto a la inclusión de una perspectiva de género en todas las áreas de la sociedad en la que las diferencias entre sexos sí importan.

Así, las áreas de oportunidad que brinda la inclusión de la perspectiva de género en la Sociedad de la Información van desde garantizar que la sociedad de la información fomente las capacidades de las mujeres y su plena participación sobre bases de igualdad en todas las esferas de la sociedad, hasta diseñar políticas públicas que hagan realidad que las mujeres logren

⁷² “...los hombres que se gradúan se concentran con fuerza como científicos y analistas de sistemas de computación, profesores de informática, programadores de computador, analistas e investigadores de sistemas y operaciones, y operadores de equipos de transmisión. Estas divisiones de sexo en el mercado laboral implican que las mujeres son ampliamente excluidas de los procesos de diseño técnico que determinan el mundo en el cual vivimos”. Wajcman, Judy y Giraldo, Elida (trads.), “TIC e inequidad, ¿ganancias en red para las mujeres?”, *Educación y Pedagogía*, vol. 24, núm. 62, 2012, pp. 117-134, texto disponible en <http://dialnet.unirioja.es/servlet/articulo?codigo=4161068>, última fecha de consulta el 24 de julio de 2014.

integrarse a una sociedad libre de paradigmas en las que el sexo femenino se asuma como débil, vulnerable, inferior al masculino. La Sociedad de la Información debe ayudar en el nuevo constructo social del género femenino y su rol en la sociedad. Pugnamos por un cambio cultural en donde el género femenino se empodere y pueda vivir dignamente en una sociedad que garantice sus libertades y respete sus derechos humanos en estricto apego a las obligaciones estatales con los instrumentos internacionales en la materia.

VI. LA INCLUSIÓN DE LA PERSPECTIVA DE GÉNERO EN LA CUMBRE MUNDIAL DE LA SOCIEDAD DE LA INFORMACIÓN

En una sociedad internacional en la que en el año 2000 se aprovechó la oportunidad de iniciar un milenio, las Naciones Unidas, los representantes de los diversos gobiernos del mundo se unieron en Nueva York para aprobar la Declaración del Milenio a fin de comprometerse a abatir la pobreza por medio de ocho objetivos conocidos como los “Objetivos del Milenio”.⁷³

1. Erradicar la pobreza extrema y el hambre
2. Lograr la enseñanza primaria universal
3. Promover la igualdad entre los sexos y el empoderamiento de la mujer
4. Reducir la mortalidad de los niños menores de 5 años
5. Mejorar la salud materna
6. Combatir el VIH/SIDA, la malaria y otras enfermedades
7. Garantizar la sostenibilidad del medio ambiente
8. Fomentar una alianza mundial para el desarrollo.

En el objetivo tres se observa la intención de erradicar las diferencias entre los sexos y dar paso a una sociedad igualitaria para las mujeres.

En diciembre de 2003 se realizó en Ginebra la primera fase de la llamada Cumbre Mundial de la Sociedad de la Información (en adelante CMSI). Esta Cumbre Mundial se dividió en dos fases. En Ginebra, la primera de ellas, se sentaron las bases de los compromisos comunes para construir una Sociedad de la Información integradora que orientara al desarrollo para crear, consultar, utilizar y compartir la información y el conocimiento para todas las personas, comunidades y pueblos. A través de estos compro-

⁷³ Véase más sobre los Objetivos del Milenio, en <http://www.un.org/es/millenniumgoals/gender.shtml>.

misos se pretendía alcanzar un desarrollo sustentable que redundaría en la mejora de una calidad de vida de todos atendiendo los principios y propósitos de la Carta de Naciones Unidas y la Declaración Universal de los Derechos Humanos.⁷⁴

En el punto dos de la Declaración se establece:

2. Nuestro Desafío es aprovechar el potencial de las tecnologías de la información y la comunicación para promover los objetivos de desarrollo de la Declaración del Milenio, a saber, la erradicación de la pobreza extrema y el hambre; lograr la enseñanza primaria universal; *promoción de la igualdad de género y el empoderamiento de la mujer*; reducción de la mortalidad infantil; mejora de la salud materna; para combatir el VIH / SIDA, el paludismo y otras enfermedades; garantizar la sostenibilidad del medio ambiente; y el desarrollo de alianzas mundiales para el desarrollo para el logro de un mundo más pacífico, justo y próspero. También reiteramos nuestro compromiso con el logro de un desarrollo sostenible y los objetivos de desarrollo acordados, tal como figura en la Declaración de Johannesburgo y Plan de Aplicación y el Consenso de Monterrey, y otros resultados de las Cumbres de las Naciones Unidas pertinentes.⁷⁵

En la Cumbre, en Ginebra, se notó la participación cada vez más activa de la sociedad civil, quienes, por medio del Caucus de Género y el Grupo de Trabajo sobre Estrategias de Género, lograron incluir el párrafo 12 de la Declaración.

Afirmamos que el desarrollo de las TIC brinda ingentes posibilidades a las mujeres, las cuales deben formar parte integrante de la sociedad de la información y han de ser actores muy destacados de dicha sociedad. Nos comprometemos a garantizar que la sociedad de la información fomente las capacidades de las mujeres y su plena participación sobre bases de igualdad en todas las esferas de la sociedad y en todas las etapas de adopción de decisiones. A dicho efecto debemos integrar una perspectiva de igualdad de género y utilizar las TIC como instrumento para conseguir ese objetivo.⁷⁶

Para la segunda fase, Cumbre de Túnez 2005, se pretendió pasar de la mera declaración a los planes de acción en la Sociedad de la Información.

⁷⁴ La Declaración de Principios de Ginebra del 12 de mayo de 2004, disponible en línea en <http://www.itu.int/wsis/docs/geneva/official/dop-es.html>, última fecha de consulta el 4 de noviembre de 2014.

⁷⁵ *Idem*. Las cursivas fueron añadidas.

⁷⁶ Sabanes Plou, Dafne, “Mujeres y nuevas tecnologías de la información y comunicación”, *op. cit.*, nota 55. Algunas citas fueron omitidas.

Desafortunadamente, algunos Estados ya no se mostraron igual de entusiasmados como en la primera fase. De esta segunda Cumbre surgieron los llamados compromisos de Túnez que pretendía ser más específico que la Declaración de Principios de Ginebra. En Túnez se habló de la creación de un Fondo de Solidaridad digital para alcanzar las metas y objetivos comunes sin especificar más pues no se lograron mayores consensos.

La inclusión del tema de género se menciona en la Declaración de Túnez en el párrafo 90 en el que se reafirman los compromisos de dar acceso equitativo a la información y los conocimientos, en función de las TIC para el crecimiento y desarrollo económico y así alcanzar los Objetivos del Milenio y en particular en el inciso c) y d) se hace mención a las mujeres:

c) *la creación de capacidades TIC* para todos y la confianza en la utilización de las TIC por todos –incluidos los jóvenes, las personas mayores, *las mujeres*, los pueblos indígenas, las personas discapacitadas y las comunidades distantes y rurales– mediante la mejora y la aplicación de sistemas y programas de educación y capacitación que incorporen un aprendizaje a distancia a lo largo de toda la vida;

d) *la promoción de la formación y la educación eficaces*, en particular en los ámbitos de la ciencia y la tecnología en materia de las TIC, que motive y promueva la plena participación de las niñas y *las mujeres* en el proceso de toma de decisiones de la creación de la Sociedad de la Información;...⁷⁷

Desafortunadamente la Sociedad de la Información, con una perspectiva de género incluyente, aún está demasiado lejana, aunque se avanza poco a poco.

Indicadores

- La pobreza es un importante obstáculo para la educación, especialmente entre las niñas de mayor edad.
- En todas las regiones en vías de desarrollo, salvo en los países de la CEI, hay más hombres que mujeres en empleos remunerados.
- A las mujeres se les suele relegar a las formas de empleo más vulnerables.
- Gran cantidad de mujeres trabajan en empleos informales, con la consiguiente falta de prestaciones y seguridad laboral.
- Los puestos en los niveles más altos siguen obteniéndolos los hombres, la diferencia es abrumadora.

⁷⁷ Agenda de Túnez para la Sociedad de la Información del 28 de junio de 2006, disponible en línea en <http://www.itu.int/wsis/docs2/tunis/off/6rev1-es.html>, última fecha de consulta el 3 de noviembre de 2014.

- Las mujeres están accediendo lentamente al poder político, pero por lo general gracias a cuotas y otras medidas especiales.⁷⁸

Los conceptos género y TIC son construcciones sociales que pueden permear un cambio de cultura respecto a los roles de las mujeres en el uso, creación y apropiación de las TIC. Una Sociedad de la Información que reproduce roles estereotipados y paradigmas que vulneran los derechos de las mujeres y les impiden acceder a una sociedad de respeto a su dignidad y derechos humanos en una sociedad que ha fracasado.

VII. CONCLUSIONES

La perspectiva de género debe ser incluida en la Sociedad de la Información. La perspectiva de género puede transformar la cultura en la que el sexo biológico determine situaciones preconcebidas para las mujeres. Esta situación se ve reflejada en cuestiones tan básicas como el diseño de videojuegos en el que se incluya la equidad de género, como se puede observar:

Corea del Sur se lleva las palmas. El 69% de los usuarios de estos juegos son mujeres mientras que en Estados Unidos la cifra llega al 39% y en el Reino Unido al 25%. Los juegos más exitosos son “La leyenda de Zelda”, “Los Sims” y “Príncipe de Persia: las arenas del tiempo”. Según los especialistas, este tipo de juego atrae por igual a varones y mujeres por la profundidad de su historia y sus personajes.⁷⁹

Se debe apostar a desarrollar programas que permitan la incorporación de las mujeres en la creación y diseño de páginas web, la gestión de bases de datos, el uso de las TIC como medio de defensa de los derechos de las mujeres, el comercio electrónico para la mujer y programas para que se incluya a las mujeres formadoras de contenidos en red.

Una aproximación tecnofeminista antepone la necesidad de investigar las formas en las cuales las identidades, necesidades y prioridades de las mujeres son reconfiguradas junto con las tecnologías digitales. Esto abre un espacio de posibilidades frescas para estudios que se sintonizan más con las formas

⁷⁸ Tomado de la Meta 3A de los Objetivos del Milenio disponible en <http://www.un.org/es/millenniumgoals/gender.shtml>, última fecha de consulta el 3 de noviembre de 2014.

⁷⁹ <http://portal.softwarelivre.org/news/2990>, citado por Sabanes Plou, Dafne, “Mujeres y nuevas tecnologías de la información y comunicación”, *op. cit.*, nota 55.

en que diferentes grupos de usuarias asimilan y responden creativamente a numerosas TIC en diversos lugares del mundo real. ...

[L]a investigación debería de estar dirigida a asegurar que las mujeres se involucren a lo largo de los procesos y las prácticas de formación de innovación tecnológica.⁸⁰

Finalmente, la brecha digital de género, como apuntan Susana Velázquez y Cecilia Castaño:

...es en realidad una enorme brecha social que se sustenta en factores de exclusión como la capacidad económica, la disponibilidad de tiempo, los conocimientos, las habilidades y experiencia, el bagaje cultural y lingüístico. Pero además, la tecnología está diseñada por y para hombres, y esto resta protagonismo al papel de las mujeres en su desarrollo y uso. ...la difusión de las TIC no es neutral respecto al género y sus efectos varían en función del origen de las mujeres, así como su clase social, raza, acceso a educación y a la formación, edad y estatus social. Las oportunidades de acceso (que implican tecnología, información y conocimiento) y el control sobre las nuevas tecnologías, varían en función del colectivo de mujeres en el que centremos nuestra atención. Y en este sentido, la edad, el nivel educativo y la profesión, así como los conocimientos, la experiencia y el interés por el aprendizaje, son variables a tener en cuenta a la hora de profundizar en el conocimiento de la brecha digital de género.⁸¹

La inclusión de la perspectiva de género en la Sociedad de la Información puede ser de gran trascendencia para el logro del objetivo 3 del Milenio *Promover la igualdad entre los sexos y el empoderamiento de la mujer*, las TIC pueden ser una herramienta y un parteaguas para cambiar la situación de desigualdad y vulnerabilidad en la que viven en la actualidad muchas mujeres.

VIII. BIBLIOGRAFÍA

AGUILERA PORTALES, Rafael Enrique, *Nuevas perspectivas y desafíos en la protección de los derechos humanos*, México, Instituto de Investigaciones Jurídicas, 2011.

⁸⁰ Wajcman, Judy y Giraldo, Elida (trads.), "TIC e inequidad, ¿ganancias en red para las mujeres?", *op. cit.*, nota 64.

⁸¹ Vázquez Susana y Castaño, Cecilia, "La brecha digital del género: prácticas de e-inclusión y razones de la exclusión de las mujeres", *Asparika*, investigación feminista, núm. 22, 2011, p. 3. Disponible en <http://dialnet.unirioja.es/servlet/articulo?codigo=4161068>, última fecha de consulta el 17 de junio de 2014. Algunas citas fueron omitidas.

- DICCIONARIO DE LA LENGUA ESPAÑOLA, en su versión en línea disponible en <http://lema.rae.es/drae/?val=feminismo>, última fecha de consulta el 16 de junio de 2014.
- BEUCHOT, Mauricio, *Derechos humanos y filosofía*, 5a. ed., México, Fontamara, 2011.
- BURGENTHAL, Thomas, “Human rights”, en *Enciclopedia de Derecho Internacional Público*, en <http://www.mpepil.com>, última fecha de consulta el 23 de febrero de 2014.
- CASSESE, Antonio, *Human Rights in a Changing World*, Inglaterra, Polity Press, 1990.
- CORCUERA CABEZUT, Santiago, “Prólogo”, SERVÍN RODRÍGUEZ, Christopher Alexis, *La Paz, ¿un objetivo de la Corte Penal Internacional?*, México, Porrúa, Universidad Veracruzana, 2013.
- FERRAJOLI, Luigi, “Por una teoría de los derechos fundamentales”, en GONZÁLEZ PLASCENCIA, Luis y MORALES SÁNCHEZ, Julieta (coords.), *Derechos humanos. Actualidades y desafíos*, t. I, núm. 61, México, Fontamara, 2012.
- FISHER, Helen, *El primer sexo. Las capacidades innatas de las mujeres y cómo están cambiando el mundo*, México, Taurus, 2006.
- GARCÍA BARRERA, Myrna Elia, *Derecho de las nuevas tecnologías*, México, UNAM, Instituto de Investigaciones Jurídicas, 2011.
- HUNT, Lynn, *La invención de los derechos humanos*, trad. de Jordi Beltrán Ferrer, Barcelona, Tusquets, 2009.
- LAPORTA, Francisco, “El concepto de derechos humanos”, *Diógenes*.
- PANKIKKAR, R., “Is the Notion of Human Rights a Western Concept?”, *Revista Diógenes*, núm. 30, vol. 75, 1982.
- SABANES PLOU, Dafne, “Mujeres y nuevas tecnologías de la información y comunicación”, en *Tecnologías de la información y la comunicación*, cuadernos internacionales de tecnología para el desarrollo humano, vol. 9, núm. 1, 2011, España, Ingeniería sin Fronteras, Universidad de la Rioja, disponible en <http://dialnet.unirioja.es/servlet/articulo?codigo=3962256>.
- SAU, Victoria, *Diccionario ideológico feminista*, vol. I, Barcelona, Icaira, 2000.
- VARELA, Nuria, *Feminismo para principiantes*, Barcelona, No ficción, 2013.
- VÁZQUEZ Susana y CASTAÑO, Cecilia, “La brecha digital del género: prácticas de e-inclusión y razones de la exclusión de las mujeres”, *Asparika*, investigación feminista, núm. 22, 2011.
- WAJCMAN, Judy y GIRALDO, Elida (trads.), “TIC e inequidad, ¿ganancias en red para las mujeres?”, *Educación y Pedagogía*, vol. 24, núm. 62, 2012.

TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC), PROTECCIÓN DE DATOS Y DERECHOS HUMANOS EN LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

Florian HUBER*

SUMARIO: I. *Introducción.* II. *Contexto, antecedentes y fundamentos normativos de la protección de datos en Europa.* III. *Definición y ámbito de protección de los datos personales.* IV. *Obligaciones estatales en materia de protección de datos personales.* V. *Los requisitos para una injerencia justificada en virtud de la CEDH.* VI. *Categorías de interferencia y su justificación en la jurisprudencia del TEDH.* VII. *Conclusiones.* VIII. *Bibliografía.* IX. *Anexos de jurisprudencia del TEDH.*

I. INTRODUCCIÓN

El uso de nuevas tecnologías de información y comunicación (TIC) plantea numerosas cuestiones y debates en el ámbito cultural, social, político, económico y jurídico. El Tribunal Europeo de Derechos Humanos (en adelante TEDH) se ha pronunciado sobre la compatibilidad del uso de las TIC y nuevas tecnologías informáticas con los derechos humanos consagrados en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, más conocido como la Convención Europea de Derechos Humanos (en adelante la CEDH), en muchas sentencias. A lo largo de su jurisprudencia, el TEDH ha examinado múltiples situaciones relacionadas con la protección de datos, entre otras la admisibilidad de interceptaciones de la comunicación, diversas formas de vigilancia electrónica

* Profesor visitante de la Escuela de Política y Relaciones Internacionales e investigador del Instituto de Derechos Humanos y Derecho Internacional Humanitario (IDHUSA), de la Escuela de Derecho, Universidad Sergio Arboleda, Bogotá, Colombia. El autor agradece los valiosos comentarios, aportes y sugerencias de Evelyn Téllez Carvajal y Ángela María Peralta Figueredo. Posibles errores son de responsabilidad exclusiva del autor.

y la protección contra el almacenamiento de datos personales por parte de las autoridades públicas. Tal jurisprudencia se ha establecido gradualmente desde los años setenta.

El siguiente artículo pretende dar un panorama general sobre los lineamientos jurisprudenciales del TEDH, analizando primero, el contexto, antecedentes y fundamentos normativos de la protección de datos en Europa; segundo, la definición y el ámbito de protección de los datos personales; tercero, las obligaciones estatales en materia de protección de datos personales; cuarto, los requisitos para una injerencia justificada en virtud de la CEDH, y quinto, las categorías de interferencia y su justificación en la jurisprudencia del TEDH.

II. CONTEXTO, ANTECEDENTES Y FUNDAMENTOS NORMATIVOS DE LA PROTECCIÓN DE DATOS EN EUROPA

1. *El Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950)*

En 1950 se aprobó el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que entró en vigor en 1953. Según tal convención, los Estados tienen la obligación internacional de respetar y cumplir lo establecido en ella. Todo Estado miembro del Consejo de Europa debe incorporar o hacer efectiva la CEDH en su legislación nacional, lo cual obliga a las instituciones estatales a actuar en conformidad con las disposiciones del Convenio. El derecho a la protección de los datos personales forma parte de los derechos protegidos por el artículo 8 de la CEDH,¹ que garantiza el derecho a la vida privada y familiar, el domicilio y la correspondencia, y establece las condiciones para restringir este derecho.²

¹ El artículo 8o. de la CEDH establece: “1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás”.

² Boehm, F., *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, pp. 25-84.

2. *El Convenio núm. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (1981)*

Con el auge de las nuevas tecnologías informáticas en la década de los años sesenta se planteó la creciente necesidad de desarrollar reglas más detalladas y precisas para ofrecer un marco normativo adecuado para la protección de los datos de las personas. Para tal fin, a mediados de la década de los años setenta, el Comité de Ministros del Consejo de Europa adoptó varias resoluciones sobre la protección de datos de carácter personal, en referencia al artículo 8o. de la CEDH.³ En 1981 se estableció el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (el Convenio núm. 108).⁴ En 1999 el Convenio núm. 108 fue modificado para permitir que la UE se convirtiera en una de las Partes del Convenio.⁵ Asimismo, el Convenio núm. 108 está abierto a la adhesión de los Estados no miembros del Consejo de Europa, incluyendo países no europeos. El potencial del Convenio núm. 108 como estándar universal y su carácter abierto podrían servir como base para la promoción de la protección de datos a nivel mundial. Hasta el momento, 45 de las 46 partes contratantes del Convenio núm. 108 son Estados miembros del Consejo de Europa. Asimismo, todos los Estados miembros de la UE han ratificado el Convenio núm. 108. Uruguay, el primer país no europeo, se adhirió en agosto de 2013 y Marruecos, que ha sido invitado a adherirse al Convenio núm. 108 por el Comité de Ministros, está en el proceso de formalización de la adhesión. En 2001 se adoptó un Protocolo Adicional al Convenio núm. 108, que establece disposiciones respecto a flujos transfronterizos de datos a países no partes del Convenio, y

³ Consejo de Europa, Comité de Ministros (1973), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 26 de septiembre de 1973; Comité de Ministros (1974), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 de septiembre de 1974.

⁴ El Convenio se encuentra en el siguiente link: http://www.coe.int/t/dghl/standard-setting/dataprotection/Global_standard/Conv%20108_es.pdf, consultado por última vez el 13 de octubre de 2014; véase al respecto, Schwartz, P., "European Data Protection Law and Restrictions on International Data Flows", 80 *Iowa L. Rev.* (1994-95), 477 y 478.

⁵ Consejo de Europa, Comité de Ministros, Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data (ETS núm. 108) allowing the European Communities to accede, 15 de junio 1999; artículo 23(2) del Convenio núm. 108.

respecto al establecimiento obligatorio de instancias nacionales de control de datos.⁶ Con la finalidad de modernizar el Convenio núm. 108 y a través de una consulta pública llevada a cabo en 2011, se consolidaron dos objetivos principales: el refuerzo de la protección de la intimidad en el ámbito digital y el fortalecimiento de mecanismos de seguimiento a la implementación del Convenio núm. 108.⁷

El Convenio núm. 108 ha sido, y sigue siendo, el único instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos. Se aplica a todo el procesamiento de datos efectuado por sectores privados y públicos, por ejemplo, por parte del Poder Judicial y las autoridades policiales. Se protege al individuo contra los abusos, que pueden acompañar a la recopilación y el tratamiento automatizado de los datos personales, y busca, al mismo tiempo, regular el flujo transfronterizo de los datos personales. En cuanto a la recolección y el tratamiento automatizados de los datos personales, los principios establecidos en el Convenio núm. 108 se refieren, en particular, a la colección legal y el tratamiento automatizado de datos, almacenados con fines legítimos determinados y no para su uso con fines incompatibles a éstos, ni conservarse durante más tiempo del necesario. También se refieren a la calidad de los datos, en particular, que deben ser adecuados, pertinentes y no excesivos (principio de proporcionalidad), así como precisos. Además de ofrecer garantías sobre la recolección y el tratamiento de los datos personales, que prohíbe, en la ausencia de garantías jurídicas adecuadas, el tratamiento de los datos “sensibles”, como el origen étnico de una persona, las tendencias o preferencias políticas, la salud, la religión, la vida sexual o el registro de los antecedentes criminales. El Convenio consagra el derecho del individuo a conocer qué información sobre su persona se encuentra almacenada y, si es necesario, proceder a su rectificación. Las restricciones a los derechos establecidos en la Convención son posibles sólo bajo imperiosas causales de interés, tales como la seguridad del Estado o la defensa del mismo que estén en juego.

⁶ Consejo de Europa, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, CETS núm. 181, 2001.

⁷ Handbook on European Data Protection Law, disponible en: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, p. 17, última fecha de consulta el 13 de octubre de 2014.

3. *La protección de datos en la Unión Europea*

Respecto a la protección de datos en la UE,⁸ el primer instrumento jurídico de la UE sobre protección de datos fue la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva de protección de datos).⁹ Fue adoptada en 1995 cuando varios Estados miembros ya habían adoptado leyes nacionales de protección de datos, considerando que la libre circulación de bienes, capitales, servicios y personas en el mercado común europeo requiere el flujo libre de los datos, lo cual no podría realizarse sin que los Estados miembros contarán con un sistema común de protección de datos. El objetivo de adoptar la Directiva de protección de datos era la armonización europea de las leyes nacionales en materia de protección de datos. La Directiva ofrece un alto grado de especificidad comparable al de las leyes nacionales de protección de datos. En consecuencia, los Estados miembros de la UE disponen de una discreción limitada respecto a la implementación de la Directiva.

El ámbito de aplicación material de la Directiva se limitaba a los asuntos del mercado común europeo. Fuera de su ámbito de aplicación se encontraban, sobre todo, cuestiones relacionadas con la cooperación policial y de justicia penal. Respecto al ámbito de aplicación personal, la Directiva contenía una excepción, la denominada exención de los hogares, es decir, el tratamiento de los datos personales por particulares con meros fines personales o para su hogar privado. Asimismo, es importante tener en cuenta que la aplicación territorial de la Directiva de protección de datos se extendía más allá de los Estados miembros de la UE e incluye los Estados no pertenecientes a la UE que forman parte del Espacio Económico Europeo (EEE), es decir, Islandia, Liechtenstein y Noruega.

Dado que la Directiva de Protección de Datos establecía solamente obligaciones para los Estados miembros de la UE y del EEE, era necesario

⁸ Arenas Ramiro, M., “La protección de datos personales en los países de la Unión Europea”, 16 *Revista Jurídica de Castilla y León* (2008), pp. 113-168.

⁹ Directiva 95/46/CE (24 de octubre de 1995) del Parlamento Europeo y del Consejo, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos. Korff, D., EC study on implementation of data protection Directive (StudyContract ETD/2001/B5-3001/A/49) Human Rights Centre, Essex; Cambridge, 2002, disponible en: <http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE>, última fecha de consulta el 13 de octubre de 2014.

un instrumento legal adicional para garantizar la protección de datos frente a las instituciones y órganos de la UE. Por tal razón, se aprobó el Reglamento (CE) núm. 45/2001 del Parlamento Europeo y del Consejo sobre la protección de las personas con respecto al tratamiento de datos personales por las instituciones y los organismos comunitarios y la libre circulación de estos datos.¹⁰

Además de la Directiva sobre protección de datos, se han aprobado varios instrumentos que contienen disposiciones más detalladas respecto a materias específicas para lograr claridad respecto a los criterios de ponderación y equilibrio de intereses legítimos en conflicto. Un ejemplo es la Directiva 97/66/CE, sobre Protección de Datos y Telecomunicaciones, encargada de regular la protección de datos personales en el sector de las telecomunicaciones,¹¹ que ha sido derogada por la Directiva 2002/58/CE, sobre Protección de Datos y Comunicaciones Electrónicas,¹² la cual por su parte ha sido modificada por la Directiva 2006/24/CE sobre Conservación de Datos de Tráfico en las Comunicaciones Electrónicas respecto a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.¹³

III. DEFINICIÓN Y ÁMBITO DE PROTECCIÓN DE LOS DATOS PERSONALES

De acuerdo con el Convenio del Consejo de Europa para la protección respecto al tratamiento automatizado de los datos personales de 1981, se define como “datos personales” a cualquier información relativa a una per-

¹⁰ Reglamento (CE) núm. 45/2001 (18 de diciembre de 2001), del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, y a la libre circulación de esos datos.

¹¹ Directiva 97/66/CE (15 de diciembre de 1997), del Parlamento Europeo y del Consejo, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el sector de las Telecomunicaciones.

¹² Directiva 2002/58/CE (12 de julio de 2002), del Parlamento Europeo y del Consejo, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el sector de las Comunicaciones Electrónicas.

¹³ Directiva 2006/24/CE (15 de marzo de 2006), del Parlamento Europeo y del Consejo, relativa a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

sona física identificada o identificable.¹⁴ La recopilación, el almacenamiento y el uso de datos personales caen claramente dentro del ámbito de la vida privada protegida por el artículo 8o. de la Convención, que abarca una amplia gama de intereses, es decir, la vida privada y familiar, el hogar y la correspondencia. La protección de los datos personales es de importancia fundamental para el disfrute del derecho a la vida privada y familiar de una persona.¹⁵ La vida privada incluye la privacidad de las comunicaciones, que cubre la seguridad y la privacidad de correo, teléfono, correo electrónico y otras formas de comunicación, y la privacidad de la información, que incluye la privacidad en Internet.

El concepto de la vida privada incluye elementos relacionados con el derecho de una persona a su imagen.¹⁶ En otras palabras, fotografías, videos u otros retratos que contienen la imagen de una persona caen en el ámbito del artículo 8o. Esto es relevante para el almacenamiento de imágenes en los sitios web comunitarios o sociales. Asimismo, la grabación de la voz de una persona, por ejemplo, para su posterior uso, difusión o análisis también equivale a una injerencia en su derecho al respeto de la vida privada.¹⁷ Los datos obtenidos mediante cualquier medio de grabación en lugares públicos en condiciones o circunstancias que vayan más allá de lo normalmente previsible, también ubica tales datos dentro del ámbito del artículo 8o.¹⁸ Por ejemplo, en *Uzun vs. Alemania* el TEDH consideró que la vigilancia del demandante a través de GPS y el tratamiento y la utilización de los datos obtenidos de este modo implicaba una injerencia en su vida privada protegida por el artículo 8o. de la CEDH.¹⁹ En síntesis, el TEDH ha señalado que ya desde la mera recopilación y el almacenamiento de información sobre la vida privada de un individuo se está ante una injerencia en el ámbito de protección del artículo 8o. de la CEDH, independientemente del uso de tal información.²⁰ La recopilación y el almacenamiento de información perso-

¹⁴ Artículo 2o.(a) del Convenio núm. 108.

¹⁵ TEDH, Caso *S. y Marper vs. Reino Unido* [GC], núms. 30562/04 y 30566/04, 4 de diciembre de 2008, § 41.

¹⁶ TEDH, Caso *Sciacca vs. Italia*, núm. 50774/99, 11 de enero de 2005, § 29.

¹⁷ TEDH, Caso *P.G. y J.H. vs. Reino Unido*, núm. 44787/98, 25 de septiembre de 2001, §§ 59-60.

¹⁸ TEDH, Caso *Peck vs. Reino Unido*, núm. 44647/98, 28 de enero de 2003, §§ 60-63.

¹⁹ TEDH, Caso *Uzun vs. Alemania*, núm. 35623/05, 2 de septiembre de 2010, § 46.

²⁰ TEDH, Caso *Leander vs. Suecia*, núm. 9248/81, 26 de marzo de 1987; TEDH, Caso *Kopp vs. Suiza*, núm. 23224/94, 25 de marzo de 1998; TEDH, Caso *Amann vs. Suiza* [GC], núm. 27798/95, 16 de febrero de 2000, § 69 (“The storing by a public authority of information relating to an individual’s private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding”).

nal por parte del Estado, por ejemplo, mediante un registro policial, toca el ámbito de protección del derecho al respeto de la vida privada,²¹ sin que el uso posterior de la información almacenada influya en esta apreciación.²² Respecto al impacto de las técnicas científicas modernas para la protección de la vida privada, el TEDH ha resaltado que “la protección ...se debilitaría inaceptablemente si el uso de técnicas científicas modernas ...fuera permitido a cualquier costo y sin equilibrar cuidadosamente los beneficios potenciales del uso extensivo de tales técnicas contra importantes intereses de la vida privada”.²³

IV. OBLIGACIONES ESTATALES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

El TEDH ha aclarado que el artículo 8o. de la CEDH no sólo obliga a los Estados a abstenerse de cualquier acción que pueda violar los derechos consagrados en la Convención, sino que, bajo ciertas circunstancias, los Estados tienen la obligación positiva de asegurar activamente el respeto efectivo del derecho a la vida privada y familiar. En este sentido, el artículo 8o. de la CEDH abarca, por un lado, la obligación negativa para los Estados de respetar el derecho a la vida privada de los ciudadanos frente a injerencias arbitrarias de las autoridades públicas; por otro lado, contiene una obligación positiva inherente a la obligación de protección efectiva de la vida privada.²⁴ Esta obligación positiva implica el deber de adoptar medidas por parte del Estado destinadas a asegurar el respeto de la vida privada, incluso en el ámbito de las relaciones de los individuos entre sí, por ejemplo, para un usuario de Internet o los que proporcionan el acceso a un sitio web en particular. En otras palabras, existe una obligación positiva del Estado de garantizar una disuasión eficaz contra los actos graves a los datos personales de una persona, a veces necesariamente por medio de disposiciones penales.²⁵

²¹ TEDH, Caso *Leander vs. Suecia*, núm. 9248/81, 26 de marzo de 1987, § 48.

²² TEDH, Caso *Amann vs. Suiza* [GC], núm. 27798/95, 16 de febrero de 2000, § 69.

²³ TEDH, Caso *S. y Marper vs. Reino Unido* [GC], núms. 30562/04 y 30566/04, 4 de diciembre de 2008, § 112.

²⁴ TEDH, Caso *Airey vs. Irlanda*, núm. 6289/73, 9 de octubre de 1979, § 32.

²⁵ TEDH, Caso *X y Y vs. Países Bajos*, núm. 8978/80, 26 de marzo de 1985, §§ 23-24 y 27; TEDH, Caso *August vs. Reino Unido*, núm. 36505/02, 21 de enero de 2003; TEDH, Caso *M.C. vs. Bulgaria*, núm. 39272/98, 4 de diciembre de 2003, § 150; TEDH, Caso *K.U. vs. Finlandia*, núm. 2872/02, 2 de diciembre de 2008, § 43.

V. LOS REQUISITOS PARA UNA INJERENCIA JUSTIFICADA EN VIRTUD DE LA CEDH

El tratamiento de los datos personales puede constituir una injerencia en el derecho al respeto de la vida privada de la persona afectada. Sin embargo, el derecho al respeto de la vida privada no es un derecho absoluto, sino que debe ser equilibrado y ponderado con otros intereses legítimos, ya sean de otras personas (intereses privados), o de la sociedad como un todo (intereses públicos). Las condiciones en las que se justifica la interferencia del Estado son las siguientes.

1. *En conformidad con la ley*

De acuerdo con la jurisprudencia del TEDH, la interferencia es en conformidad con la ley si se basa en una disposición del derecho interno, que tiene ciertas cualidades. La ley debe ser “accesible a las personas interesadas y previsible en cuanto a sus efectos”.²⁶ Una regla es previsible “si está formulada con la suficiente precisión para permitir a cualquier particular, en caso necesario con el asesoramiento adecuado, para regular su conducta”.²⁷ El grado de precisión requerido respecto a una ley en este sentido dependerá de la materia particular en cuestión.²⁸ Por ejemplo, en *Rotaru vs. Rumania*, el TEDH consideró una violación del artículo 8o. de la CEDH, dado que la ley rumana permitía la recopilación, el registro y el almacenamiento de archivos secretos de información que afectarían la seguridad nacional, sin que se hubieran establecido límites respecto al ejercicio de dicha competencia, y que se encontraba bajo la total discreción de las autoridades estatales.²⁹ Dado que la legislación nacional no definía el tipo de información que podía ser procesada y guardada, las categorías de personas contra las cuales se

²⁶ TEDH, Caso *Amann vs. Suiza* [GC], núm. 27798/95, 16 de febrero de 2000, § 50; TEDH, *Kopp vs. Suiza*, núm. 23224/94, 25 de marzo de 1998, § 55; TEDH, Caso *Iordachi y otros vs. Moldavia* núm. 25198/02, 10 de febrero de 2009, § 50.

²⁷ TEDH, Caso *Amann vs. Suiza* [GC], núm. 27798/95, 16 de febrero de 2000, § 56; TEDH, Caso *Malone vs. Reino Unido*, núm. 8691/79, 2 de agosto de 1984, § 66; TEDH, Caso *Silver y otros vs. Reino Unido*, núms. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 y 7113/75, 25 de marzo de 1983, § 88.

²⁸ TEDH, Caso *The Sunday Times vs. Reino Unido*, núm. 6538/74, 26 de abril de 1979, § 49; TEDH, Caso *Silver y otros vs. Reino Unido*, núms. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 y 7113/75, 25 de marzo de 1983, § 88.

²⁹ TEDH, Caso *Rotaru vs. Rumania* [GC], núm. 28341/95, 4 de mayo de 2000, § 61.

podrían tomar medidas de vigilancia, o las circunstancias en que tales medidas pudieran ser utilizadas para la investigación y el procesamiento contra una persona, el Tribunal llegó a la conclusión de que el derecho interno no cumplía con el requisito de previsibilidad de la ley en virtud del artículo 8o. de la CEDH.³⁰ En *Taylor-Sabori vs. Reino Unido*, el demandante había sido el objetivo de actos de vigilancia de la policía. Con el uso de un “clon” de un buscapersonas del demandante, la policía pudo interceptar los mensajes enviados a él. El demandante fue arrestado y acusado de conspiración para suministrar drogas. Una parte de la acusación contra él se basaba en los mensajes escritos mediante el buscapersonas que habían sido transcritas por la policía. Sin embargo, en el momento del juicio contra el demandante, no había ninguna disposición en la ley británica que regulara la interceptación de las comunicaciones transmitidas a través de un sistema de telecomunicaciones privadas.³¹ Por tanto, el TEDH concluyó que la interferencia con sus derechos no había ocurrido “en conformidad con la ley”.³²

2. *Fin legítimo*

El fin u objetivo legítimo puede ser uno de los intereses públicos mencionados en el artículo 8o. de la CEDH, o los derechos y libertades de los demás. En este sentido, en *Peck vs. Reino Unido* el demandante intentó suicidarse en la calle cortándose las muñecas, sin saber que una cámara de circuito cerrado de televisión (CCTV) le estaba filmando durante el intento. Después de que la policía había revisado las cámaras de circuito cerrado, se pasó la grabación del CCTV a los medios de comunicación que publicaron las escenas. El TEDH consideró que no había razones pertinentes o suficientes que justificaran la revelación directa de las imágenes por las autoridades al público sin haber obtenido el consentimiento previo del demandante o haber enmascarado su identidad.³³ Por tanto, el Tribunal llegó a la conclusión de que había habido una violación del artículo 8o. de la CEDH.³⁴

³⁰ TEDH, Caso *Rotaru vs. Rumania* [GC], núm. 28341/95, 4 de mayo de 2000, § 62.

³¹ TEDH, Caso *Taylor-Sabori vs. Reino Unido*, núm. 47114/99, 22 de enero de 2003, § 19.

³² TEDH, Caso *Taylor-Sabori vs. Reino Unido*, núm. 47114/99, 22 de enero de 2003, § 19.

³³ TEDH, Caso *Peck vs. Reino Unido*, núm. 44647/98, 28 de enero de 2003, § 85.

³⁴ TEDH, Caso *Peck vs. Reino Unido*, núm. 44647/98, 28 de enero de 2003, § 87.

3. *Medida necesaria en una sociedad democrática*

El TEDH ha declarado que la noción de la necesidad de la medida en una sociedad democrática implica que la interferencia corresponde a una necesidad social imperiosa y que, en particular, es proporcional al fin legítimo perseguido.³⁵ En *Khelili vs. Suiza*³⁶ el TEDH reconoció que, en principio, la retención de datos personales de un individuo, que podría cometer otro delito, puede ser proporcionada bajo ciertas circunstancias.³⁷ Sin embargo, en el caso concreto, la consideración de estar ante un caso de prostitución ilegal parecía demasiado vaga y general, y no fue apoyada por los hechos concretos, ya que la demandante nunca había sido declarada culpable de la prostitución ilegal. Por lo tanto, la medida no podía ser considerada como una “necesidad social imperiosa” en el sentido del artículo 8o. de la CEDH.³⁸ En *Leander vs. Suecia*, el TEDH resolvió que el escrutinio secreto de personas que solicitan empleo en puestos de importancia para la seguridad nacional no era, en sí misma, incompatible con el requisito de una medida necesaria en una sociedad democrática. Las salvaguardias especiales establecidas en la legislación nacional para la protección de los intereses del titular de los datos (por ejemplo, mediante los controles ejercidos por el Parlamento y el Canciller de Justicia) le permitió concluir al TEDH que el sistema de control de personal cumplía con los requisitos del artículo 8o.(2) de la CEDH.³⁹ Dado el amplio margen de apreciación, el Estado demandado tenía derecho a considerar que, en el caso del demandante, los intereses de la seguridad nacional prevalecían sobre el derecho a la privacidad de los individuales.⁴⁰ Por lo tanto, el Tribunal llegó a la conclusión de que no se había producido una violación del artículo 8o. de la CEDH.⁴¹

³⁵ TEDH, Caso *Leander vs. Suecia*, núm. 9248/81, 26 de marzo de 1987, § 58.

³⁶ TEDH, Caso *Khelili vs. Suiza*, núm. 16188/07, 18 de octubre de 2011. En este caso la policía encontró durante una requisa de la demandante varias tarjetas con el texto “Mujer, bastante agradable, treinta y tantos años, le gustaría conocer a un hombre para tomar una copa juntos o salir de vez en cuando. Tel. No. ...”, la demandante alegó que a raíz de este descubrimiento la policía la llevó en sus registros como una prostituta. La demandante solicitó que la palabra “prostituta” fuera borrada de los registros informáticos de la policía.

³⁷ TEDH, Caso *Khelili vs. Suiza*, núm. 16188/07, 18 de octubre de 2011, §§ 61-62.

³⁸ TEDH, Caso *Khelili vs. Suiza*, núm. 16188/07, 18 de octubre de 2011, §§ 63-71.

³⁹ TEDH, Caso *Leander vs. Suecia*, núm. 9248/81, 26 de marzo de 1987, §§ 66-67.

⁴⁰ TEDH, Caso *Leander vs. Suecia*, núm. 9248/81, 26 de marzo de 1987, § 67.

⁴¹ TEDH, Caso *Leander vs. Suecia*, núm. 9248/81, 26 de marzo de 1987, § 67.

VI. CATEGORÍAS DE INTERFERENCIA Y SU JUSTIFICACIÓN EN LA JURISPRUDENCIA DEL TEDH

1. *Inclusión de datos personales en una base de datos electrónica*

En *S. y Marper vs. Reino Unido*⁴² el TEDH encontró una violación del artículo 8 de la CEDH, considerando que no se podía permitir el uso de técnicas científicas modernas en el sistema de justicia penal a cualquier costo y sin equilibrar cuidadosamente los beneficios potenciales de la amplia utilización de tales técnicas frente al derecho a la vida privada.⁴³ El Tribunal concluyó que el almacenamiento generalizado de las huellas dactilares, muestras celulares y pruebas de ADN de personas sospechosas pero no condenadas por delitos, tal como ocurrió en ese caso particular, no pudieron llegar a un equilibrio justo entre el interés público y el derecho a la privacidad.⁴⁴ En un sentido similar, en *M.K. vs. Francia*⁴⁵ el Tribunal consideró que, en vista de las circunstancias del caso, el almacenamiento de los datos en cuestión había sido una injerencia desproporcionada respecto a la vida privada.⁴⁶ Por otro lado, en *B.B. vs. Francia*,⁴⁷ *Gardel vs. Francia*⁴⁸ y *M.B. vs. Francia*,⁴⁹ relacionados con tres condenados por violación sexual de menores de 15 años, y que se quejaron, en particular, por su inclusión en la base de datos nacional de delincuentes sexuales, el TEDH no encontró una violación del artículo 8o. de la CEDH, dado que la duración de la conservación de datos (30 años como máximo) no era desproporcionada en relación con la finalidad perseguida (la prevención de la delincuencia) por la retención de

⁴² TEDH, Caso *S. y Marper vs. Reino Unido* [GC], núms. 30562/04 y 30566/04, 4 de diciembre de 2008, que se refiere al almacenamiento temporalmente ilimitado de huellas dactilares, muestras celulares y de ADN de dos procesados en una base de datos después de un proceso penal, en el cual uno de los procesados había sido absuelto, mientras respecto al otro procesado se archivó el caso.

⁴³ TEDH, Caso *S. y Marper vs. Reino Unido* [GC], núms. 30562/04 y 30566/04, 4 de diciembre de 2008, § 112.

⁴⁴ TEDH, Caso *S. y Marper vs. Reino Unido* [GC], núms. 30562/04 y 30566/04, 4 de diciembre de 2008, § 125.

⁴⁵ TEDH, Caso *M.K. vs. Francia*, núm. 19522/09, 18 de abril de 2013, en el cual el demandante, un ciudadano francés, se opuso a que después de dos investigaciones por presunto hurto, que terminaron en un caso con su absolución y en el otro con una decisión de no procesar, sus huellas quedaran incluidas en una base de datos por las autoridades francesas.

⁴⁶ TEDH, Caso *M.K. vs. Francia*, núm. 19522/09, 18 de abril de 2013, § 43.

⁴⁷ TEDH, Caso *B.B. vs. Francia*, núm. 5335/06, 17 de diciembre de 2009.

⁴⁸ TEDH, Caso *Gardel vs. Francia*, núm. 16428/05, 17 de diciembre de 2009.

⁴⁹ TEDH, Caso *M.B. vs. Francia*, núm. 22115/06, 17 de diciembre de 2009.

la información, y que la consulta de estos datos por las autoridades judiciales y administrativas estaba sujeta a determinadas situaciones y un deber de confidencialidad. Asimismo, el TEDH consideró manifiestamente infundada la demanda en *Peruzzo y Martens vs. Alemania*, en el cual los demandantes, condenados por delitos graves, se habían quejado sobre las órdenes de los tribunales nacionales de recoger material celular de ellos y almacenarlos en una base de datos en forma de los perfiles de ADN para el propósito de facilitar la investigación de posibles futuros crímenes. El Tribunal declaró inadmisibile la demanda, considerando que las medidas impugnadas podían considerarse una injerencia necesaria en una sociedad democrática.⁵⁰

2. *Vigilancia de la comunicación privada por autoridades estatales*

El TEDH ha analizado la admisibilidad de actos de vigilancia de medios de comunicación por autoridades estatales de seguridad, como centros de reclusión, la policía, los servicios secretos, las autoridades judiciales u otras instituciones públicas.

A. *Vigilancia de la comunicación privada de detenidos*

En varios casos el TEDH se ha pronunciado sobre la admisibilidad de la vigilancia y el control de la correspondencia de personas detenidas. En varios casos contra Polonia, entre éstos *Pisk-Piskowski vs. Polonia*,⁵¹ *Matwiejczuk vs. Polonia*⁵² y *Przyjemski vs. Polonia*,⁵³ el Tribunal sostuvo que, ante la práctica de las autoridades nacionales de estampar la expresión “censurado” en las cartas de los detenidos, la Corte no tenía otra alternativa que suponer que esas cartas habían sido abiertas y su contenido leído, en violación del artículo 8o. de la CEDH. Posteriormente, ante la adopción de reformas normativas, en *Bista vs. Polonia*⁵⁴ el Tribunal estableció que en el derecho nacional existía un recurso efectivo para quejas de los presos en la censura de correspondencia.⁵⁵ Respecto al establecimiento de obstácu-

⁵⁰ TEDH, Caso *Peruzzo y Martens vs. Alemania*, núms. 7841/08 y 57900/12, 4 de junio de 2013, §§ 49-50.

⁵¹ TEDH, Caso *Pisk-Piskowski vs. Polonia*, núm. 92/03, 14 de junio de 2005.

⁵² TEDH, Caso *Matwiejczuk vs. Polonia*, núm. 37641/97, 2 de diciembre de 2003.

⁵³ TEDH, Caso *Przyjemski vs. Polonia*, núm. 6820/07, 5 de octubre de 2010.

⁵⁴ TEDH, Caso *Bista vs. Polonia*, núm. 22807/07, 12 de enero de 2010.

⁵⁵ TEDH, Caso *Bista vs. Polonia*, núm. 22807/07, 12 de enero de 2010, §§ 47-50.

los para la libre correspondencia, en *Golder vs. Reino Unido* el TEDH encontró una violación del artículo 8o., dado que el Tribunal no podía discernir cómo la necesidad de prevenir un desorden podría requerir que el demandante no pudiera comunicarse con su abogado con miras a mostrar su inocencia respecto a los cargos presentados contra él.⁵⁶ Finalmente, respecto a la interceptación de la correspondencia por su contenido, el TEDH distinguió en *Silver y otros vs. Reino Unido*⁵⁷ entre la violación del artículo 8o. de la CEDH en relación con cartas interceptadas que contenían un lenguaje ofensivo, y la no violación del artículo 8o. en cuanto a cartas que contenían amenazas.⁵⁸ Por último, las limitaciones a la correspondencia se han analizado en el contexto de procesos ante la Comisión Europea de Derechos Humanos o el Tribunal mismo. Asimismo, en *Campbell vs. Reino Unido*⁵⁹ se produjo una violación del artículo 8o. de la CEDH por la revisión de la correspondencia del demandante con su abogado y con la Comisión. En *Cotlet vs. Rumania*, relacionado con la existencia de obstáculos respecto al intercambio de correspondencia con el Tribunal, éste determinó una violación del artículo 8o. de la CEDH por los retrasos en el envío de cartas del demandante, la apertura de su correspondencia y la negativa de las autoridades penitenciarias a suministrarle los materiales necesarios para su correspondencia con el Tribunal.⁶⁰

En cuanto a la interceptación acústica de detenidos y sus familiares, el TEDH determinó en *Wisse vs. Francia*,⁶¹ que el sistema de interceptaciones de las conversaciones entre los detenidos y sus familiares en las salas de visita en una cárcel constituía una violación del artículo 8o. de la CEDH, porque la legislación francesa no indicaba con suficiente claridad cómo y en qué forma las autoridades estatales podían interferir en la vida privada de los detenidos, así como la ley no determinaba para las autoridades el alcance y la forma de ejercicio de su discreción de control y vigilancia en esa área.⁶²

⁵⁶ TEDH, Caso *Golder vs. Reino Unido*, núm. 4451/70, 21 de febrero de 1975, § 45.

⁵⁷ TEDH, Caso *Silver y otros vs. Reino Unido*, núms. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 y 7113/75, 25 de marzo de 1983.

⁵⁸ TEDH, Caso *Silver y otros vs. Reino Unido*, núms. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 y 7113/75, 25 de marzo de 1983, §§ 97-104.

⁵⁹ TEDH, Caso *Campbell vs. Reino Unido*, núm. 13590/88, 25 de marzo de 1992.

⁶⁰ TEDH, Caso *Cotlet vs. Rumania*, núm. 38565/97, 3 de junio de 2003, §§ 63-65.

⁶¹ TEDH, Caso *Wisse vs. Francia*, núm. 71611/01, 20 de diciembre de 2005.

⁶² TEDH, Caso *Wisse vs. Francia*, núm. 71611/01, 20 de diciembre de 2005, § 34.

B. *Vigilancia electrónica por la policía, las autoridades judiciales y los servicios secretos*

a. *Vigilancia electrónica por la policía*

El TEDH ha condenado durante los últimos 30 años en reiteradas ocasiones a varios Estados por la vigilancia electrónica efectuada por la Policía, debido a la falta o violación de leyes nacionales regulatorias de la materia. Por ejemplo, en *Malone vs. Reino Unido*,⁶³ que trató de la interceptación de conversaciones en el contexto de un juicio penal por posesión de bienes robados y el registro de los números marcados en un teléfono en particular, tales actividades no habían estado de acuerdo con la ley nacional. Por la misma razón, el TEDH encontró una violación del artículo 8o. de la CEDH en *Khan vs. Reino Unido*⁶⁴ por vigilancia del demandante por el uso de un dispositivo de interceptación en un proceso por delitos de tráfico de drogas. En *A. vs. Francia*⁶⁵ relacionado con la grabación acústica por un particular, con la asistencia de la policía en el contexto de una investigación preliminar, de una conversación telefónica con el demandante, quien presuntamente lo había contratado para llevar a cabo un asesinato. El TEDH encontró una violación del artículo 8o. de la CEDH, ya que la grabación no se había llevado a cabo de conformidad con el procedimiento judicial y no había sido ordenada por un juez de instrucción.⁶⁶ En *P.G. y J.H. vs. Reino Unido*,⁶⁷ que trata sobre la grabación de las voces de los demandantes en una estación de policía por la sospecha de haber intentado cometer un robo, se violó el artículo 8o. Lo anterior dado que en el momento de los acontecimientos no existía una regulación del uso de las escuchas secretas mediante dispositivos por la policía.⁶⁸ En este caso, el TEDH determinó una violación del artículo 8o. de la CEDH por la instalación de un dispositivo de interceptación clandestina por la policía en el apartamento utilizado por uno de los demandantes, lo cual no estaba en conformidad con la ley.⁶⁹ En un sentido si-

⁶³ TEDH, Caso *Malone vs. Reino Unido*, núm. 8691/79, 2 de agosto de 1984.

⁶⁴ TEDH, Caso *Khan vs. Reino Unido*, núm. 6222/10, 20 de diciembre de 2011.

⁶⁵ TEDH, Caso *A. vs. Francia*, núm. 14838/89, 23 de noviembre de 1993.

⁶⁶ TEDH, Caso *A. vs. Francia*, núm. 14838/89, 23 de noviembre de 1993, § 38.

⁶⁷ TEDH, Caso *P.G. y J.H. vs. Reino Unido*, núm. 44787/98, 25 de septiembre de 2001.

⁶⁸ TEDH, Caso *P.G. y J.H. vs. Reino Unido*, núm. 44787/98, 25 de septiembre de 2001, § 63.

⁶⁹ TEDH, Caso *P.G. y J.H. vs. Reino Unido*, núm. 44787/98, 25 de septiembre de 2001, § 38.

milar, en *Vetter vs. Francia*,⁷⁰ la policía, ante la sospecha de que el demandante había cometido un asesinato, instaló un dispositivo en un apartamento que visitaba frecuentemente. EL TEDH determinó una violación del artículo 8o., dado que el derecho francés no indicaba con suficiente claridad y precisión el alcance y la forma de utilizar los dispositivos de interceptación.⁷¹ En *Draksas vs. Lituania*⁷² el TEDH encontró una violación del artículo 8o. a causa de la filtración de una conversación del demandante a la prensa,⁷³ pero no por la interceptación y grabación de las conversaciones *per se*, sino por su posterior divulgación en los procedimientos de la Corte Constitucional en el juicio político contra el ex presidente.⁷⁴

b. Vigilancia electrónica por las autoridades judiciales

Respecto a la vigilancia electrónica de comunicaciones privadas autorizada por autoridades judiciales, el TEDH encontró en *Kruslin vs. Francia*,⁷⁵ que se relacionó con escuchas telefónicas ordenadas por un juez de instrucción en un caso de asesinato, una violación del artículo 8o. Había violación puesto que la legislación francesa no indicaba con suficiente claridad el alcance y la forma de ejercicio de la discreción de las autoridades en este ámbito.⁷⁶ En cuanto a la lucha contra el terrorismo, el TEDH señaló en *Klaas vs. Alemania*,⁷⁷ que “las sociedades democráticas hoy en día se encuentran amenazadas por formas muy sofisticadas de espionaje y por el terrorismo, con la consecuencia de que el Estado, para contrarrestar eficazmente esas

⁷⁰ TEDH, Caso *Vetter vs. Francia*, núm. 59842/00, 31 de mayo de 2005.

⁷¹ TEDH, Caso *Vetter vs. Francia*, núm. 59842/00, 31 de mayo de 2005, §§ 28-29.

⁷² TEDH, Caso *Draksas vs. Lituania*, núm. 36662/04, 31 de julio de 2012, que se relacionó con un político de Lituania, miembro fundador del partido político liberal-demócrata liderado por el ex presidente del país, cuyo teléfono fue interceptado por el Departamento de Seguridad del Estado, y cuyas conversaciones grabadas se filtraron posteriormente a la prensa para ser reveladas por los medios de comunicación en la televisión nacional durante el juicio político contra el ex presidente.

⁷³ TEDH, Caso *Draksas vs. Lituania*, núm. 36662/04, 31 de julio de 2012, § 60. En cuanto a la divulgación de la conversación del demandante con uno de los principales contribuyentes a la campaña electoral del entonces presidente, el TEDH consideró que si bien la ciudadanía tenía derecho a la información sobre los funcionarios públicos, el Departamento de Seguridad del Estado debió mantener la grabación confidencial.

⁷⁴ TEDH, Caso *Draksas vs. Lituania*, núm. 36662/04, 31 de julio de 2012, §§ 56, 58, 61. La revelación de las conversaciones del demandante con sus socios de negocios en el marco de los procedimientos de la Corte Constitucional había estado en conformidad con la ley.

⁷⁵ TEDH, Caso *Kruslin vs. Francia*, núm. 11801/85, 24 de abril de 1990.

⁷⁶ TEDH, Caso *Kruslin vs. Francia*, núm. 11801/85, 24 de abril de 1990, § 36.

⁷⁷ TEDH, Caso *Klaas vs. Alemania*, núm. 5029/71, 6 de septiembre de 1978.

amenazas, debe ser capaz de llevar a cabo la vigilancia secreta de elementos subversivos que operan dentro de su jurisdicción”.⁷⁸ No obstante, el Tribunal, “siendo consciente del peligro, inherente en las medidas de vigilancia secreta, de debilitar o incluso destruir la democracia con la justificación de defenderla, afirma que los Estados contratantes no podrán, en nombre de la lucha contra el espionaje y el terrorismo, adoptar cualquier medida que consideren apropiada”.⁷⁹ Sin embargo, respecto al caso concreto, el Tribunal no encontró ninguna violación del artículo 8 de la CEDH, dado que la ley impugnada por los demandantes, y que prevenía restricciones respecto al secreto de la correspondencia, correos y telecomunicaciones fue considerada por el TEDH como necesaria en una sociedad democrática.⁸⁰ Asimismo, en *Uzun vs. Alemania*,⁸¹ el Tribunal llegó a la conclusión de que la vigilancia de la demandante a través de GPS ordenada por el Fiscal General con los objetivos de investigar varios cargos de intento de asesinato atribuidos a un movimiento terrorista y de prevenir nuevos atentados con explosivos, servía a los intereses de la seguridad nacional y pública, la prevención del delito y la protección de los derechos de las víctimas. En conclusión, la interferencia fue proporcional frente a los fines legítimos perseguidos, y por lo tanto, “necesaria en una sociedad democrática” en el sentido del artículo 8(2) de la CEDH.⁸²

c. Vigilancia clandestina por los servicios secretos

Respecto a la vigilancia secreta por los servicios secretos de los Estados, en *Asociación “21 de diciembre 1989” y otros vs. Rumania*⁸³ el TEDH encontró una violación del artículo 8 por la ausencia de garantías suficientes en el derecho interno que impidieran que la información recopilada en 1990 por los servicios de inteligencia sobre el demandante se mantuvieran aún 16 años después.⁸⁴ De igual manera, el TEDH consideró que, ante la falta

⁷⁸ TEDH, Caso *Klaas vs. Alemania*, núm. 5029/71, 6 de septiembre de 1978, § 42.

⁷⁹ TEDH, Caso *Klaas vs. Alemania*, núm. 5029/71, 6 de septiembre de 1978, § 49.

⁸⁰ TEDH, Caso *Klaas vs. Alemania*, núm. 5029/71, 6 de septiembre de 1978, §§ 56-60.

⁸¹ TEDH, Caso *Uzun vs. Alemania*, núm. 35623/05, 2 de septiembre de 2010.

⁸² TEDH, Caso *Uzun vs. Alemania*, núm. 35623/05, 2 de septiembre de 2010, § 80.

⁸³ TEDH, Caso *Asociación “21 de diciembre 1989” y otros vs. Rumania*, núms. 33810/07 y 18817/08, 24 de mayo de 2011, en el cual el presidente de una asociación para la defensa de los derechos de los participantes de las manifestaciones contra el gobierno en Rumania en 1989, fue objeto de medidas de vigilancia de los servicios secretos.

⁸⁴ TEDH, Caso *Asociación “21 de diciembre 1989” y otros vs. Rumania*, núms. 33810/07 y 18817/08, 24 de mayo de 2011, § 121.

de garantías en la legislación nacional, el demandante corría el grave riesgo de que sus llamadas telefónicas pudieran ser interceptadas.⁸⁵ En dicha sentencia, el Tribunal se refirió a la sentencia de la Gran Cámara en *Rotaru vs. Rumania*,⁸⁶ en la cual la Gran Cámara ya había establecido que el sistema rumano de recopilar y archivar información de manera secreta no establecía las garantías necesarias para la protección de la vida privada de los individuos.⁸⁷ Posteriormente, el Comité de Ministros del Consejo de Europa había emitido una resolución provisional pidiendo que se remediara las carencias normativas, pero tal resolución aún no se había implementado al momento de la sentencia en el caso *Asociación “21 de diciembre 1989”*. Además, el Tribunal estableció en *Dumitru Popescu vs. Rumania*,⁸⁸ que a pesar de varias enmiendas legislativas posteriores al Código de Procedimiento Penal, todavía era posible la vigilancia secreta y la adopción de medidas de control en caso de una supuesta amenaza a la seguridad nacional.⁸⁹ En un caso similar respecto al almacenamiento de información en una base de datos de los servicios secretos, el TEDH determinó en *Shimovolos vs. Rusia* una violación del artículo 8o., argumentando que la base de datos se había creado apoyándose en una decisión ministerial, que no había sido pública ni accesible al público.⁹⁰ No se podía saber por qué las personas estaban registradas en tal base, ni qué tipo de información se incluía, ni por cuánto tiempo, ni cómo se almacenaba. La información se utilizaba por las autoridades estatales que tenían el control sobre la base de datos.⁹¹

d. Garantías necesarias para la legalidad de interceptaciones

De la citada jurisprudencia, el TEDH ha desarrollado una serie de garantías para frenar el riesgo de abuso por interceptaciones telefónicas u otras medidas de vigilancia. Estas medidas se pueden dividir según los requisitos relativos a la base jurídica para la autorización de las escuchas telefónicas y las protecciones que aplican para la fase en la que la interceptación de las

⁸⁵ TEDH, Caso Asociación “21 de diciembre 1989” y otros vs. Rumania, núms. 33810/07 y 18817/08, 24 de mayo de 2011, § 122.

⁸⁶ TEDH, Caso Rotaru vs. Rumania [GC], núm. 28341/95, 4 de mayo de 2000.

⁸⁷ TEDH, Caso Rotaru vs. Rumania [GC], núm. 28341/95, 4 de mayo de 2000, § 43.

⁸⁸ TEDH, Caso Dumitru Popescu vs. Rumania (núm. 2), núm. 71525/01, 26 de abril de 2007.

⁸⁹ TEDH, Caso Dumitru Popescu vs. Rumania (núm. 2), núm. 71525/01, 26 de abril de 2007, § 84.

⁹⁰ TEDH, Caso Shimovolos vs. Rusia, núm. 30194/09, 21 de junio de 2011, § 69.

⁹¹ TEDH, Caso Shimovolos vs. Rusia, núm. 30194/09, 21 de junio de 2011, § 69.

comunicaciones se lleva a cabo. Para la autorización de las interceptaciones telefónicas u otras medidas de vigilancia tiene que existir una base legal para la interceptación de las comunicaciones. Esta base tiene que ser accesible al público y especificar la naturaleza de los delitos que dan lugar a una orden de inicio, la categoría de las personas que puedan tener su teléfono intervenido, un límite en la duración de las escuchas telefónicas o medidas de vigilancia, el procedimiento que debe seguirse para el examen de la legalidad de la medida, el uso y el almacenamiento de los datos obtenidos y las circunstancias bajo las cuales pueden o se deben borrar las grabaciones o cintas. Debe haber precauciones para proteger la comunicación privilegiada en la relación abogado-cliente. Las protecciones en relación con la forma en que una interceptación se lleva a cabo tienen que ser mecanismos de control eficaces para garantizar que la ley se cumpla. La supervisión tiene que estar en concordancia con los principios democráticos generalmente aceptados (en conformidad con la ley, fin legítimo y necesidad de la medida en una sociedad democrática) y tiene que ser llevado a cabo por una autoridad independiente de la que lleva a cabo la medida.

C. *Vigilancia electrónica en el ámbito laboral*

Las actividades profesionales o empresariales no están excluidas del ámbito de protección del derecho a la vida privada.⁹² Por lo tanto, la realización de llamadas telefónicas o el uso de otros medios de comunicación, como Internet, desde la oficina o el lugar de trabajo están protegidos en principio por el derecho a la vida privada según el artículo 8o. de la CEDH. Los correos electrónicos enviados desde el trabajo deben ser protegidos de la misma manera que la información derivada del monitoreo del uso personal de Internet.⁹³ En *Copland vs. Reino Unido*⁹⁴ el TEDH encontró una violación del artículo 8o.,⁹⁵ considerando en primer lugar que las llamadas telefónicas y correos enviados desde el colegio son abarcados por las expresiones “vida pri-

⁹² TEDH, Caso *Niemietz vs. Alemania*, núm. 13710/88, 16 de diciembre de 1992, § 29; TEDH, Caso *Halford vs. Reino Unido*, núm. 20605/92, 25 de junio de 1997, § 42.

⁹³ TEDH, Caso *Copland vs. Reino Unido*, núm. 62617/00, 3 de abril de 2007, § 30.

⁹⁴ TEDH, Caso *Copland vs. Reino Unido*, núm. 62617/00, 3 de abril de 2007, el demandante que era empleado de un colegio de educación pública administrado por el Estado, fue sometido a una vigilancia de su teléfono, correo electrónico y uso de Internet por iniciativa del director adjunto del colegio, con el objetivo de determinar si el demandante estaba haciendo un uso excesivo de las instalaciones del colegio para fines personales.

⁹⁵ TEDH, Caso *Copland vs. Reino Unido*, núm. 62617/00, 3 de abril de 2007, § 49.

vada” y “correspondencia”, y por lo tanto, protegidos como la información derivada del uso personal de Internet.⁹⁶ En segundo lugar, la recopilación y almacenamiento de datos personales en relación con el uso del teléfono, el correo electrónico e Internet, sin conocimiento del demandante, constituyó una injerencia en la vida privada y la confidencialidad de la correspondencia.⁹⁷ En tercer lugar, si bien el TEDH dejó abierta la cuestión de si la vigilancia del teléfono, correo electrónico o Internet de una persona en el lugar de trabajo puede ser considerado “necesaria en una sociedad democrática” en ciertas situaciones, cuando constituyen un objetivo legítimo. El Tribunal llegó a la conclusión que, en ausencia de cualquier supervisión reguladora en la legislación nacional en el momento de los hechos, la interferencia no era “de conformidad con la ley”.⁹⁸ Por otro lado, en *Köpke vs. Alemania*,⁹⁹ la demandante era una cajera que fue despedida sin previo aviso por hurto después de haber sido detectada mediante una acción de vigilancia de video encubierta llevada a cabo por su empleador con la ayuda de una agencia de detectives privados. Köpke alegó una violación del artículo 8o. de la CEDH por haber sido declarado legal el despido por los tribunales laborales. El TEDH rechazó la demanda como inadmisibles por ser manifiestamente infundada, llegando a la conclusión que las autoridades nacionales habían logrado un equilibrio justo entre el derecho de la empleada a que se respete su vida privada y el interés de su empleador en la protección de sus derechos a la propiedad y el interés público en la administración de justicia.¹⁰⁰

3. *El uso de Internet y otros medios de comunicación de masas, el derecho a la vida privada y su relación con otros derechos humanos*

A. *El uso de Internet como medio de comunicación y obligaciones de restricción estatal para garantizar el derecho a la vida privada de terceros*

Respecto al uso de Internet el TEDH ha tratado casos en los cuales los demandantes alegaron la violación de su derecho a la vida privada por la

⁹⁶ TEDH, Caso Copland vs. Reino Unido, núm. 62617/00, 3 de abril de 2007, § 41.

⁹⁷ TEDH, Caso Copland vs. Reino Unido, núm. 62617/00, 3 de abril de 2007, § 44.

⁹⁸ TEDH, Caso Copland vs. Reino Unido, núm. 62617/00, 3 de abril de 2007, § 48.

⁹⁹ TEDH, Caso Köpke vs. Alemania, núm. 420/07, 5 de octubre de 2010.

¹⁰⁰ Sin embargo, el TEDH expresó que los intereses en conflicto podrían ser balanceados de manera diferente en el futuro, teniendo en cuenta el grado de interferencia en la vida privada de nuevas y cada vez más sofisticadas tecnologías.

presunta omisión estatal de controlar tal uso. En *Muscio vs. Italia*,¹⁰¹ sobre el envío de correos electrónicos no solicitados (*spam*) con carácter obsceno al demandante por desconocidos y la decisión de las autoridades de no adoptar medidas después de la queja por el demandante por considerarlas inútiles, el TEDH declaró inadmisibles las demandas por ser manifiestamente infundadas. El Tribunal argumentó que si bien la recepción de mensajes no deseados constituye una injerencia en el derecho al respeto de la vida privada, una vez conectados a Internet, los usuarios de correos electrónicos se exponen voluntariamente a situaciones de riesgo de recibir mensajes no deseados, respecto a las cuales las autoridades nacionales y los proveedores de servicios de Internet enfrentan dificultades objetivas en la lucha contra el *spam*. Por tanto, el TEDH concluyó que el Estado no había violado sus obligaciones positivas de garantizar la protección de la vida privada del demandante al momento de utilizar Internet. En sentido similar, en *Benediktsdottir vs. Islandia*,¹⁰² el TEDH declaró inadmisibles las demandas respecto a la alegada protección insuficiente de la vida privada del demandante debido a la publicación ilegal de sus correos electrónicos privados en los medios de comunicación por terceros. Lo anterior dado que, para el TEDH las autoridades estatales en Islandia no habían fallado en encontrar un justo equilibrio entre la protección de la libertad de expresión y el derecho del demandante al respeto de su vida privada y su correspondencia en virtud del artículo 8o. de la CEDH.

Por otro lado, en *K.U. vs. Finlandia* respecto a un anuncio de carácter sexual publicado sobre un niño de 12 años de edad en un sitio de citas por Internet, del cual conforme a la legislación finlandesa, la policía y los tribunales judiciales no podían exigir al proveedor de Internet la identificación de la persona que había publicado el anuncio, el Tribunal consideró que se había producido una violación del artículo 8o. de la CEDH. Según el criterio del TEDH, la publicación del anuncio constituía un acto criminal por involucrar un menor de edad como objetivo para pedófilos, por lo que la legislatura debía haber proporcionado un marco para la conciliación de la confidencialidad de los servicios de Internet con la prevención de las infracciones penales y la protección de los derechos y libertades de los demás, y en particular los niños y otras personas vulnerables.¹⁰³ Siguiendo esta lógica, en *Perrin vs. Reino Unido*,¹⁰⁴ el TEDH declaró inadmisibles las demandas

¹⁰¹ TEDH, Caso *Muscio vs. Italia*, núm. 31358/03, 13 de noviembre de 2007.

¹⁰² TEDH, Caso *Benediktsdottir vs. Islandia*, núm. 38079/06, 16 de junio de 2009.

¹⁰³ TEDH, Caso *K.U. vs. Finlandia*, núm. 2872/02, 2 de diciembre de 2008, § 49.

¹⁰⁴ TEDH, Caso *Perrin vs. Reino Unido*, núm. 5446/03, 18 de octubre de 2005.

mente infundada una demanda dirigida contra una sentencia condenatoria de un ciudadano francés en el Reino Unido por publicar artículos obscenos por Internet. El Tribunal rechazó la demanda, basada en el artículo 10 (libertad de expresión) de la Convención, reconociendo que la condena penal podía ser considerada necesaria en una sociedad democrática en interés de la protección de la moral y de los derechos de los demás.

B. El uso de otros medios de comunicación de masas a la luz de la relación entre el derecho a la vida privada, la libertad y la libertad de expresión

Además de estos casos relacionados con el uso de Internet como medio de comunicación, el TEDH se ha pronunciado sobre la relación entre el derecho a la protección de la vida privada frente a la libertad de expresión, consagrada en el artículo 10 de la CEDH, en contextos del uso de medios de comunicación de masas.¹⁰⁵

En *von Hannover vs. Alemania No. 2*, la Gran Sala del TEDH señaló que “la imagen de una persona constituye uno de los principales atributos de su personalidad, ya que revela las características particulares de la persona y distingue a la persona de otros. El derecho a la protección de la imagen de uno es, por lo tanto, uno de los componentes esenciales del desarrollo personal. Supone, sobre todo, el derecho del individuo a controlar el uso de esa imagen, incluyendo el derecho a rechazar la publicación de la misma”.¹⁰⁶ Respecto a la relación entre la libertad de expresión y el derecho a la imagen precisó que “la libertad de expresión incluye la publicación de fotos... Esta es, sin embargo, un área en la que la protección de los derechos y la reputación de los demás adquiere una especial importancia, ya que las fotos

¹⁰⁵ El artículo 10 de la CEDH estipula al respecto: “1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa. 2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial”.

¹⁰⁶ TEDH, *Caso von Hannover vs. Alemania* (núm. 2) [GC], núms. 40660/08 y 60641/08, 7 de febrero de 2012, § 96.

pueden contener información muy personal o íntima de una persona o de su familia”.¹⁰⁷

a) Principios generales

En cuanto a la ponderación entre los derechos a la vida privada y la protección de datos con el derecho a la libertad de expresión, el TEDH ha dictado varias sentencias históricas. La libertad de expresión constituye una base esencial de una sociedad democrática.¹⁰⁸ Limitaciones a este derecho, previstas en el artículo 10(2) de la CEDH, tienen que ser interpretadas estrictamente. La interferencia de los Estados en el ejercicio de esa libertad es posible, siempre y cuando, como en el caso del derecho a la vida privada, se trate de la persecución de un fin legítimo, que la medida esté “prevista por la ley” y que sea “necesaria en una sociedad democrática”, es decir, que debe corresponder a una “necesidad social imperiosa”, constituyendo una medida proporcionada frente al objetivo legítimo que se persigue. Si bien las autoridades nacionales disponen de un cierto margen de apreciación, éste no es ilimitado.¹⁰⁹

En *Editorial Board of Pravoye Delo and Shtekel vs. Ucrania*, el TEDH señaló que el artículo 10 de la CEDH impone a los Estados no sólo una obligación negativa de no limitar de manera injustificada la libertad de expresión, sino también una obligación positiva para crear un marco normativo adecuado para garantizar la protección efectiva de la libertad de expresión de los periodistas, particularmente, en Internet.¹¹⁰ En ese caso, los demandantes habían sido condenados a pagar por los daños y perjuicios producidos por la publicación de un texto anónimo y difamatorio que descargaron de Internet, a pesar de que el texto iba acompañado por una nota editorial que indicaba la fuente y que los periodistas se distanciaban del texto.¹¹¹ También fueron obligados a publicar una retractación y una disculpa, a pesar de que

¹⁰⁷ TEDH, Caso von Hannover *vs.* Alemania (núm. 2) [GC], Nos. 40660/08 y 60641/08, 7 de febrero de 2012, § 103.

¹⁰⁸ TEDH, Caso Handyside *vs.* Reino Unido, núm. 5493/72, 7 de diciembre de 1976, § 49.

¹⁰⁹ TEDH, Caso Aleksey Ovchinnikov *vs.* Rusia, núm. 24061/04, 16 de diciembre de 2010, § 51.

¹¹⁰ TEDH, Caso Editorial Board of Pravoye Delo and Shtekel *vs.* Ucrania, núm. 33014/05, 5 de mayo de 2011, § 64.

¹¹¹ TEDH, Caso Editorial Board of Pravoye Delo and Shtekel *vs.* Ucrania, núm. 33014/05, 5 de mayo de 2011, § 9.

esta última no estaba prevista por la ley.¹¹² Examinando el caso en virtud del artículo 10 de la Convención, el TEDH consideró que la injerencia a través del fallo contra los periodistas no se había “establecido por la ley”, requisito exigido por el artículo 10(2) de la CEDH, ya que en ese momento, la legislación de Ucrania no preveía un marco legal de protección para periodistas en caso de reproducir textos o noticias en Internet.¹¹³ Además, los tribunales nacionales se habían negado a aplicar para tales situaciones las disposiciones que protegían a los periodistas de los medios impresos en situaciones similares.¹¹⁴ Respecto a la violación del artículo 10 debido a la falta de garantías adecuadas para los periodistas que utilizan la información obtenida a través de Internet, el TEDH, resaltando la importancia de proteger de manera adecuada a los periodistas cuando utilizan Internet como medio de comunicación, señaló que “teniendo en cuenta el papel que desempeña Internet en el contexto de las actividades profesionales de los medios... y su importancia para el ejercicio del derecho a la libertad de expresión en general..., la ausencia de un marco legal suficiente a nivel nacional permitiendo que los periodistas utilicen la información obtenida a través de Internet sin temor a incurrir en sanciones, obstaculiza gravemente el ejercicio de la función vital de la prensa como un ‘perro guardián’”.¹¹⁵

El artículo 10(2) de la CEDH deja poco espacio para la restricción de la libertad de expresión cuando se trata del discurso político o de asuntos de interés público. Si bien requiere que una persona, cuando participa en un debate público sobre una cuestión de interés general, no sobrepase ciertos límites respecto a los derechos de los demás, sí se le permite recurrir a un cierto grado de exageración, provocación, o el uso de declaraciones inmoderadas. En el caso de *Sürek vs. Turquía*, el TEDH declaró con respecto al discurso político:

Los límites de la crítica admisible son más amplios con respecto al gobierno que en relación a un ciudadano privado o incluso a un político. En un sistema democrático las acciones u omisiones del gobierno deben estar sujetas al escrutinio no sólo de las autoridades legislativas y judiciales, sino también de la

¹¹² TEDH, Caso Editorial Board of Pravoye Delo and Shtekel vs. Ucrania, núm. 33014/05, 5 de mayo de 2011, §§ 54-59.

¹¹³ TEDH, Caso Editorial Board of Pravoye Delo and Shtekel vs. Ucrania, núm. 33014/05, 5 de mayo de 2011, § 66.

¹¹⁴ TEDH, Caso Editorial Board of Pravoye Delo and Shtekel vs. Ucrania, núm. 33014/05, 5 de mayo de 2011, § 56.

¹¹⁵ TEDH, Caso Editorial Board of Pravoye Delo and Shtekel vs. Ucrania, núm. 33014/05, 5 de mayo de 2011, § 64; véase también TEDH, Caso Aleksey Ovchinnikov vs. Rusia, núm. 24061/04, 16 de diciembre de 2010, § 41.

opinión pública. Por otra parte, la posición dominante que ocupa el gobierno hace que sea necesario, para que se muestre moderación en el recurso a un procedimiento penal, sobre todo cuando otros medios están disponibles para responder a los ataques y críticas injustificados de sus adversarios. No obstante, sigue abierta a las autoridades estatales competentes para adoptar, en su calidad de garantes del orden público, medidas, incluso de carácter penal, la intención de una respuesta adecuada y sin excesos de tales comentarios... Por último, cuando tales comentarios incitan a la violencia [sic] contra un individuo o un funcionario público o un sector de la población, las autoridades del Estado gozan de un mayor margen de apreciación al examinar la necesidad de una injerencia en la libertad de expresión.¹¹⁶

La crítica y la sátira están protegidas por el artículo 10 de la CEDH, dado que dicho artículo incluye “información” o “ideas” que ofendan, resulten chocantes o perturben al Estado o a cualquier sector de la población. Según el TEDH, la crítica y la sátira forman parte de las demandas de pluralismo, la tolerancia y la apertura mental, sin las cuales no existe una “sociedad democrática”.¹¹⁷ Sin embargo, es importante distinguir entre la crítica y el insulto. Particularmente, un discurso de odio no se encuentra protegido por el artículo 10 de la CEDH, y, en virtud del artículo 17 de la CEDH, es incompatible con los valores proclamados y garantizados por la Convención.¹¹⁸ Por ejemplo, *Willem vs. Francia* se refería al llamado público a un boicot por parte de un alcalde contra productos israelíes a través de la página-web del municipio, declarado posteriormente culpable por los tribunales franceses de provocar discriminación. El TEDH no encontró una violación del artículo 10 de la CEDH, considerando que las razones dadas por los tribunales para justificar la interferencia en la libertad de expresión del demandante habían sido “pertinentes y suficientes”.¹¹⁹ Además, el Tribunal consideró que la multa impuesta al demandante había sido relativamente moderada y proporcional frente al objetivo perseguido.¹²⁰ En sentido contrario, en *Renaud vs. Francia* el Tribunal consideró que se había producido una violación del artículo 10 dado que la condena del demandante por haber difamado e insultado a un alcalde francés mediante la página-web de la

¹¹⁶ TEDH, Caso *Sürek vs. Turquía*, núm. 26682/95, 8 de julio de 1999, § 61.

¹¹⁷ TEDH, Caso *Müller vs. Suiza*, núm. 41202/98, 5 de noviembre de 2002, §§ 32-35; TEDH, Caso *Handyside vs. Reino Unido*, núm. 5493/72, 7 de diciembre de 1976, § 49; también TEDH, Caso *Perrin vs. Reino Unido*, núm. 5446/03, 18 de octubre de 2005.

¹¹⁸ TEDH, Caso *Gündüz vs. Turquía*, núm. 35071/97, 4 de diciembre de 2003, § 41.

¹¹⁹ TEDH, Caso *Willem vs. Francia*, núm. 10883/05, 16 de julio de 2009, § 40.

¹²⁰ TEDH, Caso *Willem vs. Francia*, núm. 10883/05, 16 de julio de 2009, § 41.

asociación de la que era presidente y editor, había sido desproporcionada en relación con el fin legítimo perseguido.¹²¹

En conclusión, el Artículo 10 no garantiza la libertad de expresión de manera ilimitada, sobre todo cuando la información publicada por la prensa con una intención difamatoria o sin perseguir un interés público tiene graves repercusiones en la reputación y los derechos de terceros. Sin embargo, cuando las autoridades nacionales impiden la publicación o imponen sanciones por difamación deben dar una explicación suficiente de sus razones y sustentar debidamente sus motivos, para demostrar la existencia de una “necesidad social imperiosa” para la sanción u orden de retractación.¹²² Para justificar una sentencia que declara que alguien ha cometido difamación en Internet, los tribunales nacionales deben dar razones pertinentes y suficientes que el Tribunal tendrá que verificar.

Por otro lado, si bien las autoridades nacionales deben respetar el derecho de los periodistas a difundir información sobre cuestiones de interés general, incluso si éstos recurren a un cierto grado de exageración o provocación. La protección de los periodistas está sujeta a la condición de que actúen de buena fe y proporcionen información fiable y precisa de acuerdo con el periodismo responsable.¹²³ El TEDH ha aplicado estos principios generales a los casos de publicaciones por Internet, considerando que

...en vista de su accesibilidad y su capacidad para almacenar y comunicar grandes cantidades de información, Internet juega un papel importante en la mejora del acceso del público a las noticias y la divulgación de información general. El mantenimiento de archivos de Internet es un aspecto crítico de este papel y, por tanto, la Corte considera que esos archivos están comprendidos en el ámbito de la protección del artículo 10.¹²⁴

¹²¹ TEDH, Caso *Renaud vs. Francia*, núm. 13290/07, 25 de febrero de 2010; § 43; véase también United Nations Human Rights Council, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”, § 27, A/HRC/17/27, 16 de mayo de 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (“For example, in cases of defamation of individuals reputation, given the ability of the individual concerned to exercise his/her right of reply instantly to restore the harm caused, the types of sanctions that are applied to offline defamation may be unnecessary or disproportionate”).

¹²² TEDH, Caso *Fatullayev vs. Azerbaiyán*, núm. 40984/07, 22 de abril de 2010, § 100.

¹²³ TEDH, Caso *Stoll vs. Suiza*, [GC] núm. 69698/01, 10 de diciembre de 2007, § 104.

¹²⁴ TEDH, Caso *Times Newspapers Ltd vs. Reino Unido* (núm. 1 y 2), núms. 3002/03 y 23676/03, 10 de marzo de 2009, § 27.

Respecto a la justificación de la interferencia en la libertad de expresión para la protección de la intimidad de terceros el TEDH ha distinguido entre personas públicas o políticas y personas privadas. Las primeras gozan de una protección menor en la medida que son sujetos del debate público o la vida pública y, por lo tanto, objetos de un mayor escrutinio o interés público, mientras que las personas privadas, por ser particularmente vulnerables, merecen una protección especial.

b. Derecho a la libertad de expresión y protección de la vida privada de personas públicas o políticas

En *von Hannover vs. Alemania*, la demandante, la princesa Carolina von Hannover, había solicitado a los tribunales alemanes que se impidiera cualquier publicación en revistas alemanas de dos series de fotografías relativas a su vida privada, por considerar violado su derecho a la vida privada y su propia imagen. Finalmente, mediante decisiones del Tribunal Federal de Justicia y del Tribunal Constitucional Federal se rechazaron las pretensiones de la demandante. Ante el TEDH alegó que estas decisiones habían vulnerado su derecho al respeto de su vida privada, ya que no se le había garantizado protección adecuada contra la publicación de las fotografías tomadas sin su conocimiento con el argumento de que era por excelencia una figura de la sociedad contemporánea.¹²⁵ El Tribunal consideró que había una violación del artículo 8o. (derecho al respeto de la vida privada) de la CEDH, dado que los tribunales alemanes no habían logrado, en el caso concreto, un equilibrio justo entre los intereses en juego.¹²⁶ El Tribunal observó en particular que si bien el público en general puede tener un derecho a la información, incluyendo en circunstancias especiales, respecto a la vida privada de personajes públicos, no existía tal derecho en este caso.¹²⁷ El TEDH consideró que el público en general no tenía un interés legítimo en recibir información sobre el paradero de la demandante o de cómo se comportaba generalmente en su vida privada, aunque ella apareciera en lugares conocidos por el público.¹²⁸ A juicio del TEDH, el interés comercial de las revistas alemanas por publicar las fotografías y artículos, tenía que ceder ante el

¹²⁵ TEDH, Caso von Hannover *vs.* Alemania, núm. 59320/00, 24 de junio de 2004, § 25.

¹²⁶ TEDH, Caso von Hannover *vs.* Alemania, núm. 59320/00, 24 de junio de 2004, § 79.

¹²⁷ TEDH, Caso von Hannover *vs.* Alemania, núm. 59320/00, 24 de junio de 2004, §§ 76-78.

¹²⁸ TEDH, Caso von Hannover *vs.* Alemania, núm. 59320/00, 24 de junio de 2004, § 77.

derecho de la demandante a la protección efectiva de su vida privada.¹²⁹ Según el Tribunal, todas las personas, incluidas las personas conocidas por el público, tienen una expectativa legítima a la protección de su vida privada.¹³⁰ Para el TEDH, los criterios establecidos por los tribunales alemanes para distinguir una persona pública por excelencia no eran adecuados para garantizar la protección efectiva de la vida privada de la demandante.¹³¹

Posteriormente, en *von Hannover contra Alemania (No. 2)*¹³² el Tribunal negó la violación del artículo 8o. de la Convención, señalando en particular que los tribunales alemanes habían balanceado cuidadosamente el derecho de las empresas editoriales a la libertad de expresión frente al derecho de los solicitantes al respeto de su vida privada. Al hacerlo, el Tribunal concedió importancia fundamental a la cuestión de si las fotografías y los artículos que las acompañaban, contribuyeron a un debate de interés general. También examinó las circunstancias en que se tomaron las fotografías. El Tribunal Federal de Justicia había cambiado su enfoque a raíz de la primera sentencia *von Hannover* del Tribunal Europeo en 2004 (véase más arriba), mientras que, el Tribunal Constitucional Federal no sólo confirmó ese nuevo enfoque, sino que llevó a cabo un análisis detallado del caso a la luz de la jurisprudencia y los criterios del TEDH.¹³³

Finalmente, en *von Hannover vs. Alemania (No. 3)*,¹³⁴ el TEDH sostuvo que no hubo una violación del artículo 8 de la CEDH, puesto que los tribunales alemanes habían tenido en cuenta los criterios esenciales y la jurisprudencia del Tribunal en el equilibrio de los distintos intereses en juego en el caso. Observó en particular que no podía afirmarse que el artículo en cuestión no había sido más que un pretexto para la publicación de la fotografía en cues-

¹²⁹ TEDH, Caso *von Hannover vs. Alemania*, núm. 59320/00, 24 de junio de 2004, § 77.

¹³⁰ TEDH, Caso *von Hannover vs. Alemania*, núm. 59320/00, 24 de junio de 2004, § 73.

¹³¹ TEDH, Caso *von Hannover vs. Alemania*, núm. 59320/00, 24 de junio de 2004, §§ 72-75.

¹³² TEDH, Caso *von Hannover vs. Alemania* (núm. 2) [GC], núms. 40660/08 y 60641/08, 7 de febrero de 2012. En este caso, los demandantes, la princesa Carolina von Hannover y su esposo, el príncipe Ernst August von Hannover, se quejaron de la negativa de los tribunales alemanes para prohibir cualquier publicación ulterior de dos fotografías que habían sido tomadas durante sus vacaciones sin su conocimiento y que habían aparecido en dos revistas alemanas. Alegaron en particular que los tribunales nacionales no habían tenido suficiente en cuenta la sentencia del Tribunal de 2004 en *von Hannover contra Alemania*.

¹³³ TEDH, Caso *von Hannover vs. Alemania* (núm. 2) [GC], núms. 40660/08 y 60641/08, 7 de febrero de 2012, § 125.

¹³⁴ TEDH, Caso *von Hannover* (núm. 3) *vs. Alemania*, núm. 8772/10, 19 de septiembre de 2013, que se refirió a una denuncia presentada por la princesa Carolina von Hannover en relación con la negativa de los tribunales alemanes de prohibir la publicación de una fotografía de ella y su marido, tomada sin su conocimiento, mientras estaban de vacaciones.

tión o que la conexión entre el artículo y la fotografía había sido puramente artificial. La caracterización por primera vez del tema del artículo como un acontecimiento de interés general, por parte de la Corte Constitucional Federal y luego por el Tribunal Federal de Justicia, no puede considerarse irrazonable. Por consiguiente, el Tribunal podía aceptar que la fotografía en cuestión había hecho una contribución a un debate de interés general.

En *Schüssel vs. Austria*¹³⁵ el TEDH declaró inadmisibles las demandas por ser manifiestamente infundadas, considerando que el Tribunal Supremo de Austria había ponderado correctamente el interés general en un debate político abierto, protegido por el artículo 10 (libertad de expresión) de la Convención contra el interés del solicitante en la protección contra la publicación de su fotografía.¹³⁶ Expresó que los límites de la crítica aceptable eran más amplios con respecto a un político que con respecto a un particular. En un sentido similar, en *Minelli vs. Suiza*,¹³⁷ el Tribunal declaró inadmisibles las demandas por ser manifiestamente infundadas, compartiendo el criterio de la Corte Federal de Suiza, según el cual el demandante no podía reclamar la protección absoluta de su derecho a la intimidad después de haberse expuesto al escrutinio público. En *Axel Springer AG vs. Alemania*, el TEDH sostuvo que la prohibición impuesta por un tribunal nacional sobre el propietario de un periódico que quería publicar un artículo sobre la detención y condena de un conocido actor violó el artículo 10 de la CEDH. El Tribunal reiteró los criterios que había establecido en su jurisprudencia al equilibrar el derecho a la libertad de expresión contra el derecho al respeto de la vida privada. Consideró en primer lugar, si el artículo publicado era de interés público, la detención y condena de una persona era un hecho judicial público y, por lo tanto, de interés público; en segundo lugar, si la persona en cuestión era una figura pública, la persona en cuestión era un actor bastante conocido para calificar como una figura pública; en tercer lugar, cómo se obtuvo la información y si era fiable, la información había sido proporcionada por la oficina del fiscal y la exactitud de la información conteni-

¹³⁵ TEDH, Caso *Schüssel vs. Austria*, núm. 42409/98, 21 de febrero de 2002; el demandante, siendo el vice primer ministro de Austria, se quejó en particular sobre el uso público de su imagen, medio solapada por la cara del político de derecha Jörg Haider con el siguiente lema: “Los cortadores de la seguridad social y los ladrones de la educación comparten una cara común”.

¹³⁶ TEDH, Caso *Schüssel vs. Austria*, núm. 42409/98, 21 de febrero de 2002.

¹³⁷ TEDH, Caso *Minelli vs. Suiza*, núm. 14991/02, 14 de junio de 2005. En este caso, el demandante, un abogado y periodista públicamente conocido por su frecuente participación en los debates públicos sobre temas de actualidad, alegó una violación de su privacidad debido a la utilización del término “cazador furtivo” en un artículo sobre su persona publicado en una revista. También se quejó de la publicación de su fotografía junto con el artículo.

da en ambas publicaciones no estaba en disputa entre las partes; en cuarto lugar, el contenido, la forma y las consecuencias del artículo, el artículo no contenía información infundada, y en quinto lugar la proporcionalidad de la sanción impuesta.¹³⁸ Tomando en consideración estos criterios, el TEDH dictaminó que las restricciones impuestas a la empresa demandante no habían sido razonablemente proporcionales frente al fin legítimo de proteger la vida privada de un tercero.¹³⁹ En *Mosley vs. Reino Unido*¹⁴⁰ el TEDH señaló en particular que el CEDH no requiere que los medios de comunicación den aviso previo de las publicaciones planeadas.¹⁴¹

c. Derecho a la libertad de expresión y protección de la vida privada de personas vulnerables

En la jurisprudencia del TEDH, uno de los criterios cruciales relativos a la ponderación de estos derechos es si la expresión en cuestión contribuye a un debate de interés público. Por ejemplo, en *Biriuk vs. Lituania*, la parte demandante solicitó una indemnización de un periódico porque había publicado un artículo de que era VIH positivo. Esa información supuestamente había sido confirmada por los médicos en el hospital local. El TEDH no consideró el artículo en cuestión como una contribución a un debate de interés público y reiteró que la protección de los datos personales, incluyendo datos médicos, eran de importancia fundamental para el disfrute del derecho al respeto de la vida privada y familiar garantizado por el artículo 8o. de la CEDH.¹⁴² El Tribunal concedió especial importancia al hecho de que, según el informe en el periódico, el personal médico de un hospital había proporcionado información sobre la infección por el VIH en violación evidente de su obligación de secreto médico.¹⁴³

¹³⁸ TEDH, Caso Axel Springer AG vs. Alemania [GC], núm. 39954/08, 7 de febrero de 2012, §§ 96-109.

¹³⁹ TEDH, Caso Axel Springer AG vs. Alemania [GC], núm. 39954/08, 7 de febrero de 2012, § 110.

¹⁴⁰ TEDH, Caso Mosley vs. Reino Unido, núm. 48009/08, 10 de mayo de 2011, que se refirió a la publicación de artículos, imágenes y vídeos en un periódico y en su página web sobre las actividades sexuales del demandante, que se quejó de que las autoridades no habían establecido una obligación para el periódico de notificarle con antelación a la publicación del material, para que pudiera solicitar un mandamiento judicial provisional. Al respecto, el Tribunal consideró que no había habido una violación del artículo 8o. de la CEDH.

¹⁴¹ TEDH, Caso Mosley vs. Reino Unido, núm. 48009/08, 10 de mayo de 2011, § 132.

¹⁴² TEDH, Caso Biriuk vs. Lituania, núm. 23373/03, 25 de febrero de 2008, § 42.

¹⁴³ TEDH, Caso Biriuk vs. Lituania, núm. 23373/03, 25 de febrero de 2008, § 43.

d. La publicación de imágenes e información de personas bajo investigación penal

La ponderación entre la libertad de prensa y el derecho a la vida privada es de especial importancia en el contexto de la publicación de información e imágenes de personas bajo investigación penal. El TEDH ha encontrado una violación del derecho a la vida privada de personas investigadas en varios casos. En *Sciacca vs. Italia*, después de una rueda de prensa ofrecida por el Ministerio Público respecto a una investigación contra el demandante por irregularidades en la gestión de la escuela donde enseñaba, evasión fiscal y falsificación, dos periódicos publicaron artículos sobre los hechos, junto con una fotografía del demandante. Esta fotografía, publicada en varias ocasiones, había sido tomada por la Policía y presentada a la prensa. Al respecto, el Tribunal consideró una violación del artículo 8o. de la CEDH por la entrega de la fotografía por la policía.¹⁴⁴ Además, no había una ley que reglamentara la toma de fotografías de personas bajo sospecha y la entrega de fotos a la prensa.¹⁴⁵ Por ello, el Tribunal consideró que la injerencia en el derecho a la vida privada del demandante no había ocurrido “en concordancia con la ley”.¹⁴⁶ Una situación similar se presentó en *Khuzhin y otros vs. Rusia*.¹⁴⁷ El Tribunal encontró en las circunstancias concretas una violación del artículo 8o. de la CEDH por la entrega de la foto de una persona sospechosa de un delito a la prensa, por la falta de un fin legítimo según el artículo 8o.(2) de la CEDH.¹⁴⁸ En *Toma vs. Rumania*,¹⁴⁹ el Tribunal consideró

¹⁴⁴ TEDH, Caso *Sciacca vs. Italia*, núm. 50774/99, 11 de enero de 2005, § 31.

¹⁴⁵ TEDH, Caso *Sciacca vs. Italia*, núm. 50774/99, 11 de enero de 2005, § 30.

¹⁴⁶ TEDH, Caso *Sciacca vs. Italia*, núm. 50774/99, 11 de enero de 2005, § 30.

¹⁴⁷ TEDH, Caso *Khuzhin y otros vs. Rusia*, núm. 13470/02, 23 de octubre de 2008, en el cual un miembro de la policía entregó a un periodista antes del inicio del juicio penal la foto de uno de los procesados sin su consentimiento, la cual fue utilizada en un programa de televisión.

¹⁴⁸ TEDH, Caso *Khuzhin y otros vs. Rusia*, núm. 13470/02, 23 de octubre de 2008, § 117; por un lado, el demandante se encontraba detenido en el momento de los hechos pues no era un fugitivo de la justicia, la exhibición de su fotografía no era necesaria para obtener el apoyo del público para determinar su paradero. Por otro lado, tampoco podría decirse que se había reforzado el carácter público de los procedimientos judiciales, dado que en el momento de la grabación y la primera emisión del programa de televisión el juicio aún no había comenzado.

¹⁴⁹ TEDH, Caso *Toma vs. Rumania*, núm. 42716/02, 24 de febrero de 2009. En este caso, la policía había llamado a los periodistas y les había permitido tomar fotografías del demandante bajo custodia policial después de haber sido detenido por posesión de 800 gramos de cannabis. Al día siguiente, una fotografía del demandante fue publicada en la primera página de un periódico, junto con un artículo llamándolo “narcotraficante”.

como una violación del derecho a la vida privada el comportamiento de la policía de llamar a periodistas y permitirles filmar al demandante en la estación de policía sin su consentimiento y con el fin de publicar las imágenes en los medios de comunicación.¹⁵⁰ El TEDH argumentó que el Estado rumano no había ofrecido ninguna justificación para tal injerencia, y tampoco nada que sugiriera que la difusión de las imágenes, sin valor informativo alguno, hubiera servido a los intereses de la justicia.¹⁵¹ Posteriormente, el Tribunal no encontró una violación del artículo 10 de la CEDH en *Egeland y Hanseid vs. Noruega* por la condena de dos periodistas a una multa tras haber publicado fotografías de una persona saliendo de la audiencia de juicio donde había sido condenada a prisión por un triple homicidio. El TEDH argumentó que aunque las fotografías habían afectado un acto público y se habían tomado en un lugar público en un momento en que la identidad de la persona ya era conocida por el público, el Tribunal consideró que su publicación había sido particularmente intrusiva.¹⁵² Por otra parte, el interesado no había dado su consentimiento de que las fotografías fueran tomadas o publicadas, y el hecho de que había cooperado con la prensa en ocasiones anteriores no podía justificar privarle de la protección de su imagen en esas circunstancias.¹⁵³ Además, las multas impuestas a los demandantes no habían sido particularmente graves.¹⁵⁴

C. *El uso de Internet y la protección del derecho a la propiedad intelectual*

Finalmente, el uso de Internet juega una gran importancia en el contexto de la protección del derecho a la propiedad intelectual.¹⁵⁵ Aun así, la

¹⁵⁰ TEDH, Caso Toma *vs.* Rumania, núm. 42716/02, 24 de febrero de 2009, § 91.

¹⁵¹ TEDH, Caso Toma *vs.* Rumania, núm. 42716/02, 24 de febrero de 2009, § 92.

¹⁵² TEDH, Caso Egeland y Hanseid *vs.* Noruega, núm. 34438/04, 16 de abril de 2009, § 61.

¹⁵³ TEDH, Caso Egeland y Hanseid *vs.* Noruega, núm. 34438/04, 16 de abril de 2009, § 62.

¹⁵⁴ TEDH, Caso Egeland y Hanseid *vs.* Noruega, núm. 34438/04, 16 de abril de 2009, § 64.

¹⁵⁵ En el convenio sobre la creación de la Organización Mundial de la Propiedad Intelectual de 1967 se enumeran los derechos contemplados en la noción de la propiedad intelectual: las obras literarias y artísticas, performances, invenciones, descubrimientos científicos, diseños industriales, marcas comerciales, marcas de servicio, nombres comerciales, etc. No sólo son protegidas las ideas, sino también la forma real en la que esas derivan. Los autores de estas obras tienen por un lado un derecho moral (el derecho a comunicar la obra, lo cual implica que un tercero debe obtener una autorización para usar o reproducir la obra) y, por otro lado, un derecho económico de sacar provecho de la obra (por ejemplo por el

jurisprudencia del Tribunal Europeo de Derechos Humanos en este ámbito es relativamente escasa. En *Paeffgen GmbH vs. Alemania*,¹⁵⁶ el TEDH declaró inadmisibles las demandas de la empresa demandante, basada en el artículo 1o. (protección de la propiedad) del Protocolo núm. 1 de la CEDH, considerando que las órdenes dirigidas a la empresa demandante en la sentencia para la cancelación de las direcciones electrónicas registradas constituían una limitación proporcional ante las exigencias del interés general de evitar que la empresa siguiera violando los derechos de marca de terceros. En *Ashby Donald y otros vs. Francia*,¹⁵⁷ el Tribunal sostuvo que no había habido violación del derecho a la libertad de expresión de los fotógrafos, dado que ante las circunstancias del caso, en particular el amplio margen de apreciación para las autoridades nacionales y la naturaleza y tipo de penas impuestas, la injerencia en cuestión no era desproporcionada frente al fin perseguido.¹⁵⁸ Finalmente, en *Neij y Sunde Kolmisoppi vs. Suecia*,¹⁵⁹ el Tribunal declaró inadmisibles las demandas por ser manifiestamente infundadas. Si bien compartir, o permitir que otros compartan los archivos de tipo *torrent* en Internet, incluso material protegido por el copyright y con fines de lucro, está cubierta por el derecho de “recibir y difundir información” en virtud de la libertad de expresión. El TEDH estableció que los tribunales nacionales, al imponer las sanciones correspondientes, habían respetado el balance justo entre los derechos en conflicto, es decir, el derecho de los demandantes de recibir y difundir información y la necesidad de proteger los derechos de autor, que prevalecía en ese caso.

rendimiento, la reproducción o la venta). En el ámbito de la tecnología de información, el *software* es un ejemplo de la propiedad intelectual, al igual que cualquier otro trabajo (artículos, imágenes, sonidos, entre otros) creado por una computadora. Un artículo, como por ejemplo un libro, distribuido a través de Internet puede ser también intrínsecamente sujeto a la protección.

¹⁵⁶ TEDH, Caso *Paeffgen GmbH vs. Alemania*, núms. 25379/04, 21688/05, 21722/05 y 21770/05, 18 de septiembre de 2007, que se refería a una sentencia contra la empresa demandante, según la cual el registro y uso de determinadas direcciones de Internet violaban los derechos de marca de varias empresas y particulares.

¹⁵⁷ TEDH, Caso *Ashby Donald y otros vs. Francia*, núm. 36769/08, 10 de enero de 2013, relacionado con la condena de fotógrafos de moda por la infracción de derechos de autor a raíz de la publicación en Internet de fotos tomadas en desfiles de moda sin la autorización debida.

¹⁵⁸ TEDH, Caso *Ashby Donald y otros vs. Francia*, núm. 36769/08, 10 de enero de 2013, § 44.

¹⁵⁹ TEDH, Caso *Neij y Sunde Kolmisoppi vs. Suecia*, núm. 40397/12, 19 de febrero de 2013, relacionado con la demanda presentada por dos co-fundadores de “The Pirate Bay” (uno de los sitios web más grandes del mundo para compartir archivos *torrent*), contra su condena por complicidad para cometer delitos en violación de la Ley de Propiedad Intelectual.

VII. CONCLUSIONES

El TEDH ha producido una amplia y detallada jurisprudencia respecto al uso de las TIC, la protección de datos y el respeto del derecho a la vida privada y otros derechos relacionados, tanto en la esfera pública frente a entidades públicas como en el ámbito privado entre particulares. Basándose en el criterio de la “conformidad con la ley”, el Tribunal demanda de los Estados un suficiente grado de precisión y previsibilidad respecto a sus leyes reguladoras de la protección de datos personales. Por otro lado, mediante los criterios del “fin legítimo” y de la “medida necesaria en una sociedad democrática” otorga un marco de diseño de políticas públicas y la respectiva reglamentación jurídica, suficientemente amplio a las instituciones estatales para resolver las tensiones entre la protección de los datos y otros fines, como la protección de intereses estatales o los derechos de terceros. La adecuada ponderación entre los derechos en conflicto en materia de la regulación de las TIC requiere un comportamiento responsable de las instituciones estatales, que, como lo ha señalado el TEDH, implica que las técnicas científicas modernas en una sociedad tecnológicamente avanzada no pueden utilizarse a cualquier costo y sin equilibrar cuidadosamente los beneficios potenciales del uso extensivo de tales técnicas frente a los derechos humanos consagrados internacionalmente.

VIII. BIBLIOGRAFÍA

- ARENAS Ramiro, M., “La protección de datos personales en los países de la Unión Europea”, 16 *Revista Jurídica de Castilla y León* (2008), 113-168.
- BOEHM, F., *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-Level*, Springer, Berlín Heidelberg, 2012.
- CONVENIO EUROPEO PARA LA PROTECCIÓN DE LOS DERECHOS HUMANOS Y DE LAS LIBERTADES FUNDAMENTALES (E.T.S. 5; 213 U.N.T.S. 221).
- CONVENIO NÚM. 108 PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL (E.T.S. 108; 4 E.C.A. 264; 1496 U.N.T.S. 66).
- CONVENIO QUE ESTABLECE LA ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL, 14 de julio de 1967.
- DIRECTIVA 95/46/CE (24 de octubre de 1995) del Parlamento Europeo y del Consejo, relativa a la Protección de las Personas Físicas en lo que res-

pecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos.

DIRECTIVA 97/66/CE (15 de diciembre de 1997), del Parlamento Europeo y del Consejo, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el sector de las Telecomunicaciones.

DIRECTIVA 2002/58/CE (12 de julio de 2002), del Parlamento Europeo y del Consejo, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el sector de las Comunicaciones Electrónicas.

DIRECTIVA 2006/24/CE (15 de marzo de 2006), del Parlamento Europeo y del Consejo, relativa a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

EUROPEAN COURT OF HUMAN RIGHTS, Internet: Case-law of the European Court of Human Rights, Council of Europe, 2011.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHT, Handbook on European Data Protection Law, Council of Europe, 2014.

KORFF, D., EC study on implementation of data protection Directive (Study Contract ETD/2001/B5-3001/A/49) Human Rights Centre, Essex, Cambridge, 2002

REGLAMENTO (CE) NÚM. 45/2001 (18 de diciembre de 2001), del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, y a la libre circulación de esos datos.

SCHWARTZ, P., “European Data Protection Law and Restrictions on International Data Flows”, 80 *Iowa L. Rev.* (1994-95), 471-496.

IX. ANEXOS DE JURISPRUDENCIA DEL TEDH

TEDH, Caso A. *vs.* Francia, núm. 14838/89, 23 de noviembre de 1993.

TEDH, Caso Airey *vs.* Irlanda, núm. 6289/73, 9 de octubre de 1979.

TEDH, Caso Aleksey Ovchinnikov *vs.* Rusia, núm. 24061/04, 16 de diciembre de 2010.

TEDH, Caso Amann *vs.* Suiza [GC], núm. 27798/95, 16 de febrero de 2000.

TEDH, Caso Ashby Donald y otros *vs.* Francia, núm. 36769/08, 10 de enero de 2013.

- TEDH, Caso Asociación “21 de diciembre 1989” y otros *vs.* Rumania, Nos. 33810/07 y 18817/08, 24 de mayo de 2011.
- TEDH, Caso August *vs.* Reino Unido, núm. 36505/02, 21 de enero de 2003.
- TEDH, Caso Axel Springer AG *vs.* Alemania [GC], núm. 39954/08, 7 de febrero de 2012.
- TEDH, Casos B.B. *vs.* Francia, núm. 5335/06, 17 de diciembre de 2009.
- TEDH, Caso Benediktsdottir *vs.* Islandia, núm. 38079/06, 16 de junio de 2009.
- TEDH, Caso Biriuk *vs.* Lituania, núm. 23373/03, 25 de febrero de 2009.
- TEDH, Caso Bista *vs.* Polonia, núm. 22807/07, 12 de enero de 2010.
- TEDH, Caso Campbell *vs.* Reino Unido, núm. 13590/88, 25 de marzo de 1992.
- TEDH, Caso Copland *vs.* Reino Unido, núm. 62617/00, 3 de abril de 2007.
- TEDH, Caso Cotlet *vs.* Rumania, núm. 38565/97, 3 de junio de 2003.
- TEDH, Caso Draksas *vs.* Lituania, núm. 36662/04, 31 de julio de 2012.
- TEDH, Caso Dumitru Popescu *vs.* Rumania (núm. 2), núm. 71525/01, 26 de abril de 2007.
- TEDH, Caso Editorial Board of Pravoye Delo and Shtekel *vs.* Ucrania, núm. 33014/05, 5 de mayo de 2011.
- TEDH, Caso Fatullayev *vs.* Azerbaiyán, núm. 40984/07, 22 de abril de 2010.
- TEDH, Caso Gardel *vs.* Francia, núm. 16428/05, 17 de diciembre de 2009.
- TEDH, Caso Golder *vs.* Reino Unido, núm. 4451/70, 21 de febrero de 1975.
- TEDH, Caso Gündüz *vs.* Turquía, núm. 35071/97, 4 de diciembre de 2003.
- TEDH, Caso Halford *vs.* Reino Unido, núm. 20605/92, 25 de junio de 1997.
- TEDH, Caso Handyside *vs.* Reino Unido, núm. 5493/72, 7 de diciembre de 1976.
- TEDH, Caso Iordachi y otros *vs.* Moldavia, núm. 25198/02, 10 de febrero de 2009.
- TEDH, Caso Khan *vs.* Reino Unido, núm. 6222/10, 20 de diciembre de 2011.
- TEDH, Caso Khelili *vs.* Suiza, núm. 16188/07, 18 de octubre de 2011.
- TEDH, Caso Khuzhin y otros *vs.* Rusia, núm. 13470/02, 23 de octubre de 2008.
- TEDH, Caso Klaas *vs.* Alemania, núm. 5029/71, 6 de septiembre de 1978.
- TEDH, Caso Köpke *vs.* Alemania, núm. 420/07, 5 de octubre de 2010.
- TEDH, Caso Kopp *vs.* Suiza, núm. 23224/94, 25 de marzo de 1998.

- TEDH, Caso *Kruslin vs. Francia*, núm. 11801/85, 24 de abril de 1990.
- TEDH, Caso *K.U. vs. Finlandia*, núm. 2872/02, 2 de diciembre de 2008.
- TEDH, Caso *Leander vs. Suecia*, núm. 9248/81, 26 de marzo de 1987.
- TEDH, Caso *Malone vs. Reino Unido*, núm. 8691/79, 2 de agosto de 1984.
- TEDH, Caso *Matwiejczuk vs. Polonia*, núm. 37641/97, 2 de diciembre de 2003.
- TEDH, Caso *M.B. vs. Francia*, núm. 22115/06, 17 de diciembre de 2009.
- TEDH, Caso *M.C. vs. Bulgaria*, núm. 39272/98, 4 de diciembre de 2003.
- TEDH, Caso *Minelli vs. Suiza*, núm. 14991/02, 14 de junio de 2005.
- TEDH, Caso *M.K. vs. Francia*, núm. 19522/09, 18 de abril de 2013.
- TEDH, Caso *Mosley vs. Reino Unido*, núm. 48009/08, 10 de mayo de 2011.
- TEDH, Caso *Muscio vs. Italia*, núm. 31358/03, 13 de noviembre de 2007.
- TEDH, Caso *Neij y Sunde Kolmisoppi vs. Suecia*, núm. 40397/12, 19 de febrero de 2013.
- TEDH, Caso *Niemietz vs. Alemania*, núm. 13710/88, 16 de diciembre de 1992.
- TEDH, Caso *Paeffgen GmbH vs. Alemania*, núms. 25379/04, 21688/05, 21722/05 y 21770/05, 18 de septiembre de 2007.
- TEDH, Caso *Peck vs. Reino Unido*, núm. 44647/98, 28 de enero de 2003.
- TEDH, Caso *Perrin vs. Reino Unido*, núm. 5446/03, 18 de octubre de 2005.
- TEDH, Caso *Peruzzo y Martens vs. Alemania*, núms. 7841/08 y 57900/12, 4 de junio de 2013.
- TEDH, Caso *P.G. y J.H. vs. Reino Unido*, núm. 44787/98, 25 de septiembre de 2001.
- TEDH, Caso *Pisk-Piskowski vs. Polonia*, núm. 92/03, 14 de junio de 2005.
- TEDH, Caso *Przyjemski vs. Polonia*, núm. 6820/07, 5 de octubre de 2010.
- TEDH, Caso *Renaud vs. Francia*, núm. 13290/07, 25 de febrero de 2010.
- TEDH, Caso *Rotaru vs. Rumania [GC]*, núm. 28341/95, 4 de mayo de 2000.
- TEDH, Caso *S. y Marper vs. Reino Unido [GC]*, núms. 30562/04 y 30566/04, 4 de diciembre de 2008.
- TEDH, Caso *Schüssel vs. Austria*, núm. 42409/98, 21 de febrero de 2002.
- TEDH, Caso *Sciacca vs. Italia*, núm. 50774/99, 11 de enero de 2005.
- TEDH, Caso *Shimovolos vs. Rusia*, núm. 30194/09, 21 de junio de 2011.
- TEDH, Caso *Silver y otros vs. Reino Unido*, núms. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 y 7113/75, 25 de marzo de 1983.

- TEDH, Caso *Stoll vs. Suiza* [GC], núm. 69698/01, 10 de diciembre de 2007.
- TEDH, Caso *Sürek vs. Turquía* [GC], núm. 26682/95, 8 de julio de 1999.
- TEDH, Caso *Taylor-Sabori vs. Reino Unido*, núm. 47114/99, 22 de enero de 2003.
- TEDH, Caso *The Sunday Times vs. Reino Unido*, núm. 6538/74, 26 de abril de 1979.
- TEDH, Caso *Times Newspapers Ltd vs. Reino Unido* (núms. 1 y 2), Nos. 3002/03 y 23676/03, 10 de marzo de 2009.
- TEDH, Caso *Toma vs. Rumania*, núm. 42716/02, 24 de febrero de 2009.
- TEDH, Caso *Uzun vs. Alemania*, núm. 35623/05, 2 de septiembre de 2010.
- TEDH, Caso *Vetter vs. Francia*, núm. 59842/00, 31 de mayo de 2005.
- TEDH, Caso *von Hannover vs. Alemania*, núm. 59320/00, 24 de junio de 2004.
- TEDH, Caso *von Hannover vs. Alemania* (núm. 2) [GC], núms. 40660/08 y 60641/08, 7 de febrero de 2012.
- TEDH, Caso *von Hannover* (núm. 3) *vs. Alemania*, núm. 8772/10, 19 de septiembre de 2013.
- TEDH, Caso *Willem vs. Francia*, núm. 10883/05, 16 de julio de 2009.
- TEDH, Caso *Wisse vs. Francia*, núm. 71611/01, 20 de diciembre de 2005.
- TEDH, Caso *X y Y vs. Países Bajos*, núm. 8978/80, 26 de marzo de 1985.

EL EJERCICIO DE LOS DERECHOS ARCO ANTE EL FLUJO TRANSFRONTERIZO DE INFORMACIÓN BIOMÉTRICA*

Vanessa DÍAZ**

SUMARIO: I. *Introducción*. II. *Información biométrica y su protección jurídica*. III. *Despliegue de sistemas biométricos en un Estado constitucional*. IV. *El ejercicio de los derechos ARCO ante el flujo transfronterizo de información biométrica*. V. *Conclusiones*. VI. *Bibliografía*.

I. INTRODUCCIÓN

Las Tecnologías de la Información y Comunicación (TIC) están revolucionando la forma en la obtención, procesamiento y generación de datos. Uno de los avances más importantes de las TIC ha sido la capacidad de recopilar, almacenar, procesar e intercambiar información biométrica, facilitando el flujo de datos biométricos no sólo a nivel nacional sino también internacional.

Si bien existen grandes ventajas tecnológicas impulsadas por esta revolución digital, lo cierto es que la implementación de la tecnología biométrica genera una serie de retos, desafíos y problemas jurídicos que deben explorarse en su totalidad.

Nuestro estudio se centra en el pleno ejercicio de los derechos de acceso, rectificación, cancelación y oposición, también llamados derechos ARCO, en el flujo transfronterizo de la información biométrica. Para ello, analiza-

* Este artículo forma parte del proyecto de investigación de tesis doctoral sobre *Trans-border Biometric Information Flow: Legal Challenges to Personal Privacy and the Need for Public Debate*. Realizado con becas del Consejo Nacional de Ciencia y Tecnología (Conacyt), el Instituto de Ciencia y Tecnología del Distrito Federal y el apoyo del Institute for the Study of Social Change de la Universidad de Tasmania.

** Académica del Instituto de Investigaciones Jurídicas de la UNAM y University Associate de la Facultad de Derecho de la Universidad de Tasmania.

remos los sistemas biométricos regionales existentes: en Europa, el Sistema de Información de Schengen (SIS) y EURODAC; y, en el foro Asia-Pacífico de Cooperación Económica (APEC), la Tarjeta de Viajes de Negocios de APEC.

Ante la falta de acuerdo internacional sobre la implementación de sistemas biométricos, la investigación revela que la comunidad internacional utiliza los acuerdos internacionales y las leyes nacionales en materia de protección de datos personales para regular el flujo transfronterizo de información biométrica. Sin embargo, las diferencias normativas en materia de protección de datos personales hacen suponer la existencia de lagunas jurídicas para el efectivo ejercicio de los derechos ARCO en las diferentes jurisdicciones a nivel internacional.

Este artículo se encuentra dividido en cinco secciones; en la primera se introduce el objeto de estudio, en la segunda se establece la información biométrica como bien jurídico tutelado por los derechos de la privacidad y protección de datos personales, en la tercera se aborda el despliegue de sistemas biométricos, en la cuarta se analizan los sistemas biométricos regionales de Europa y en el foro Asia-Pacífico de Cooperación Económica (APEC), con el objetivo de identificar el ejercicio de los derechos ARCO ante el flujo de información biométrica y, finalmente, en la quinta se desarrollan las conclusiones.

II. INFORMACIÓN BIOMÉTRICA Y SU PROTECCIÓN JURÍDICA

No existe una definición unívoca sobre el término biometría o biométrico en sentido estricto. La doctrina se divide al clasificarla como ciencia o técnica;¹ sin embargo, desde una perspectiva científica² la definición de la

¹ Al analizar la literatura especializada de la materia, ésta se puede clasificar en dos grupos. En el primer grupo se ubican aquellas obras que consideran a la biometría como “técnica” que a través de la estadística auxilia a diferentes ciencias para resolver problemas. *Cfr.* King, Robert C. y William D., Stansfield, *A Dictionary of Genetics*, 5a. ed., Oxford University Press, 1997. *Cfr.* Sokal, Robert y James, Rohlf, *Biometry*, 3a. ed., W.H. Freeman, 2003. *Cfr.* Sokal, Robert y James, Rohlf, *Introduction to Biostatistics*, W.H. Freeman, 1973. *Cfr.* Zhang, David D., *Automated Biometrics Technologies and Systems*, Kluwer Academic Publishers, 2000.

² Mientras que en el segundo grupo encontramos autores que consideran a la biometría como “ciencia”. *Cfr.* Hopkins, Richard, “An Introduction to Biometrics and Large Scale Civilian Identification”, *International Review of Law, Computers & Technology*, núm. 13, s. v., pp. 337-363; *Cfr.* Mather, Kenneth y Jinks, John L., *Biometrical Genetics. The Study of Continuous Variation*, Cornell University Press, 1971.

biometría se desarrolla a través de la estadística o la informática. Mientras que quienes la explican cómo técnica o método la abordan desde diferentes campos de la ciencia: biología, agronomía, medicina, etcétera. Sin embargo, actualmente la biometría es utilizada como método estadístico de adquisición de conocimiento, y a través de la observación y la experimentación describe los fenómenos naturales; no obstante, no logra explicar los fenómenos de la naturaleza por sí misma.³

Por tanto, el término “biometría” hace referencia a las técnicas y sistemas automatizados de identificación (reconocimiento) y/o verificación (autenticación) de los individuos con base en características específicas, únicas e intransferibles. Es así como se puede establecer la definición de datos biométricos como: *todas aquellas características fisiológicas y morfológicas que nos identifican como individuos únicos*. Cabe señalar que, dentro de las características físicas se encuentran el reconocimiento del iris, de la mano, de las huellas dactilares, del rostro, entre otras. Mientras que en las características de comportamiento se encuentran el reconocimiento de la voz, caminar, firmar, teclear, etcétera.

Ahora bien, existen autores, como Begoña Martínez Jarreta, que consideran a estas características también como inalterables;⁴ no obstante, nosotros no compartimos esa percepción de las características biométricas. Ya que existen algunos datos biométricos que pueden ser alterados por el solo transcurso del tiempo o bien por enfermedades, es el caso del glaucoma, enfermedad del ojo que incrementa la presión intraocular impactando directamente el iris.

Es importante destacar que la información biométrica es el resultado directo de las diferencias individuales que existen en el desarrollo anatómico del cuerpo. La información biométrica ha sido asociada a las técnicas de identificación y verificación que se utilizan para incrementar los sistemas de seguridad.⁵

Por ende, la definición normativa de información personal deberá estar conformada por aquellos datos o referencias que dan cuenta no sólo de la vida de un sujeto, es decir, que informan sobre sus transacciones financieras; su situación familiar o estado civil; su solvencia económica o manejo credi-

³ Cfr. Hopkins, Richard, “An Introduction to Biometrics and Large Scale Civilian Identification”, *op. cit.*, *supra* nota 2.

⁴ Cfr. Martínez Jarreta, Begoña, “Biometría (técnico)”, en Romero Casabona, Carlos María (dir.), *Enciclopedia de Bioderecho y Bioética*, España, Comares, Fundación BBVA, Instituto Roche, Universidad del País Vasco, Universidad de Deusto, 2013, pp. 257-261.

⁵ Díaz, Vanessa, “Sistemas biométricos en material criminal: un estudio comparado”, *IUS Revista del Instituto de Ciencias Jurídicas de Puebla*, núm. 31, vol. VII, pp. 28-47.

ticio; sus creencias religiosas, políticas; su estado de salud; las ocasiones que ha tenido acceso a alguna institución de salud; los seguros médicos o de vida que ha adquirido; los títulos académicos; las preferencias sexuales; el rango salarial; incluso el historial de antecedentes penales o administrativos, sino también de características fisiológicas y morfológicas.

Ahora bien, la información personal, designada como datos personales o información nominativa, es aquella que revela la identidad de la persona, como los datos biométricos.⁶ Por la trascendencia de la información biométrica, un manejo inadecuado o bien una excesiva revelación de cierto dato biométrico, sin que medie la autorización expresa del interesado, da lugar a la violación de la privacidad, y desde luego podría generar estigmatización y, en consecuencia, discriminación.⁷

Aunque no todas las características fisiológicas y morfológicas por sí mismas son datos biométricos “sensibles”. En algunos casos, los sistemas biométricos de reconocimiento o de autenticación podrían necesitar dos o más datos biométricos.⁸ A lo anterior se le denomina sistemas de combinación biométrica; ejemplos: el tipo de sangre, el factor RH, el peso, la estatura, la distancia entre la nariz y los ojos.⁹

Por tanto, se desprende que, según el diseño de los sistemas biométricos, éstos pueden o no revelar mucha o poca información personal. La clasificación de datos biométricos como “sensibles” estará determinada por las circunstancias específicas. Sin embargo, compartir datos biométricos con el objetivo de identificar y verificar a los individuos es información personal sensible.

El derecho de protección de datos personales busca preservar la confidencialidad, en este caso de la información biométrica, tanto en la recopilación, manejo como transmisión. Es decir, el titular de dicha información biométrica debe mantener el control de lo que sobre su persona se ha recabado y lo que se almacena en las bases de datos automatizadas, dando paso con ello al reconocimiento del derecho que se tiene de acceso y control de dicha información personal.

⁶ Muñoz de Alba Medrano, Marcia, “El acceso a la información personal en el nuevo marco jurídico mexicano”, en Villanueva, Ernesto y Luna Pla, Issa (eds.), *Derecho de acceso a la información pública, Valoraciones iniciales*, México, UNAM, Atlatl, USAID, Konrad Adenauer, 2005, p. 204.

⁷ *Idem*.

⁸ Díaz, Vanessa, “Sistemas biométricos en material criminal: un estudio comparado”, *op. cit.*, nota 5, p. 34.

⁹ *Idem*.

Lo anterior ha obligado no sólo al reconocimiento del derecho de acceso a los datos personales, sino también a la sistematización de la información personal; no obstante, la precisión de dicha regulación no siempre ha sido la adecuada.¹⁰

III. DESPLIEGUE DE SISTEMAS BIOMÉTRICOS

A nivel nacional, la recolección, el almacenamiento y procesamiento de datos biométricos deben ser considerados cuidadosamente al crear bases de datos. Generalmente, los países deben considerar que la creación de bases biométricas son excepciones o limitaciones al derecho de la privacidad y protección de datos personales de los individuos cuyos datos están contenidos en estas bases de datos. Además, debe garantizarse el pleno ejercicio de los derechos de acceso, rectificación, cancelación y oposición de procesar la información biométrica. La implementación de sistemas biométricos debe equilibrar y conciliar, por un lado, los intereses individuales tales como los derechos humanos y libertades públicas, y, por el otro, los intereses públicos, como la defensa y seguridad pública.

En este sentido, cabe señalar que los sistemas biométricos solamente tienen dos objetivos: la identificación (reconocimiento) y la verificación (autenticación) de los individuos sobre la base de algunas características fisiológicas o morfológicas. El primero es para identificar, es decir, reconocer al individuo, por lo que su funcionamiento está basado en utilizar un dato y compararlo con una lista o base de datos, el ejemplo más común son las bases criminales. El segundo es para verificar, es decir, autenticar la identidad del individuo, por lo que su funcionamiento está basado en la utilización de un dato comparándolo con el mismo dato almacenado previamente, el ejemplo son las bases migratorias.¹¹

Así, se debe considerar que para el desarrollo de sistemas biométricos es fundamental distinguir su objetivo. Es decir, el sistema biométrico va a ser utilizado para identificar o para verificar; puesto que el reconocimiento

¹⁰ Bien señala Marcia Muñoz que el acceso a la información personal en el marco jurídico mexicano es incipiente y deja amplios espacios de interpretación y falta de respuesta jurídica en esta materia. Cfr. Muñoz de Alba Medrano, Marcia, “El acceso a la información personal en el nuevo marco jurídico mexicano”, en Villanueva, Ernesto y Luna Pla, Issa (eds.), *Derecho de acceso a la información pública, Valoraciones iniciales*, México, *op. cit.*, *supra* nota 6, p. 214.

¹¹ Díaz, Vanessa, “Sistemas biométricos en material criminal: un estudio comparado”, *op. cit.*, nota 5, p. 29.

y la autenticación son actividades totalmente diferentes y para ello algunas características fisiológicas son más apropiadas para la identificación y otras son más útiles para la verificación.¹²

Un ejemplo donde se combinan objetivos de identificación y verificación de individuos a nivel internacional son las políticas migratorias a nivel regional. Globalmente, es casi imposible alcanzar políticas migratorias uniformes y heterogéneas debido a la amplia gama de intereses económicos, sociales y culturales relacionados con inmigración en todo el mundo. Sin embargo, la armonización de las políticas migratorias sobre bases regionales es cada vez más común. En el contexto europeo, el Sistema de Información de Schengen (SIS II) y el sistema EURODAC son ejemplos de políticas de visados comunes armonizadas, en las cuales una visa es válida en cualquier país de la zona Schengen y puede ser emitida por un país para viajar a otro de la misma zona. En el contexto de Asia-Pacífico, la APEC ha creado una tarjeta de negocios llamada ABTC que facilita la entrada a corto plazo a los países miembros participantes. Estas políticas de visados comunes de la región se han desarrollado debido a la confluencia de intereses que estos países tienen en el movimiento de los migrantes a través de sus regiones.

Ahora bien, no existe un tratado o convención internacional que verse sobre la información biométrica como tal, y por ende a nivel internacional su protección recae en documentos internacionales sobre privacidad y protección de datos personales. A nivel nacional, generalmente la regulación recae en las leyes sobre privacidad y datos personales que contemplan la sistematización de la información, pero también el flujo de información nacional e internacional.

A nivel internacional sólo existen los estándares desarrollados por la Organización de Aviación Civil Internacional (OACI) para la elaboración de pasaportes, visas y credenciales o documentos de identidad.¹³ En cuestiones criminales o prevención del delito se encuentran los estándares desarrollados por Interpol, el Instituto Nacional Estadounidense de Estándares (ANSI, por sus acrónimos en inglés), el Instituto Nacional de Estándares y Tecnología (NIST, por sus acrónimos en inglés), por mencionar algunos.

¹² Cfr. Boulgouris, Nikolaos V. *et al.*, *Biometrics, Theory, Methods, and Applications*, IEEE y Wiley, 2010; Bolle, Ruud M. *et al.*, *Guide to Biometrics*, Springer, 2003. Cfr. Zhang, David D., *Automated Biometrics Technologies and Systems*, *op. cit.*, nota 1.

¹³ En este mismo sentido se han desarrollado los: ISO/IEC 19794-5:2005, Information Technology. Biometric Data Interchange Formats. Part 5: Face Image Data- AMENDMENT 1: conditions for taking photographs for face image data (2007) y el ISO (ISO/IEC) 19794-5 Biometric Data Interchange Formats defines a standard data format for digital face images to allow interoperability among face recognition systems, government agencies, and other creators and users of face images.

Estos estándares se caracterizaban por ser disimilares y por ende no ser interoperables entre sí. No obstante, a partir de noviembre de 2011, un nuevo estándar fue elaborado.

El estándar ANSI/NIST-ITL1-2011 permite la interoperabilidad entre los distintos sistemas como bases de datos de inmigración y bases de datos criminales, así como el almacenamiento, transmisión y proceso de datos geográficos (ubicación de posiciones), las imágenes contextuales asociadas y datos de audio y visual.¹⁴

Este estándar supone un nuevo desafío a mediano plazo, ya que facilita el subsecuente uso automatizado de los datos biométricos y otros tipos de datos personales entre los diferentes organismos de diferentes ámbitos, nacional e internacional. Además, este desafío puede generar otro tipo de retos en materia de protección de datos personales, como el acceso de los datos, su fiabilidad y continuidad de protección jurídica en terceros países. Es posible que la información recopilada para su uso posterior con el nuevo estándar ANSI/NIST-ITL1-2011 puede no ser completa o actualizada. Lo anterior menoscaba el principio de calidad de los datos, en dos formas; por un lado, la recolección de los datos debe ser pertinente y no excesiva, con base en la finalidad que persigue su tratamiento y, por el otro, una vez recolectados los datos deben ser actualizados y mantenerse intactos de forma que respondan con veracidad a la situación actual del titular de los datos.

Cabe mencionar que, el nuevo estándar ANSI/NIST-ITL1-2011 contraviene no sólo el principio de calidad de los datos sino también el de proporcionalidad de los datos; la información personal ha de recolectarse para un propósito específico y sólo se utiliza para ese propósito. La mayoría de los países han incorporado este principio en su legislación nacional. Por tanto, el uso posterior de información automatizado como consecuencia del nuevo estándar violenta los principios de calidad y proporcionalidad de los datos personales.

IV. EL EJERCICIO DE LOS DERECHOS ARCO ANTE EL FLUJO TRANSFRONTERIZO DE INFORMACIÓN BIOMÉTRICA

Las principales preocupaciones ante el flujo de información biométrica son: el menoscabo a la privacidad, la divulgación de información biométri-

¹⁴ http://www.nist.gov/itl/iad/ig/ansi_standard.cfm, fecha de consulta: 26 de mayo de 2014.

ca, el uso indebido y la falta de consentimiento. Sin embargo, poco se ha discutido sobre el procedimiento o ejercicio de acceso, rectificación, cancelación y oposición de los datos –también conocidos como derechos ARCO– por parte del titular ante organismos o sistemas internacionales.

Es importante destacar que, si bien no todos los sistemas biométricos son físicamente intrusivos, todos los sistemas biométricos pueden menoscabar los derechos de privacidad y protección de datos. La intensificación y diversificación de la tecnología biométrica aumenta los problemas de privacidad a nivel nacional e internacional. Aunado a lo anterior, los avances en la capacidad de almacenamiento de la información personal y la simplificación en el flujo transfronterizo de información biométrica crea desafíos jurídicos sobre la finalidad y el posible uso indebido de información.

Por ello, es importante contar con una adecuada legislación en materia de protección de datos personales a nivel nacional que contemple la continuidad de protección jurídica del dato biométrico y garantice el eficaz ejercicio de los derechos ARCO en el flujo transfronterizo de información biométrica.

En este mismo sentido, a nivel internacional se debe contemplar la uniformidad de procedimientos para ejercer los derechos ARCO en cualquier jurisdicción. Los órganos garantes en materia de privacidad o protección de datos personales deben ser capaces de monitorear adecuadamente el flujo transfronterizo de información biométrica y facilitar el ejercicio de los derechos ARCO de los individuos, sin importar el país de residencia. En la medida de lo posible también deben supervisar la operación, gestión y administración de las bases de datos biométricas.

1. *Sistemas biométricos a nivel internacional*

Hoy en día existen muchos organismos y organizaciones internacionales con diferentes objetivos, pero con roles interrelacionados, como Europol e Interpol, que operan bases de datos criminales biométricas.¹⁵ También hay diferentes sistemas biométricos, con objetivos similares pero diferentes estructuras, que administran la información criminal para fines de migración y de prevención del delito. Esta investigación identificó en Europa dos sistemas biométricos. El primero es la base de datos biométrica EURODAC y la segunda el Sistema de Información Schengen (SIS II), ampliado por la

¹⁵ Díaz, Vanessa, “Sistemas biométricos en material criminal: un estudio comparado”, *op. cit.*, nota 5.

Convención de Prüm. Mientras que, en la zona Asia-Pacífico, se identificó la base de datos biométrica de la Tarjeta de Negocios de APEC.

Cabe mencionar que poco se ha discutido sobre la rendición de cuentas de estas organizaciones y sus sistemas de trabajo; cómo se toman y aplican las recomendaciones, o cómo se establecen las especificaciones para las bases de datos biométricos. En esta sección se examina el funcionamiento de estas bases de datos biométricas en cuanto a qué información personal se recopila y cómo se hace esto. Lo anterior tiene el objetivo de establecer cómo se ejercen los derechos ARCO a nivel internacional.

Sistema EURODAC:¹⁶ En 2000 se estableció, a través del Convenio de Dublín, el sistema EURODAC, para establecer una base de datos europea centralizada de solicitantes de asilo, refugiados y para otros nacionales europeos pero que no pertenecen a la Unión Europea y que son detenidos al cruzar ilegalmente las fronteras en territorio de la UE. Incluye la recolección biométrica de las huellas dactilares, este es un sistema biométrico de identificación (reconocimiento) de individuos.

El Sistema Automatizado de Identificación de Huellas Dactilares (AFIS por sus acrónimos en inglés) de EURODAC fue creado por la empresa Steria. Ahora bien, cada Estado miembro dispone de puntos de acceso nacionales y trabaja directamente con las administraciones nacionales. Las huellas dactilares se comparan con los datos dactiloscópicos transmitidos por otros Estados miembros que ya están almacenados en la base de datos central. Si el sistema EURODAC detecta que las huellas dactilares ya se han recogido y almacenado el solicitante de asilo es re-direccionado al Estado miembro que recolectó y almacenó la información por primera vez.

Sistema de Información de Schengen (SIS II):¹⁷ Para el funcionamiento del sistema libre de control de las fronteras entre los Estados miembros de la zona Schengen, el SIS II proporciona el sistema de apoyo principal. Contiene una “lista” de las personas que han cometido un delito, falta o está bajo observación judicial. Cabe resaltar que la zona Schengen y la Unión Europea son

¹⁶ Reglamento (CE) núm. 2725/2000 del Consejo, del 11 de diciembre de 2000, relativo a la creación del sistema “Eurodac” para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/133081_es.htm, fecha de consulta el 26 de mayo de 2014.

¹⁷ Sistema de Información Schengen, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/133020_en.htm, fecha de consulta el 26 de mayo de 2014.

dos zonas diferentes; es decir, que no todos los países miembros de la Unión Europea pertenecen a la zona Schengen. Incluye la recolección de huellas dactilares y fotografías, éste es un sistema biométrico de verificación (autenticación) de individuos.

Los Estados miembros de la zona Schengen se alimentan del sistema de información a través de las redes nacionales que están conectados a un sistema central y complementado por la Red SIRENE,¹⁸ quienes son representantes de la policía nacional y local, agencias de aduanas y el poder judicial. Este sistema fue revisado y ampliado por la Convención de Prüm.¹⁹ La compañía Steria también estuvo a cargo en la segunda generación del SIS II. Su capacidad se incrementó no sólo tecnológicamente, sino también en relación con la información recopilada, almacenada e intercambiada.

Tarjeta de Negocios del Foro de Cooperación Económica de Asia-Pacífico (APEC por sus acrónimos en inglés): con el objetivo de facilitar e incrementar la movilidad de la gente de negocios en la región se creó la tarjeta de negocios ABTC (por sus acrónimos en inglés). Con base en los lineamientos previamente acordados por los Estados miembros del foro Asia-Pacífico, esta tarjeta facilita el intercambio de información a través de un sistema en línea, con el fin de mejorar la movilidad de la gente de negocios en la región. Incluye información de huellas dactilares y rostro, este es un sistema biométrico de verificación (autenticación) de individuos. El sistema aporta información sobre los documentos de viaje (pasaportes) perdidos o robados a la base de datos de Interpol.

Los países miembros son los encargados de la expedición de la Tarjeta de Viajes de Negocios para cumplir los criterios de elegibilidad de tarjetas; estándares de servicio y las normas para fabricar la tarjeta. No se elimina la solicitud de visas al visitar los miembros de APEC. Los pasaportes se mantienen como el principal documento de viaje. El flujo transfronterizo de información biométrica incluye: tramitar el despacho de antemano; recibir la autorización; y solicitar la producción de tarjetas. En los tres sistemas biométricos la transferencia de información biométrica se encuentra encriptada y se destaca que son bases de datos centralizadas.

¹⁸ La Red SIRENE es un sistema utilizado por las autoridades policiales para el intercambio de información de acuerdo con el Convenio de Schengen a efectos de la prevención e investigación de hechos delictivos en la zona Schengen por el SIS II.

¹⁹ Ampliación del Sistema de Información Schengen por Convenio Prüm, http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/jl0005_en.htm, fecha de consulta el 26 de mayo de 2014.

2. *Establecimiento de normas de protección de privacidad y protección de datos personales*

APEC es principalmente un foro para promover la cooperación en la región Asia-Pacífico en los asuntos económicos. Esta organización regional de Asia-Pacífico ha considerado las cuestiones de privacidad en relación con la cooperación económica y ha desarrollado un marco de trabajo para los Estados miembros. El marco de privacidad de APEC no es obligatorio o vinculante para los miembros, pero puede desarrollar políticas y asesorar en cuestiones legislativas a los Estados miembros.

Cabe destacar que el marco de Privacidad de la APEC es un conjunto de documentos que brindan asesoría, la cual no es vinculante y formalmente elaboran directrices para los miembros. En 1998, la APEC consideró dentro de su agenda el tema de vida privada, cuando emitió el Plan de Acción sobre el Comercio Electrónico. Pero no fue sino hasta 2004 que la APEC elabora su Marco de Privacidad, en el que resume los principios de privacidad. Los 21 países miembros voluntariamente pueden o no implementar estos principios en su legislación nacional. En consecuencia, el marco de APEC es opcional y su aplicación no ha sido consistente entre los países miembros.²⁰

El Marco de Privacidad de la APEC considera el flujo transfronterizo de datos personales, incluso fuera de la región de APEC, a través del principio de rendición de cuentas.²¹ El Marco de Privacidad de la APEC incluye un mecanismo de notificación de la aplicación interna del Marco de Privacidad, las directrices de aplicación internacional (intercambio de información entre las economías miembros) y la cooperación transfronteriza en la investigación y aplicación de la ley. Sin embargo, en el momento de escribir esta investigación ningún informe sobre su aplicación estaba disponible.

En 2007, la APEC emitió un programa piloto para la implementación del Marco de Privacidad, llamado Pathfinder de Privacidad de Datos.²² Como resultado del Plan de Trabajo Pathfinder de Privacidad, en 2012 la

²⁰ APEC Privacy Framework (2004), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/_media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx, fecha de consulta el 6 de mayo de 2014.

²¹ El principio de la rendición de cuentas se estableció por primera vez en las directrices de la OCDE.

²² El Pathfinder fija objetivos para las empresas y agencias de privacidad.

APEC emitió el Sistema de Reglas de Privacidad Transfronteriza, que es un sistema de certificación voluntario.²³

En resumen, el Marco de Privacidad de APEC es muy escueto, muy general, típico para la implementación internacional y bastante amplio para la cooperación transfronteriza y aplicación de las leyes de privacidad. Además, el Marco de Privacidad de la APEC no es obligatorio y requiere la legislación interna para ser promulgada. Además, el Marco de Privacidad de la APEC no impone controles estrictos y garantías sobre la privacidad y protección de datos en los países miembros. Por tanto, se puede concluir que el Marco de Privacidad de APEC constituye un marco razonable de directrices, pero requiere desarrollo reglamentario o eficacia normativa a nivel nacional.

En 1981, el Consejo de Europa,²⁴ influenciado por el trabajo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), desarrolló la primera Convención europea sobre el tratamiento de datos personales y las normas de privacidad y protección de datos: el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (también conocido como Convención 108). El CE es una importante organización regional que se ocupa principalmente de los derechos humanos. La CE incluye una membresía amplia de 47 Estados de Europa, más miembros que la Unión Europea con sus 28 Estados miembros. En 2001, el CE publicó un protocolo con respecto a las agencias de privacidad y los flujos transfronterizos de datos.²⁵

El Convenio 108 fortalece los derechos del individuo sobre la protección de datos relativos a las técnicas automatizadas de procesamiento, almacenamiento e intercambio de datos de carácter personal. Sin embargo, surgieron

²³ APEC Sistema de Reglas de Privacidad Transfronteriza (2012), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/_media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx, fecha de consulta el 26 de mayo de 2014.

²⁴ Organización internacional de Estrasburgo que comprende 47 países de Europa. Fue creado para promover la democracia y proteger los derechos humanos y el Estado de derecho en Europa. Para más detalles de los instrumentos jurídicos, http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp, fecha de consulta el 26 de mayo de 2014.

²⁵ Convención para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, se abrió a la firma el 28 de enero de 1981, ETS núm. 108 (entró en vigor el 1 de octubre 1985), en su versión modificada por el Tratado de Lisboa que modifica el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, abierto a la firma el 15 de junio 1995 (que entró en vigor con posterioridad a la aceptación por todas las Partes), modificado por el Protocolo del Convenio STE núm. 108, abierto a la firma el 8 de noviembre de 2001, ETS núm. 181 (entró en vigor tras la aceptación por todas las Partes).

preocupaciones sobre las medidas de protección en las leyes nacionales en materia del flujo transfronterizo de la información personal, por lo que el CE publicó un protocolo adicional al Convenio 108, que reconoce que los comisionados de privacidad juegan un papel central en la protección eficaz de las personas en los flujos transfronterizos de los datos personales.

Tres recomendaciones son especialmente significativas en el Convenio 108. Las recomendaciones no son vinculantes, pero representan un avance significativo en un intento de crear un marco para el flujo transfronterizo de información biométrica en Europa, ya que abordan cuestiones específicas relativas a técnicas automatizadas para el almacenamiento, el uso y el intercambio de datos personales. Además, responden a las preocupaciones actuales con relación a la privacidad y los principios de protección de datos. Éstos son:

- *Recomendación Núm. R(91)10* sobre la comunicación a terceros de los datos personales en poder de los organismos públicos.²⁶ Esta recomendación reconoce las tendencias crecientes de procesamiento automático de datos, el almacenamiento y el intercambio de información personal por parte de los organismos públicos y su explotación por las ventajitas comerciales por parte del sector privado. Por tanto, esta recomendación establece principios de protección de datos (PPD) sobre medidas de seguridad, con base en el Convenio 108, los cuales se pueden implementar en la legislación nacional.
- *Recomendación CM/Rec(2010)13* sobre la protección de las personas en relación con el tratamiento automatizado de los datos personales en el contexto de la creación de perfiles.²⁷ Esta Recomendación establece 13 condiciones para la recopilación y tratamiento de los datos personales, los derechos de los titulares de los datos, recursos, seguridad de datos y de las autoridades de supervisión. Sin embargo, las excepciones y restricciones limitando la privacidad individual son muy amplias. Estas excepciones son: la seguridad, la seguridad pública, los intereses monetarios del Estado o de la prevención y represión de infracciones penales.

²⁶ Recomendación R (91) 10 del Comité de Ministros a los Estados miembros sobre la comunicación a terceras personas de datos de carácter personal en poder de organismos públicos, adoptada el 9 de septiembre de 1991.

²⁷ Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, adoptada el 23 de noviembre de 2010.

- *Recomendación (74)29* sobre la protección de las personas frente a las bases de datos electrónicas en el sector público.²⁸ Esta recomendación estableció PPD comunes específicos como guía a los Estados miembros para garantizar una aplicación armonizada y uniforme de estos principios. El objetivo era evitar las asimetrías entre la legislación de protección de los datos introducidos en los Estados miembros.

Las recomendaciones y resolución de la CE, para ser vinculantes, necesitan incorporarse a la legislación nacional. No obstante, estos principios de protección de datos han sido promovidos en toda Europa, en colaboración con la Unión Europea (UE). Muchos miembros han firmado el Convenio 108 y puesto en práctica en sus marcos jurídicos nacionales.

Ahora bien, por lo que se refiere a la UE ha desarrollado un régimen obligatorio para la privacidad y protección de datos. La UE exhorta a los países miembros que adopten el marco jurídico en materia de privacidad y se lleve a cabo una evaluación de la idoneidad de las normas y recomendaciones.²⁹

El marco jurídico de la UE incluye distintos tipos de normas jurídicas: convenios, protocolos, directrices, recomendaciones y resoluciones, todas son vinculantes para todos los países miembros. Sin embargo, las Directivas³⁰ vinculantes más importantes en relación con la protección de los datos emitidos por la UE son la Directiva 95/46/CE³¹ (conocida como la Directiva de Protección de Datos), su objetivo es establecer el marco regulatorio transfronterizo y equilibrar los intereses de los individuos y de los

²⁸ Recomendación R (74) 29 relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público, adoptada el 20 de septiembre de 1974.

²⁹ Artículo 25.6 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial*, núm. L 281 de 23/11/1995.

³⁰ La directiva es un acto jurídico que la UE, que normalmente dejan los Estados miembros un cierto margen de maniobra para promulgar las normas que adopte. Folsom, Ralph y Lake, Ralph B. (eds.), *European Union Law after Maastricht: a practical guide for lawyers outside the common market*, Holanda, Kluwer Law International, 1996, p. 5.

³¹ Sobre la protección de la privacidad y protección de datos de la presente Directiva es el texto principal de referencia a nivel europeo. La presente Directiva se aplica a los datos tratados y de almacenamiento en las bases de datos no automatizados y automatizados. Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial*, núm. L 281 del 23 de noviembre de 1995.

intereses públicos para el flujo de datos personales en Europa y la Directiva 2009/136/CE.³²

La Directiva 95/46/CE prohíbe el flujo de información transfronterizo a los países que tienen regímenes de protección de datos inadecuados (incluidos los miembros europeos). El objetivo de esta prohibición es “asegurar que el flujo transfronterizo de datos personales está regulado de una manera consistente”.³³ Para la UE, un régimen adecuado de protección de datos se basa en los siguientes requisitos: a) establecimiento de principios de protección de datos personales como obligaciones impuestas a los que participen en el tratamiento de los datos; b) circunstancias bajo las cuales el procesamiento se puede llevar a cabo, incluyendo la naturaleza de los datos, el objeto, la duración de la operación de tratamiento propuestas, calidad de los datos, las normas de derecho general y sectorial en vigor en el tercer país, normas profesionales, la seguridad técnica y la notificación a la autoridad de control, y c) establecimiento de derechos conferidos a los particulares, incluyendo ser informado sobre el flujo transfronterizo de datos, el acceso a los datos transferidos, a solicitar su rectificación o de oposición a la transferencia en circunstancias específicas.³⁴

Estas Directivas son importantes y se han complementado con recomendaciones vinculantes y las resoluciones son compatibles con los sistemas biométricos. Sin embargo, estudios comparativos realizados por la CE han señalado que operativamente las leyes de privacidad y protección de datos dentro de las fronteras de los miembros de la UE tienen asimetrías. Algunos de los países miembros difieren en el alcance de su aplicación de las Directivas y en las funciones y atribuciones de sus órganos garantes de protección

³² Modifica el marco actual de la UE relativo a las redes y servicios de comunicaciones electrónicas, así como cinco directivas. Estas directrices incorporan un gran avance en la regulación del tratamiento de datos personales y a la protección de la vida privada. En primer lugar, se abordan una serie de cuestiones relativas a los sistemas de procesamiento de datos. En segundo lugar, se han actualizado después de que la Comisión Europea (CE) presentó sus conclusiones sobre la revisión del marco regulador de la UE de las redes y servicios de comunicaciones electrónicas en 2006. Directiva 2009/136/EC del Parlamento Europeo del Consejo del 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) núm. 2006/2004 sobre la cooperación en materia de protección de los consumidores.

³³ Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *op. cit.*, nota 31, artículo 25(1), párrafo 8.

³⁴ *Ibidem*, artículo 25.

de datos personales. Además, algunos estudios académicos e informes han puesto de manifiesto esta falta de armonización en los marcos jurídicos nacionales.³⁵

El marco jurídico de la UE de datos transfronterizos facilita la libre circulación de datos personales entre los miembros europeos. Sin embargo, pueden surgir algunos problemas cuando la información personal fluye fuera de la región de Europa con diferentes enfoques de la regulación que se aplican, ya que los países fuera de esta región deben ajustar sus legislaciones nacionales en el marco jurídico de la UE con el fin de transferir los datos personales legalmente.

3. Ejercicio de los derechos ARCO

En el caso de la región de Asia-Pacífico, la APEC estableció que las autoridades nacionales encargadas de supervisar el tratamiento de los datos personales serían las responsables de funcionar como enlaces para que sus ciudadanos puedan ejercer los derechos ARCO. Por tanto, el pleno ejercicio de los derechos ARCO recae en las propias legislaciones sobre protección de datos personales, las cuales deben establecer un órgano especializado para supervisar el flujo transfronterizo de información personal. Estas autoridades deben llenar un formato solicitando la cooperación de la autoridad correspondiente en materia de protección de datos personales, por lo que el individuo no ejerce directamente los derechos ARCO.

En Europa existen dos autoridades diferentes encargadas de supervisar el tratamiento de los datos personales; para el sistema EURODAC el encargado es el Supervisor Europeo de Protección de Datos Personales (SEPD),³⁶

³⁵ Korff, Douwe, “EC Study on Implementation of Data Protection Directive 95/46/EC” (2002). Disponible en <http://ssrn.com/abstract=1287667>, consultado el 26 de mayo de 2014; Bygrave, Lee, “Privacy Protection in a Global Context. A Comparative Overview”, *Scandinavian Studies in Law*, vol. 47, pp. 319-348; Kuner, Christopher, “Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future”, *Tilbrüg Institute for Law, Technology and Society* (2010), <http://dx.doi.org/10.2139/ssrn.1689483>, fecha de consulta el 26 de mayo 2014; Korff, Douwe, “Comparative Study on Different Approach to New Privacy Challenges, in Particular in the Light of Technological Developments” (2010), http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf, fecha de consulta el 26 de mayo de 2014.

³⁶ <https://secure.edps.europa.eu/EDPSWEB/edps/lang/es/EDPS>, fecha de consulta el 26 de mayo de 2014.

mientras que para el Sistema de Información Schengen II el encargado es la Autoridad Común de Control de Schengen (ACC).³⁷

El Supervisor Europeo de Protección de Datos Personales (SEPD) tiene la responsabilidad de garantizar que las instituciones y organismos de la UE respeten el derecho de las personas a la intimidad en el tratamiento de sus datos personales. Por tanto, el ejercicio de los derechos ARCO ante anomalías en el tratamiento de datos personales por parte del sistema EURODAC recae directamente al SEPD, para poder ejercerlos se puede presentar una queja electrónica cuyo formato está en su portal de Internet.³⁸ Tal vez, las únicas dificultades son el idioma y tener conocimientos básicos de navegación en Internet para poder ejercer los derechos ARCO ante el SEPD.

El ejercicio de los derechos ARCO en el Sistema de Información Schengen II es más complejo. La Autoridad Común de Control de Schengen (ACC) es un órgano independiente especializado en protección de datos personales, está compuesto por miembros de cada autoridad de protección de datos personales nacional. La ACC ha elaborado directrices para el ejercicio del derecho de acceso, rectificación y cancelación. La solicitud se rige por el régimen nacional del ciudadano que solicita la información personal. Cabe resaltar que el derecho de acceso a la información personal entre cada uno de los Estados miembros de la zona Schengen se diferencia de una agencia a otra.

Por tanto, en la región de Europa, específicamente en la zona Schengen, el ejercicio del derecho de acceso a la información personal es contradictorio y el ejercicio de los derechos ARCO no es fácil de ejercer plenamente, con los distintos procedimientos y prácticas.

En la zona Schengen a nivel nacional, es decir, entre países miembros, se presentan dos escenarios relacionados con el ejercicio del derecho de acceso a la información personal:

- El primer escenario es cuando algunos regímenes de protección de datos establecen un procedimiento directo para ser seguido por las autoridades que operan las bases de datos biométricas a nivel nacional, cuando se solicita el acceso a la información personal. En este caso, los ciudadanos ejercen sus derechos ARCO al hacer sus

³⁷ <http://schengen.consilium.europa.eu/reports/activity-report.aspx?lang=es>, fecha de consulta el 26 de mayo de 2014.

³⁸ <https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Complaints>, fecha de consulta el 26 de mayo de 2014.

peticiones directamente a la autoridad encargada de la base de datos biométrica.

- El segundo escenario es cuando los regímenes de protección de datos establecen un procedimiento indirecto para el ejercicio de los derechos ARCO a través de solicitudes presentadas ante una autoridad de protección de datos, un mediador o un órgano específico. Esta situación hace que los ciudadanos no puedan acceder directamente a la información personal debido a que la solicitud se presentó ante el comisionado de privacidad, que luego procede a solicitar la información de la autoridad correspondiente en nombre de los ciudadanos. Muy similar a lo que sucede en la zona APEC.

Cabe resaltar que la mayoría de las personas afectadas por el SIS II son extranjeros. Sin embargo, la forma en que se establecen los derechos y recursos jurídicos pareciera estar dirigidos a ciudadanos de la UE.

Con base en lo anterior, se desprende que solamente en EURODAC es posible el pleno ejercicio de los derechos ARCO mientras que en la zona Schengen y APEC resulta más complicado debido a las asimetrías legislativas en materia de protección de datos personales. La zona Schengen cuenta con 26 legislaciones en materia de protección de datos personales y la APEC con 21.

V. CONCLUSIONES

Las organizaciones regionales no sólo han facilitado la implementación de sistemas biométricos centralizados, sino también han fomentado el flujo transfronterizo de información biométrica para el control de la inmigración, prevención de delitos transfronterizos y combate al terrorismo. Estos tres sistemas biométricos regionales utilizan los estándares o normas técnicas de la OACI. Sin embargo, el hecho de que estos sistemas biométricos regionales sean bases de datos centralizadas plantea una pregunta común acerca de la vulnerabilidad tecnológica y riesgos de privacidad con relación al acceso no autorizado, *hackers* y copias de seguridad. Además, es interesante observar que la misma empresa, Steria, sea la encargada de los dos principales sistemas biométricos en Europa.

El flujo transfronterizo de información biométrica debe realizarse con ética, integridad y coherencia no sólo en términos de información, sino también en el cumplimiento de las prácticas principales de protección de datos personales. Un claro y armonizado marco jurídico sobre protección

de datos personales es esencial para reducir las preocupaciones en esta área. Además, un régimen jurídico adecuado sobre el flujo transfronterizo de información biométrica asegurará no sólo la efectividad sino también la eficiencia técnico-jurídica de protección.

Las funciones de las organizaciones regionales (APEC, CE y la UE) están haciendo esfuerzos para crear un marco jurídico internacional para la implementación de estos sistemas biométricos y la regulación del flujo transfronterizo de la información biométrica. Sin embargo, estos intentos requieren la participación activa de todos los sectores, incluido el gobierno, la industria y los actores sociales. Una estrategia inclusiva y proactiva, así como un debate público más abierto sobre los riesgos técnicos (seguridad) y las limitaciones a las libertades civiles; la promoción de los derechos de privacidad y protección de datos; la transparencia y la rendición de cuentas sobre la gestión de estas bases de datos biométricos nacionales e internacionales centralizadas, son fundamentales para garantizar el efectivo ejercicio de los derechos ARCO.

En contraste con el Marco de Privacidad de APEC y el Convenio 108 del CE, las Directivas de la UE encarnan un marco legal obligatorio. Las directivas obligatorias de la UE establecen un régimen regional e imponen estrictos controles y garantías en materia de protección de datos. El marco jurídico de protección de los datos obligatorios de la UE se extiende a países fuera de la UE, ya que estos países deben tener protecciones equivalentes en materia de protección de datos. El marco jurídico de la UE proporciona un ejemplo de la mejor práctica de la protección de la privacidad y protección de datos y garantiza la eficacia de la reglamentación a nivel nacional, así como el flujo transfronterizo de información biométrica.

Los sistemas biométricos desplegados en Asia-Pacífico y Europa representan desafíos jurídicos donde se hacen evidentes las diferencias y complejidades jurídicas para ejercer los derechos ARCO en su totalidad.

VI. BIBLIOGRAFÍA

AMPLIACIÓN DEL SISTEMA DE INFORMACIÓN SCHENGEN POR CONVENIO PRÜM http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/jl0005_en.htm.

APEC PRIVACY FRAMEWORK (2004), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

- , Sistema de Reglas de Privacidad Transfronteriza (2012), [http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx).
- BOLLE, Ruud M. *et al.*, *Guide to Biometrics*, Springer, 2003.
- BOULGOURIS, Nikolaos V. *et al.*, *Biometrics, Theory, Methods, and Applications*, IEEE y Wiley, 2010.
- BYGRAVE, Lee, “Privacy Protection in a Global Context. A Comparative Overview”, *Scandinavian Studies in Law*, vol. 47.
- CONVENCIÓN PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, se abrió a la firma el 28 de enero de 1981.
- DÍAZ, Vanessa, “Sistemas biométricos en material criminal: un estudio comparado”, *IUS Revista del Instituto de Ciencias Jurídicas de Puebla*, núm. 31, vol. VII.
- DIRECTIVA 2009/136/EC del Parlamento Europeo del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) núm. 2006/2004 sobre la cooperación en materia de protección de los consumidores.
- DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial*, núm. L 281 del 23 de noviembre de 1995.
- FOLSOM, Ralph y LAKE, Ralph B. (eds.), *European Union Law after Maastricht: a practical guide for lawyers outside the common market*, Holanda, Kluwer Law International, 1996.
- HOPKINS, Richard, “An Introduction to Biometrics and Large Scale Civilian Identification”, *International Review of Law, Computers & Technology*, núm. 13.
- KING, Robert C. y STANSFIELD, William D., *A Dictionary of Genetics*, Oxford University Press, 1997.
- KORFF, Douwe, “Comparative Study on Different Approach to New Privacy Challenges, in Particular in the Light of Technological Developments” (2010), http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf.

- , “EC Study on Implementation of Data Protection Directive 95/46/EC” (2002), <http://ssrn.com/abstract=1287667>.
- KUNER, Christopher, “Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future”, *Tilbrüg Institute for Law, Technology and Society*, 2010, <http://dx.doi.org/10.2139/ssrn.1689483>.
- MARTÍNEZ JARRETA, Begoña, “Biometría (técnico)”, en ROMERO CASABONA, Carlos María (dir.), *Enciclopedia de Bioderecho y Bioética*, España, Comares, Fundación BBVA, Instituto Roche, Universidad del País Vasco, Universidad de Deusto, 2013.
- MATHER, Kenneth y JINKS, John L., *Biometrical Genetics. The Study of Continuous Variation*, Cornell University Press, 1971.
- MUÑOZ DE ALBA MEDRANO, Marcia, “El acceso a la información personal en el nuevo marco jurídico mexicano”, en VILLANUEVA, Ernesto y LUNA PLA, Issa (eds.), *Derecho de acceso a la información pública, Valoraciones iniciales*, México, UNAM, Atlatl, USAID, Konrad Adenauer, 2005.
- RECOMENDACIÓN CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, adoptada el 23 de noviembre de 2010.
- RECOMENDACIÓN R (74) 29 relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público, adoptada el 20 de septiembre de 1974.
- RECOMENDACIÓN R (91) 10 del Comité de Ministros a los Estados miembros sobre la comunicación a terceras personas de datos de carácter personal en poder de organismos públicos, adoptada el 9 de septiembre de 1991.
- REGLAMENTO (CE) núm. 2725/2000 del Consejo, del 11 de diciembre de 2000, relativo a la creación del sistema “Eurodac” para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín.
- SISTEMA DE INFORMACIÓN SCHENGEN, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/133020_en.htm.
- SOKAL, Robert y JAMES, Rohlf, *Biometry*, 3a. ed., W.H. Freeman, 2003.
- y JAMES, Rohlf, *Introduction to Biostatistics*, W.H. Freeman, 1973.
- ZHANG, David D., *Automated Biometrics Technologies and Systems*, Kluwer Academic Publishers, 2000.

TIC: GLOBALIZACIÓN Y POLÍTICA PÚBLICA EN EL ESTADO CONTEMPORÁNEO

Gonzalo FARRERA BRAVO*
Melissa BENÍTEZ BENÍTEZ **

SUMARIO: I. *Introducción*. II. *El adelgazamiento del Estado como tendencia global*. III. *Las TIC's como política pública en América Latina*. IV. *Estado y TIC's en América Latina*. V. *Gobernanza y TIC en México*. VI. *Conclusiones*. VII. *Bibliografía*.

I. INTRODUCCIÓN

A lo largo del tiempo el aparato estatal y el gobierno han ido evolucionando de acuerdo con las necesidades de cada sociedad. En los últimos años la sociedad ha tenido una fuerte inclinación hacia las Tecnologías de la Información y Comunicación (TIC), exigiendo de alguna manera que el Estado modifique la forma de interactuar con los ciudadanos a través de las TIC.

De esta forma el gobierno ha pasado a ser un gobierno electrónico (*e-gobierno*), en el año 2000, el *Gartner group*¹ define a este gobierno como: “la continua optimización en la entrega de servicios, la participación ciudadana, y el ejercicio del gobierno mediante la transformación de las relaciones internas y externas a través de la tecnología, Internet y los nuevos medios”.

La antigua perspectiva de la administración pública únicamente englobaba el trabajo de corte burocrático que implicaba la no satisfacción de las necesidades ciudadanas que buscando sólo la simulación del ejercicio de las facultades emanadas en la ley, este nuevo gobierno atiende a nuevos

* Profesor investigador de la Escuela Libre de Derecho, catedrático de la UAM Iztapalapa.

** Estudiante de la licenciatura en ciencia política de la UAM Iztapalapa, asistente de investigador del Instituto de Investigaciones Jurídicas de la UNAM.

¹ <http://www.gartner.com/technology/about.jsp> (14/6/14).

valores, es decir, trata de aprovechar al máximo las TIC para integrar a los ciudadanos a una nueva forma de participación en las actividades del Estado. Así, las TIC han cobrado un papel importante en el desempeño del gobierno y se han convertido en un medio de interacción entre los ciudadanos y el gobierno.

Para Jason Heyes y Helen Rainbridg² la estrategia del gobierno digital tiene como objetivo aprovechar al máximo el uso de las tecnologías de información y de comunicaciones en el funcionamiento de las dependencias y entidades de la administración pública federal (APF), para agilizar los trámites que realizan los ciudadanos, coadyuvar a transparentar la función pública, elevar la calidad de los servicios gubernamentales y, en su caso, detectar con oportunidad prácticas de corrupción al interior de las instituciones públicas, con los siguientes propósitos:

- Instalación y aprovechamiento de infraestructura tecnológica gubernamental, uso intensivo de redes de intranet gubernamental e Internet, para mantener integrada la actividad del sector público en todas las dependencias y entidades de la APF, e imprimir mayor precisión y oportunidad a la gestión de los servidores públicos.
- Promoción y aplicación de la administración del conocimiento y la colaboración digital, mediante sistemas y esquemas tecnológicos para adquirir, organizar y comunicar el conocimiento en la APF en sus distintas etapas, tales como aprendizaje, colaboración, evaluación y toma de decisiones. Estas acciones han sido fundamentales para el pleno ejercicio y operación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Mejora y rediseño de procesos con tecnologías de información, para desarrollar, actualizar y consolidar los sistemas informáticos en las distintas áreas de la APF, así como para facilitar la actualización informática de los procesos que operan las tareas adjetivas y sustantivas de las instituciones públicas.
- Mayor cobertura de los servicios y trámites electrónicos (e-Servicios) del gobierno, para ofrecer a la ciudadanía la oportunidad de acceder a éstos a través de medios electrónicos con seguridad y rapidez.
- Ampliación de mecanismos como e-Democracia y participación ciudadana, para continuar aplicando y desarrollando esquemas tecnológicos de planeación, participación y atención a la población,

² Heyes, Jason y Rainbridg, Helen, “State, Business and Training”, *The Oxford Handbook of Business and Government*, United Kingdom, OUP, EBook, 2011.

así como espacios en línea que identifiquen y recojan los planteamientos, problemas, necesidades y propuestas de la ciudadanía, facilitando su seguimiento mediante Sistemas de Administración de las Relaciones con Ciudadano.

Richard Heeks³ propone pensar el *e-governance* como “el aprovechamiento de las capacidades de automatización, información y comunicación de las TIC para mejorar los procesos de gobierno; para conectar gobierno y ciudadanos; para dar servicios a los ciudadanos y para construir interacción entre el gobierno y la sociedad civil y dentro mismo de la sociedad civil”.

En este sentido cabe analizar cuál es la situación de las TIC en México, en primer lugar no hay que perder de vista que el acceso a la tecnología no es homogéneo en todo el país, pues la realidad del campo y de la ciudad es sumamente contrastante, en el campo acceder a la tecnología resulta sumamente difícil, no sólo por los escasos recursos de la población rural, sino también por la falta de servicios básicos como la energía eléctrica; mientras que en las ciudades es mucho más fácil acceder a las TIC. Según el Instituto Nacional de Estadística y Geografía:

<i>Categoría</i>	<i>2011</i>	<i>2012</i>	<i>2013</i>
Hogares con computadora (como proporción del total de hogares)	30.8%	32.2%	35.8%
Hogares con conexión a Internet (como proporción del total de hogares)	23.3%	26.0%	30.7%
Usuarios de Internet que han realizado transacciones vía Internet (como proporción del total de usuarios de Internet)	5.1%	5.4%	5.8%
Usuarios de Internet que acceden desde fuera del hogar (como proporción del total de usuarios de Internet)	50.8%	48.0%	44.1%
Crecimiento anual de la fuerza laboral del sector de Tecnologías de la Información y Comunicación	-0.3%	ND	ND

FUENTE: INEGI.⁴

³ Heeks, Richard, *Implementing and Managing eGovernment: An International Text*, Sage, Londres, 2006.

⁴ <http://www.inegi.org.mx/inegi/contenidos/espanol/prensa/contenidos/estadisticas/2014/internet0.pdf> (13/6/14).

Desde el punto de vista de las ciudades, las TIC juegan un papel importante en la relación ciudadano-gobierno, ya que a través de éstas se han abierto nuevas formas de comunicación entre los ciudadanos y el gobierno. Conviene retomar cuál es la actividad de las TIC en México.

“De acuerdo con la Organización de las Naciones Unidas (ONU), México está posicionado en el décimo primer lugar mundial en materia de sofisticación y madurez de servicios⁵ gubernamentales en línea”.⁶

El acceso a la información se ha convertido en una realidad gracias a las TIC, ya que por medio de éstas varias instituciones ponen al alcance de los ciudadanos toda la información necesaria para que éstos puedan saber de las actividades y funciones de cada institución.

En materia jurídica consideramos que es donde las TIC han tenido un gran aprovechamiento. En cuanto al Poder Judicial algunos de sus órganos ya permiten revisar en línea cuál es la situación de las demandas, agilizando así los trámites ante los tribunales, dando a las partes un acceso a la información con mayor rapidez.

El Poder Legislativo ha puesto a disposición de los ciudadanos, a través de las páginas web de cada una de sus cámaras, todo lo concerniente a las actividades que realiza, así como las leyes aprobadas y en discusión. Esto es importante ya que, además de garantizar el derecho a la información, promueve de alguna manera la participación de los ciudadanos en las actividades de dicho poder.

El Poder Ejecutivo y la administración pública a su cargo, son los que mayor aprovechamiento de las TIC han tenido, esto a través de sus secretarías, que, por un lado, cada vez complementan más sus sitios web y, por el otro han agilizado los trámites ante las secretarías reduciendo así la burocracia.⁷

⁵ Por *e servicios* entenderemos como: “un conjunto de actividades que buscan responder las necesidades de un cliente o ciudadano a través de una modalidad virtual agilizando la materialización de la necesidad y buscando el gasto mínimo por parte del gobierno”. Chadwick, Andrew, *Internet Politics: State, Citizens and New Communication Technologies*, OUP, United Kingdom, 2006.

⁶ [http://www.undp.org.mx/spip.php?page=area_interior&id_rubrique=116&id_parent\(13/6/14\)](http://www.undp.org.mx/spip.php?page=area_interior&id_rubrique=116&id_parent(13/6/14)).

⁷ Velázquez Ríos, Korina, *Gobierno electrónico en México*, México, Cámara de Diputados, Congreso de la Unión, ediciones legislativas, 2009.

El gobierno electrónico o e-gobierno (en inglés *e-government*) consiste en el uso de las tecnologías de la información y el conocimiento en los procesos internos de gobierno, así como en la entrega de los productos y servicios del Estado tanto a los ciudadanos como a la industria. Muchas de las tecnologías involucradas y sus implementaciones son las mismas o similares a aquellas correspondientes al sector privado del comercio electrónico (o *e-business*), mientras

En el ámbito educativo las TIC en los últimos años han desarrollado un papel importante, debido a que han ayudado a que la población tenga mayor acceso a la educación a través de los programas de educación a distancia, garantizando así el derecho a la educación consagrado en el artículo 3o. de nuestra Constitución.

En nuestra opinión las TIC han ayudado al gobierno mexicano a relacionarse con los ciudadanos en tres ejes: el acceso a la información, los trámites en línea y el fomento a la participación ciudadana; además, gracias a las TIC se pueden ir garantizando derechos como la educación y el derecho a la información, con esto no queremos decir que todos los derechos se puedan cumplir a través de las TIC, pero sí es una gran alternativa para cubrirlos.

Por otra parte, las TIC ofrecen grandes beneficios, además de los ya mencionados, uno de ellos es el bajo costo, esto nos parece sumamente importante, sobre todo para un país en vías de desarrollo como el nuestro, porque permite que la información llegue a una gran parte de la población a un costo muy bajo y además reduce la burocracia.

Falta mucho por hacer en cuanto a TIC en México, sobre todo en redes de comunicación e infraestructura, para que la información llegue hasta los lugares más recónditos del país y el acceso a la información sea una realidad para todos los mexicanos. Sin embargo, pese a estas adversidades se ha dado un buen manejo de las TIC por parte del gobierno federal.

II. EL ADELGAZAMIENTO DEL ESTADO COMO TENDENCIA GLOBAL

Distintos movimientos dentro de la administración pública han venido a dar cuenta de la necesidad de modificar el ejercicio y el perfil de las actividades de la burocracia estatal. Países como Alemania y Estados Unidos han

que otras son específicas o únicas en relación con las necesidades del Estado. Se basa principalmente en la implantación de herramientas como portales, ERPs, que en caso de los gobiernos se conocen como GRPs (*Gross Rating Points*), CRMs (*costomer relationship management*), como redes sociales o comunidades virtuales y muchas otras, buscando una mejora en la eficiencia y eficacia en los procesos estatales internos y en las vinculaciones con la sociedad.

El gobierno electrónico describe el uso de tecnologías para facilitar la operación de gobierno y la distribución de la información y los servicios del mismo. Lidia con aplicaciones pertenecientes y no pertenecientes a Internet para servir de ayuda a la tarea de los poderes del Estado y de las instituciones estatales. Este servicio a los ciudadanos se realiza con el uso a gran escala de tecnologías como: teléfono, fax, sistemas de vigilancia, identificación por sistemas de radiofrecuencia e incluso la televisión y la radio.

introducido importantes cambios con la finalidad de “aligerar” y maximizar los recursos con los que el Estado realiza sus actividades. Las tecnologías son una importante aliada en la materialización de este proceso, debido a que pueden sustituir y hacer más eficientes las actividades que antes estaban muy burocratizadas.

En este sentido, las Tecnologías de la Información (TIC)⁸ brindan una importante oportunidad de mejorar los servicios de índole administrativa; esto debido a la automatización de los servicios y que el factor humano no sea un impedimento para brindar servicios de calidad a bajo costo.

La reducción de funciones estatales al núcleo esencial significa una crítica permanente de estas funciones mediante los siguientes criterios: necesidad, proporcionalidad, rentabilidad financiera y principio de subsidiariedad. Desde esta perspectiva se analiza qué actividades del Estado pueden ser privatizadas. Otra importante tendencia es la desaparición, o la unificación de numerosas autoridades, por ejemplo, altas direcciones de finanzas, institutos de investigación y organismo paraestatales.

La privatización como consecuencia de una cualificada crítica de funciones, constituye un necesario cambio de vía por causas político-legales; corresponde al principio de subsidiaridad que consiste en que el Estado deba retroceder cuando empresas privadas puedan realizar prestaciones de igual o mejor forma que las empresas públicas se establezcan el marco idóneo de condiciones para lograr estructuras competitivas. La privatización de empresas públicas fortalece el crecimiento y el empleo.⁹ Ello presta una importante contribución a la consolidación de los presupuestos públicos y da un margen de inversiones futuras. A través de la privatización se realiza la forma más eficiente y amable para los clientes, funciones que hasta ahora eran desempeñadas por el sector público. El poder económico y la competencia de decisión política son corregidos. La recomendación de organismos

⁸ Las tecnologías de la información y la comunicación (TIC), a veces denominadas nuevas tecnologías de la información y la comunicación (NTIC) son un concepto muy asociado al de informática. Si se entiende esta última como el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, esta definición se ha matizado de la mano de las TIC, pues en la actualidad no basta con hablar de una computadora cuando se hace referencia al procesamiento de la información. Internet puede formar parte de ese procesamiento que, quizás, se realice de manera distribuida y remota. Y al hablar de procesamiento remoto, además de incorporar el concepto de telecomunicación, se puede estar haciendo referencia a un dispositivo muy distinto a lo que tradicionalmente se entiende por computadora pues podría llevarse a cabo, por ejemplo, con un teléfono móvil o una computadora ultra-portátil, con capacidad de operar en red mediante comunicación inalámbrica y con cada vez más prestaciones, facilidades y rendimiento.

⁹ Roland Gérard, *Privatization: Successes and Failures*, Columbia University Press, 2008.

como la Organización para la Cooperación y el Desarrollo Económicos (en adelante OCDE),¹⁰ es que la privatización de los servicios debe hacerse en el sector de infraestructura pública. Otra perspectiva relevante con respecto a este tema es el cambio de paradigma que implica la administración burocrática a la empresa de prestación de servicios. Esto implica una nueva estructuración de organizaciones más grandes y flexibles, una conducta cooperativa responsable, equipos de trabajo con responsabilidad propia, un control operativo en conjunto, así como un control estratégico.

La inclusión de todos los empleados en el proceso de reforma es un componente esencial de la moderna gestión de personal. El miedo y la inseguridad pueden ser compensados mediante su participación en los procesos de cambio. Instrumentos como los círculos de calidad, la competitividad en las innovaciones o los talleres de ideas integran la creatividad disponible, los conocimientos y las experiencias de los empleados. Una gestión personal moderna significa una evolución personal consecuente, con aspectos como el perfil funcional, las estimaciones potenciales, la planificación de las necesidades, la capacidad, la protección de las mujeres y la movilidad laboral transnacional.

La reforma del régimen de administración económica es considerada como el resorte para la modernización de la administración. Una descentralización de la ejecución de la administración tributaria aumenta la motivación y los propios intereses de todos los participantes. Con ello pueden establecerse nuevas prioridades y puede reaccionarse adecuadamente frente a sucesos imprevistos. La introducción de presupuestos con un marco financiero rígido, con más años de vigencia, abre aspectos completamente nuevos para la economía de las finanzas públicas.¹¹

Parte de la política económica se encarga de formular los objetivos, señalando los instrumentos adecuados para controlar los ingresos y administrarlos, así como para elaborar el gasto del sector público. La política financiera se encarga del control del sistema bancario, así como de la política monetaria y crediticia. El gasto público en México está determinado por la

¹⁰ *Privatization in the 21st Century: Recent Experiences of OECD Countries*, 2011.

Por ejemplo, la OCDE ha expuesto en diversos documentos, la necesidad de privatizar áreas estratégicas en los Estados, ya sea las experiencias en América Latina o en los países satélites de la extinta URSS, el proceso de privatización se considera como un paso relevante dentro del desarrollo de Estados en vía de democratizarse, <http://www.oecd.org/daf/ca/corporategovernanceofstate-ownedenterprises/48476423.pdf> (15/6/14).

¹¹ Harcourt, G. C. y Peter Kriesler, "Reinventing Macroeconomics: What Are the Questions?", en Harcourt, G. C. y Kriesler, Peter (ed.), *Oxford Handbook Post-Keynesian Economics*, vol. I, *Theory and Origins*, OUP, United Kingdom, eBook, 2011, http://esa.un.org/techcoop/documents/Finance_Spanish.pdf (15/6/14).

Ley de Egresos de la Federación. Dicha Ley, que se emite en forma anual, marca las pautas y lineamientos, autoriza la forma y el monto en que se efectuará el gasto público; esta ley representa en sí el presupuesto de ingresos de la Federación.

El gasto público es uno de los principales instrumentos no sólo de la política financiera, sino de la política económica en general, ya que financia todas las actividades del Estado, tanto del subsector gobierno como de las empresas del Estado.

El Estado o sector público realiza su gasto corriente y su gasto inversión, de acuerdo con los lineamientos planteados en el Presupuesto de Egresos de la Federación.

La política financiera, sobre todo en lo que se refiere al gasto público, está a cargo de la Secretaría de Hacienda y Crédito Público. Las principales funciones de esta dependencia son las siguientes, de acuerdo con el artículo 31 de la Ley Orgánica de la Administración Pública Federal.

- Proyectar y coordinar la planeación nacional del desarrollo y elaborar, con la participación de los grupos sociales interesados, el Plan Nacional correspondiente.
- Proyectar y calcular los ingresos de la federación, del departamento del Distrito Federal y de las entidades paraestatales, considerando las necesidades del gasto público federal, la utilización razonable del crédito público y la sanidad financiera de la administración pública federal.

Para reforzar la comunicación y optimización de los procesos, la administración debe hacer uso de las TIC más destacadas. Con ello, y con la consiguiente reducción del trabajo rutinario a través de la automatización, aumenta la motivación y la capacidad de servicio de los empleados. Técnicamente hoy es posible, sin recorrer un largo camino y sin tomar en consideración los horarios de oficina, transmitir una instancia directamente a un organismo oficial desde una computadora personal. También la resolución puede ser comunicada al domicilio desde esta vía. El presupuesto para ello consiste en un acercamiento de los estándares nacionales e internacionales sobre el intercambio de documentos. La conversión exige especialmente la existencia de sistemas de seguridad dignos de confianza y que garanticen la protección de los datos de los usuarios.

En este sentido las TIC son parte de la política del Estado mínimo dentro de la renovación conceptual y ejecución de las labores de los Estados en nuestros días, así como la disminución de la regulación de índole

administrativa y de los estándares técnicos como objetivo primario de la desregulación.

III. LAS TIC COMO POLÍTICA PÚBLICA EN AMÉRICA LATINA

Las TIC se pueden considerar como un concepto dinámico y en constante cambio. A pesar de esto, en un concepto amplio, se puede considerar que el teléfono, la televisión y la computadora forman parte de lo que se llama TIC, en tanto que tecnologías que favorecen la comunicación y el intercambio de información en el mundo actual, pero con la revolución informática y tecnológica en la que vivimos cada día encontramos paradigmas que se rompen en la materia, y que hacen que el ejercicio del poder público sea más dinámico y que involucre al ciudadano,¹² desde diversas plataformas. Actualmente, en América Latina se empiezan a multiplicar los encuentros y proyectos ciudadanos¹³ en torno al concepto “Cultura de Red”. A través de

¹² Castells, Manuel, *End of Millennium: The Information Age: Economy, Society, and Culture*, Wiley, Blackwell Publishers, 2010.

Manuel Castell en su trilogía intitulada: “la era de la información”, centra su explicación en la dimensión sociológica del cambio tecnológico y sus efectos sociales de las tecnologías de la información. Para ello, nos muestra los principios y avances de las nuevas tecnologías, donde la información será la materia prima sobre la que actúan las tecnologías. Define tecnología como “el uso del conocimiento científico para especificar modos de hacer cosas de manera reproducible”. Dentro del campo de la información destaca cuatro áreas: la microelectrónica, la informática, las telecomunicaciones/televisión/radio y optoelectrónica y la ingeniería genética. Las cuatro formarán el núcleo de tecnologías de la información, durante las últimas décadas del siglo XX, creando un campo tecnológico donde la información se genera, almacena, recobra, y transmite. Pone en relación esta revolución con la revolución industrial del siglo XVIII, ya que ambas se caracterizan por su capacidad de penetración en todos los dominios de la actividad humana, convirtiéndose en la base de dichas actividades que se orientarán hacia el progreso. En este punto, considera que la innovación tecnológica no es un acontecimiento aislado, sino que se produce por acumulación y depende de las condiciones específicas de cada sociedad.

¹³ El concepto de ciudadanía digital (también denominado *ciberciudadanía* o *e-ciudadanía*) se emplea con dos sentidos, partiendo desde dos ópticas y áreas de conocimiento distintas pero confluentes: por un lado, hay quien lo utiliza para referirse a la aplicación de los derechos humanos y derechos de ciudadanía a la sociedad de la información y, por otro, quien lo limita a aquellas nuevas cuestiones relativas a los derechos y deberes de los ciudadanos que surgen en el entorno de las nuevas tecnologías. También existe un empleo menos riguroso que lo hace referente únicamente a la alfabetización digital de los ciudadanos, sin entrar en cuestiones éticas, ni relativas al concepto, ni al ejercicio de la ciudadanía. *La ciudadanía digital* supone la comprensión de asuntos humanos, culturales y sociales relacionados con el uso de las TIC, así como la aplicación de conductas pertinentes a esa comprensión y a los principios

espacios virtuales y presenciales, creadores y promotores buscan consolidar estrategias incluyentes de cooperación cultural para la región.

Para esto es necesario adherirse a un concepto de cultura dúctil para que podamos utilizarlo de referencia en los procesos de socialización y tecnologías. Para Clifford Geertz la cultura es:

El concepto de cultura al cual me adhiero ... denota una norma de significados transmitidos históricamente, personificados en símbolos, un sistema de concepciones heredadas expresadas en formas simbólicas, por medio de las cuales los hombres se comunican, perpetúan y desarrollan su conocimiento de la vida y sus actitudes con respecto a ésta.¹⁴

Para Geertz la cultura se entiende como un sistema de concepciones heredadas, es decir, transmitidas entre diferentes personas. Para establecer este sistema resulta necesario que existan un conjunto de conexiones o redes entre individuos que faciliten el traspaso cultural.

Hoy en día las herramientas digitales facilitan la interacción en tiempo real entre las personas y, en consecuencia, potencian el establecimiento de las conexiones necesarias para generar innovación en los procesos culturales. El desarrollo de la web 2.0 ha permitido a los usuarios de la red interactuar directamente entre ellos y colaborar entre sí para producir contenidos libremente. Con la web 2.0 se pasó de una “cultura” del *download* a una “cultura” del *upload*.

La web comenzó a transformarse en un punto de encuentro para la creación de contenidos de forma colectiva. Esta forma de creación puede ser entendida a través del modelo P2P (entre pares, entre iguales) que comenzó como un sistema de red entre computadoras que actuaban sin un servidor central, y ha evolucionado socialmente a una red distribuida de personas, una relación en red en la que cada uno de nosotros está conectado con los demás sin pasar por ningún centro, es decir entre pares, iguales.

que la orientan: ética, legalidad, seguridad y responsabilidad en el uso de Internet, las redes sociales y las tecnologías disponibles.

En la actualidad cada vez se le da una mayor importancia a la enseñanza para una ciudadanía responsable, que nos ayude a prevenir los riesgos que se pueden originar a partir del uso de las Tecnologías de Información y Comunicación (TIC) cotidianamente, sobre todo para los chicos. Hay algunas realidades, como el ciberbullying o ciberacoso, que son demasiado peligrosas para los niños y adolescentes que usan Internet.

Coleman, Stephen y Blumler, Jay G., *The Internet and Democratic Citizenship: Theory, Practice and Policy*, OUP, United Kingdom, 2011.

¹⁴ Geertz, Clifford, *The Interpretation of Cultures*, Basic books, Kindle Amazon, 1977.

La cultura de red deriva de los procesos en red, que existen desde siempre, ya que la conducta de redes se ha manifestado en el comportamiento humano, pero ahora se ve favorecida por los procesos digitales que amplían y transforman las redes, que favorecen nuevas formas de pensar, sentir y conocer, de adaptarnos para poder actuar en nuestros entornos tanto a nivel local como global.

El uso de las TIC no para de crecer y de extenderse, sobre todo en los países ricos, con el riesgo de acentuar localmente la brecha digital, social y la diferencia entre generaciones, desde la agricultura de precisión y la gestión del bosque a la monitorización global del medio ambiente planetario o de la democracia participativa.

Las políticas públicas¹⁵ relacionadas con la introducción de las TIC y promovidas por el gobierno federal en el país, se generaron en el contexto y por los compromisos adquiridos por el Tratado de Libre Comercio de

¹⁵ Ordóñez, Gonzalo, *Manual de análisis y diseño de política pública*, Bogotá, Universidad del Externado de Colombia, 2013.

Existen diferentes discusiones sobre el origen del enfoque de política pública. Por un lado, sostienen que nacen desde el momento mismo en que se configuran las sociedades estacionarias, es decir, que el surgimiento de dicho concepto es desde el momento en que el hombre deja de migrar y decide asentarse en un lugar fijo; por otro lado, se relaciona con el surgimiento de civilizaciones urbanas en contraprestación de ciudades tribales de la época.

Realmente el nacimiento de dicho concepto es posterior a la Segunda Guerra Mundial, cuando aumentó la preocupación por la capacidad de los gobiernos tanto como la dificultad económica, política y social en la que habrían de desenvolverse.

Sin embargo, en los años cincuenta y sesenta las políticas públicas (*policies*), eran consideradas como variables dependientes de la actividad pública (*politics*) en el sentido que se presuponía que las políticas públicas no eran más que el resultado o la consecuencia directa de la política (*politics*). En los años setenta, apareció progresivamente un interés por el estudio de la acción pública y la política pública *per se* (*policy*) se forjó como un concepto y como un objeto de estudio aparte. Empero, las políticas públicas se han desarrollado con mayor rapidez en los países avanzados, y aunque el ingreso de la disciplina en Latinoamérica es reciente, el análisis y evaluación de este concepto es un tema considerable de la discusión pública.

Hay una cifra innumerable de los autores que se han preocupado por proponer definiciones de política pública, entre la diversidad de definiciones se reconoce la tendencia práctica, en la cual se hace hincapié en la respuesta que se le da a una situación problemática, que es característica de la tradición norteamericana. De ahí que se hable sobre la importancia que tiene la acción del gobierno en la búsqueda de solucionar un problema público.

El primer esfuerzo sistemático para desarrollar una orientación explícita en políticas públicas ocurrió con la publicación de Lasswell (1971), quien estableció las características esenciales de la disciplina: “La ciencia de las políticas públicas está orientada en torno a los problemas y es contextual por naturaleza, multidisciplinaria en su enfoque y explícitamente normativa en su perspectiva”.

Lasswell, Harold, *Politics: Who Gets What, When, How*, Nueva York, Peter Smith Pub (1971), 1991.

América del Norte (TLCAN), el acuerdo internacional firmado entre México, Canadá y Estados Unidos. Expresan el imaginario que prevalecía y delinearón, de forma general, los propósitos de la apertura del país para satisfacer las necesidades de aprovechamiento de los recursos tecnológicos. Al paso del tiempo, cuando éstas se confrontan con la realidad se hace evidente la distancia cada vez mayor entre el discurso con que se formulan y los procesos generados para su aplicación con fines sociales.

La Sociedad del Conocimiento¹⁶ en el entorno nacional, de acuerdo con las políticas públicas, constituye un estado por alcanzar. Subyace una visión comercial centrada en el incremento del número de cibernautas y las actividades permitidas por la cantidad de *software* que se produce, esto a su vez permite que la ciudadanía se incorpore en los denominados derechos humanos de última generación.

Optar por la privatización en el sector de las telecomunicaciones significó ceder el poder de las decisiones a los monopolios para controlar y regular los precios y las operaciones de las empresas, en diversos rubros relacionados con las infraestructuras y servicios de comunicación. Las acciones emprendidas por los gobiernos federal y estatal de Jalisco en los últimos diez años no han sido relevantes; por el contrario, al priorizar la intervención de la empresa privada, ésta se ha convertido en obstáculo para generar procesos de inclusión digital socialmente hablando. En este ámbito el Estado mexicano ha dado una dura batalla para ir logrando que los actores comerciales pierdan cierta preponderancia para buscar una mayor competitividad y verdaderas condiciones de competitividad frente al mercado.

¹⁶ El concepto de “sociedad de la información” hace referencia a la creciente capacidad tecnológica para almacenar cada vez más información y hacerla circular cada vez más rápidamente y con mayor capacidad de difusión y la “sociedad del conocimiento” se refiere a la apropiación crítica y selectiva de la información protagonizada por ciudadanos que saben cómo aprovecharla.

Una cultura y una sociedad identificadas con estos términos son aquellas en las cuales la información y el conocimiento tienen un lugar privilegiado, y la creación, distribución y manipulación de la información forman parte estructural de las actividades culturales y económicas. La sociedad de la información es vista como la sucesora de la sociedad industrial. Relativamente similares serían los conceptos de sociedad posindustrial (término acuñado por Daniel Bell), posfordismo o sociedad postmoderna.

Norbert Wiener, creador de la cibernética, fue quien anunció el advenimiento de una “sociedad de la información” cuya base organizativa sería, según él, la circulación sin trabas de la información, a la que consideraba una nueva materia prima.

La noción de “sociedad del conocimiento” fue utilizada por primera vez por el filósofo de la gestión empresarial Peter Drucker, quien previamente había acuñado el término “trabajador del conocimiento”. En el decenio 1990-2000 fue profundizado en una serie de estudios detallados por autores como Robin Mansel o Nico Stehr.

El contexto latinoamericano ha sido muestra que no sólo se han limitado a desarrollar programas de inclusión digital, sino que internacionalmente se les reconocen avances significativos en el establecimiento de políticas públicas con respecto a las TIC, en el campo educativo y en la difusión de ciertas prestaciones como el uso de Internet en espacios públicos.

La política pública mexicana en materia de TIC en los dos últimos sexenios (2000-2012), es particularmente relevante por tratarse de las primeras decisiones tendientes a la inclusión-exclusión de la sociedad de la información y el conocimiento. No obstante que México destacó al inicio por haber sido el primer país en América Latina que logró un enlace a la red de la NSF (National Science Foundation), y otras compañías privadas en el ámbito de telecomunicaciones como la española Telefónica para buscar una mayor difusión dentro de la sociedad del tema. El significativo rezago en la promoción en el uso de las TIC prevalece. Una de las causas del complejo proceso vivido ha sido la mínima disposición en materia de inversión de infraestructuras que encarece significativamente los servicios. La OCDE ha reportado a México, en reiteradas evaluaciones, entre los países con los precios más altos para Internet de banda ancha, las reformas estructurales que planteó el presidente Enrique Peña Nieto, se ha destacado la concerniente al rubro de las telecomunicaciones, en donde las compañías dominantes van perdiendo cada día terreno comercial y en materia de infraestructura, frente a la competencia de otras nuevas que se introducen al mercado mexicano, como el caso de la británica *Virgin*.

El entonces presidente Vicente Fox con el proyecto: el *Sistema Nacional e-México* propuso como objetivo reducir la brecha digital entre el gobierno, los sectores y regiones del país y, en particular, las zonas más alejadas y pobres; los propósitos no se alcanzaron. La brecha digital entre los socios del Tratado de Libre Comercio de América del Norte, sigue siendo, como un rubro económico, muy significativa, al grado que esta especie de nueva desigualdad marca mucho el desarrollo industrial y tecnológico del país.

El reto para el presidente Peña Nieto será adecuar las necesidades tecnológicas de una economía en desarrollo que busca integrarse con mayor profundidad al reto que implica la globalización, ya que en este caso los capitales buscan lugares que oferten precios competitivos y mano de obra calificada que permita hacer una diferencia en la denominada sociedad del conocimiento. Las TIC están llamadas a ser uno de los ejes articuladores de este proyecto global, y buscan sumergir al ciudadano en la dinámica de la automatización y de la competencia económica en los niveles de macro y microeconomía. México juega un rol como economía emergente frente a los BRICS (Brasil, Rusia, India, China y Sudáfrica), y esto es una apuesta

que los países de occidente catapultarán a la economía mexicana como uno de los mercados más destacados en el ámbito financiero en el mundo.

IV. ESTADO Y TIC'S EN AMÉRICA LATINA

Tan inherente al ser humano como su tendencia a socializar, lo es su propensión al desarrollo de nuevas herramientas, mecanismos, técnicas y procedimientos que nos permiten dejar de lado las limitaciones físicas que nuestra naturaleza nos impone y dar paso a la modificación de nuestro entorno por conducto de la focalización de nuestro intelecto, al grado de alcanzar su total adaptación y moldeamiento en satisfacción plena de nuestras necesidades. Indudablemente, somos seres caracterizados no sólo por la búsqueda de una comunión armónica y organizada con nuestros pares, sino por la gran curiosidad que nos despierta nuestra propia identidad y la de nuestro entorno, lo cual nos ha conducido a emprender profundas reflexiones a la exploración del medio en que nos desenvolvemos en busca de su entera comprensión y manipulación.

De esta forma, el desarrollo tecnológico ha hecho transitar al hombre por un sendero en el que su subsistencia ya no se encuentra supeditada a su capacidad de adaptación al entorno, sino que es el lugar en el que decidimos asentarnos el que sufre un proceso de moldeamiento forzado, hasta alcanzar su adaptación en satisfacción de las necesidades del individuo. Hoy en día es fácil voltear y ser testigos de cómo áridos desiertos han sido convertidos en grandes oasis de prosperidad para el desarrollo urbano en tan sólo algunas décadas, o como se le ha ganado terreno al océano mediante la construcción de diques e islas artificiales.

En otras palabras, las fronteras de las conquistas del hombre sobre los elementos están determinadas por su intelecto y el desarrollo que éste nos ha permitido alcanzar, siendo las tecnologías un fruto de nuestra inventiva y un medio para alcanzar nuestros objetivos.

Dentro de una sociedad organizada, son muchas las necesidades por satisfacer y es aquí donde las tecnologías, a la par de proveer productos, servicios y comodidades, también nos proporcionan herramientas de productividad que hacen más eficiente toda aquella actividad en la que decidimos invertir nuestros esfuerzos.

Bajo este contexto, siendo que una necesidad primordial que la sociedad como ente colectivo debe cubrir, es la de garantizar una organización estatal exitosa a través de una correcta administración y ejercicio del poder público (*gobernanza*) –en inteligencia de que somos los ciudadanos los que

delegamos representación y facultad de dirección en los órganos públicos (hablando por supuesto de regímenes democráticos)— es que, por tanto, trasciende al interés público contar con un gobierno no sólo eficaz, sino además eficiente, es decir, un gobierno que con el menor número de recursos cumpla sus encomiendas a la mayor celeridad y trabaje día a día en la consecución de objetivos concretos que reafirmen el paso de la colectividad hacia metas específicas, como lo son el bien común, la ayuda mutua, la equidad y la seguridad jurídica, mismas que finalmente son las que dan sentido al Estado contemporáneo.

Este es un rubro en donde las tecnologías también ponen su grano de arena. A este respecto, debemos decir que las TIC se han convertido en importantes herramientas para la evolución de la vida democrática de nuestro país. Gracias a ellas es posible mitigar cualquier dificultad de comunicación derivada de las distancias geográficas, agilizar trámites, circular información eficientemente, facilitar el acceso a expedientes y registros de cualquier tipo, y simplificar procesos administrativos.

La implementación de las TIC, también ha coadyuvado en la gestión de recursos del erario, así como en el seguimiento de trámites y procesos, impulsando de igual forma la transparencia de las actividades de gobierno. Son herramientas que incluso han venido abonando a la solidificación de la certeza jurídica y principios democráticos del país. Sólo por mencionar un ejemplo del papel trascendental que los elementos tecnológicos han venido cobrando a este respecto, debemos apuntar a las contiendas electorales que a nivel federal se han suscitado en nuestro país en años recientes (particularmente desde las elecciones del año 2000), en donde sistemas como el “PREP” (Programa de Resultados Preliminares implementado por el Instituto Federal Electoral) y los sistemas de estadística implementados por empresas privadas, tomaron partido como mecanismos que pueden dar información y certeza a la ciudadanía de la tendencia de una elección, a escasos minutos de haber concluido el ejercicio democrático. Incluso el futuro de este tema, la urna electrónica, será el fin de las corruptelas clásicas en el ámbito electoral mexicano.

Así pues, en la misma forma el sistema político y la administración pública se han visto fortalecidos a través de la implementación de las TIC's, la administración y la gobernanza en la región en la que vivimos.

No es de extrañar que con el crecimiento exponencial de la población, la escasez de recursos, el deterioro ambiental, la carestía, la falta de liquidez, la ausencia de oportunidades de empleo, la inseguridad y muchos otros factores o fenómenos sociales, se venga suscitando un incremento en los conflictos de intereses que buscan una salida ante los tribunales. En Amé-

rica Latina, en muchos *libros blancos* se ha hablado de la necesidad de hacer una apuesta más fuerte de las TIC's en ámbitos no sólo administrativos que corresponden al poder ejecutivo sino también en el ámbito parlamentario y judicial.

Pese al incremento en la instalación de tribunales, no ha sido fácil que éstos se pongan al día en la atención dada a los negocios que ingresan al órgano jurisdiccional. Basta remitirnos a las estadísticas judiciales para darnos cuenta que el rezago sigue siendo importante y como los juicios, en lugar de convertirse en un medio para poner fin a un conflicto, terminan convirtiéndose en un peregrinar en donde las diferencias entre contendientes se agravan con la prolongación de litigios que tornan aún más ríspidas sus relaciones.

Frente a ello, es que, en un vuelco hacia el acogimiento de las nuevas TIC con las que hoy en día se cuenta, los órganos encargados de la administración y del gobierno en los diversos niveles han buscado hacer más eficiente su labor, implementando nuevos protocolos de captura de datos, sistematizando la información bajo su resguardo y dando oportunidad a los interesados de dar seguimiento de la actividad burocrática desde cualquier lugar en que se encuentren, anulando con ello las barreras de la distancia.

Asimismo, se han generado nuevas vías de comunicación interna y de contraloría estadística de la gestión de procesos y del ejercicio del poder. Se ha dotado al personal de equipo informático que les permite mantener una comunicación constante e inmediata, así como consultar archivos públicos y cualquier información de relevancia para su labor.

Los avances tecnológicos han incrementado la eficiencia del funcionario estatal al permitirle redactar notas y memorándums a través de mecanismos que facilitan las labores de corrección y propician una disminución en el desperdicio de papel. La consulta de criterios administrativos se ha simplificado notablemente a través de la sistematización de bancos de datos y criterios federales.

El Estado en América Latina sufre una compleja transición del modelo de administración pública de corte francés a un modelo inspirado en los países anglosajones, conocido como Gobernanza, que implica la interacción de los ciudadanos, la clase política y los servidores públicos contratados por el Estado. En este sentido las TIC vienen a darle un nuevo significado a esta perspectiva ya que tiene como objetivo primordial hacer eficiente el ejercicio del poder y reducir tiempos y costos de la labor burocrática de los Estados.

La tendencia en el continente ha marcado tendencias irregulares en este sentido, ya que las condiciones de casi todos los Estados no son propi-

cias para la tecnología, al no disponer de la infraestructura básica; en casos como el de México, el atraso es doble debido a la concentración de los medios tecnológicos en pocas manos, es propicio para generar una tiranía que condena al país y en cierta medida al continente al atraso. La política pública de muchos estados de Asia, por ejemplo, Corea del Sur,¹⁷ ha sido uno de los importantes detonadores de crecimiento de dicho tigre asiático, y en muchos sentidos han realizado una importante sincronía entre el Estado y la tecnología como eje toral del desarrollo capitalista de nuestros tiempos.

V. GOBERNANZA¹⁸ Y TIC EN MÉXICO

En la comunidad de naciones, la gobernanza se considera “buena” y “democrática”, en la medida en que las instituciones y procesos de cada país sean transparentes. Las instituciones hacen referencia a órganos tales como el parlamento y sus diversos ministros. Los procesos incluyen actividades fundamentales como elecciones y procesos legales, los cuales deben estar exentos de corrupción y deben ser responsables ante el pueblo. El cumplimiento de esta normativa se ha convertido en un baremo imprescindible para medir la credibilidad y el respeto de los países en el panorama mundial. La buena gobernanza promueve la equidad, la participación, el pluralismo, la transparencia, la responsabilidad y el Estado de derecho, de modo que sea efectivo, eficiente y duradero. Llevando estos principios a la práctica, somos testigos de elecciones frecuentes, libres y limpias, parlamentos representativos que redactan leyes y proporcionan una visión de conjunto, y un sistema jurídico independiente para interpretar dichas leyes.

¹⁷ Odagiri, Hiroyuki, “The East Asian (mostly Japanese) Model of Capitalism”, en Denis C. Mueller, *The Oxford Handbook of Capitalism*, OUP, United Kingdom, 2012.

¹⁸ El término gobernanza viene utilizándose desde la década de 1990 para designar la eficacia, calidad y buena orientación de la intervención del Estado, que proporciona a éste buena parte de su legitimidad en lo que a veces se define como una “nueva forma de gobernar” en la globalización del mundo posterior a la caída del muro de Berlín.

Sobre todo se emplea en términos económicos (lo que también se conoce como una de las acepciones del término quinto poder), pero también sociales o de funcionamiento institucional, esencialmente la interacción entre sus distintos niveles, sobre todo cuando se producen grandes cesiones competenciales hacia arriba (por ejemplo, la integración en la Unión Europea) y hacia abajo (la descentralización territorial, lo que se ha podido designar con el término sexto poder). También, y muy especialmente, la forma de interacción de las administraciones públicas con el mercado y las organizaciones privadas o de la denominada sociedad civil (empresas, patronales, sindicatos y otras), que no obedecen a una subordinación jerárquica, sino a una integración en red, en lo que se ha denominado “redes de interacción público-privado-civil a lo largo del eje local/global”.

La mayor amenaza para la buena gobernanza viene de la corrupción, la violencia y la pobreza, todo lo cual debilita la transparencia, la seguridad, la participación y las libertades fundamentales.

La gobernanza democrática fomenta el desarrollo y dedica su energía a influir en tareas como la erradicación de la pobreza, la protección del medio ambiente, garantizar la igualdad entre los géneros y proporcionar los medios de subsistencia sostenibles. Garantiza que la sociedad civil desempeñe un papel activo al establecer prioridades y dar a conocer las necesidades de los sectores más vulnerables de la sociedad.

En este sentido las TIC¹⁹ pueden ser claves para su posible ejecución, si se piensa que a través de ellas se pueden materializar las diversas aspiraciones de los gobiernos democráticos. La gobernabilidad electrónica implica nuevos estilos de dirección, nuevas formas de debatir y decidir políticas e inversiones, nuevas maneras de escuchar a los ciudadanos y de organizar y proporcionar información y servicios.

La gobernabilidad se refiere al ejercicio de la autoridad política, económica y administrativa en la gestión de los asuntos de un país, incluyendo la expresión por parte de los ciudadanos de sus intereses y el ejercicio de sus derechos legales y obligaciones. La gobernabilidad electrónica se puede entender como la capacidad de esta gobernabilidad, a través del medio electrónico, de facilitar un proceso de disseminación de la información eficaz, rápida y transparente para el público y otras agencias, y para desarrollar actividades administrativas eficaces por parte del gobierno.

La gobernabilidad electrónica es considerada generalmente como un concepto más amplio que el de gobierno electrónico, ya que puede traer consigo un cambio en la manera en como los ciudadanos se relacionan con el gobierno y entre ellos. La idea de adoptar las TIC es para ir más allá que la información pasiva dada hasta ahora para activar la participación en el proceso de toma de decisiones. La gobernabilidad electrónica puede presentar nuevos conceptos de ciudadanía, tanto refiriéndose a las necesidades del ciudadano como a sus responsabilidades. Su objetivo es comprometer, capacitar y dar poder al ciudadano.

¹⁹ Gobernanza de TI es el alineamiento de las Tecnologías de la Información y la comunicación (TI) con la estrategia del negocio. Hereda las metas y la estrategia a todos los departamentos de la empresa, y proporciona el mejor uso de la tecnología y de sus estructuras organizativas para alcanzarlas.

Aun cuando no existe una definición exacta de lo que es la gobernanza de Tecnologías de la Información (TI), trataremos de conceptualizarla tomando los puntos clave de los conceptos que mayormente se utilizan para hacer referencia a la gobernanza de TI.

El propósito de implementar la gobernabilidad local es lograr una mejora de la gobernanza. Las características que definen una buena gobernanza son generalmente la participación, la transparencia y la información. Los avances recientes en las tecnologías de la comunicación y en Internet proporcionan oportunidades para transformar la relación entre gobiernos y ciudadanos de una nueva manera, así se contribuye al logro de los objetivos de una buena gobernanza. El uso de la tecnología de la información puede aumentar la participación de los ciudadanos en el proceso de gobernanza en todos los niveles proporcionando la posibilidad de una discusión de grupos *on-line* y mejorar el rápido desarrollo y la eficacia de los grupos de presión.

Las ventajas que conlleva para el gobierno implican que éste pueda proporcionar un mejor servicio en cuanto al tiempo, haciendo la gobernanza más eficaz y más efectiva. Además, el costo de transacción puede ser menor y los servicios del gobierno ser más accesibles. Los campos de implementación de la gobernabilidad electrónica son:

- Administración electrónica (*e-administration*). Se refiere a la mejora de los procesos gubernamentales y de los funcionarios del sector público gracias a las nuevas TIC y a los procesos de ejecución de información.
- Servicios electrónicos (*e-services*). Se refiere a la mejora en la facilitación de los servicios públicos a los ciudadanos. Algunos ejemplos de servicios interactivos son: solicitudes de documentos públicos, solicitudes de documentos legales y certificados, expedición de permisos y licencias.
- Democracia electrónica (*e-democracy*). Implica una mayor y más activa participación ciudadana en el proceso de la toma de decisiones gracias a las TIC.²⁰

Objetivos de la gobernabilidad electrónica

- Mejorar la organización de los procesos internos de los gobiernos.
- Proporcionar mejor información y un mejor servicio.
- Acrecentar la transparencia gubernamental con el fin de reducir la corrupción.
- Reforzar la credibilidad política y la responsabilidad.

²⁰ Lam, Wai Fung, "Governing the Commons", en Bevir, Mark (ed.), *The SAGE Handbook of Governance*, United Kingdom, Sage, *eBook*, 2011.

- Promover prácticas democráticas a través de la participación y la consulta del público.

En el caso particular de nuestro país, la perspectiva de la gobernanza electrónica da pasos muy lentos, pero esto se debe conjugar con el paquete de reformas estructurales contempladas en el Plan Nacional de Desarrollo 2013-2018, ya que las mismas son el eje explicativo de la renovación del Estado mexicano. En este sentido, la globalización da estímulos relevantes para llevar al país a una importante reestructuración de la administración pública, las TIC aportan elementos de gran relevancia para cumplir con este objetivo. El Estado mexicano paulatinamente va adoptando criterios de modernización de los servicios que presta a la ciudadanía, pero aún falta mucho por hacer.

VI. CONCLUSIONES

La tecnología es uno de los parámetros evolutivos de las sociedades en nuestros días, su desarrollo, consumo y masificación es consecuencia de la sistematización de la vida cotidiana. Regiones como el sureste de Asia han incrementado el nivel de desarrollo humano de sus habitantes debido a la explosión de sus mercados en el ámbito de la tecnología.

Las TIC son de incuestionable practicidad, y tanto en el ámbito público como en el privado han marcado un hito con respecto a la eficiencia y el incremento de productividad a bajo costo; esto implica que las TIC han venido a contribuir con los cambios que se plantean dentro de la administración pública, consecuencia de tendencias como el *new public management*.²¹

Otro aspecto importante a destacar es la tendencia global a minimizar las funciones del Estado, con el argumento que las funciones burocráticas pueden mejorarse y ser más eficientes, del mismo modo en que en el mundo privado se logra que los procesos se encuadren en dinámicas competitivas: *hacer más con menos*.

En la actualidad, las TIC nos proveen de:

- Fácil acceso a todo tipo de información, sobre cualquier tema y en cualquier formato (textual, icónico, sonoro), especialmente a través

²¹ Lane, Erik Jane, *New Public Management: An Introduction*, United Kingdom, Routledge, 2011.

Klijin, Erik-Hans, “New Public Management and Governance: A Comparison”, en Levi-Faur, David (ed.), *The Oxford Handbook of Governance*, United Kingdom, OUP, 2012.

de la televisión e Internet, pero también mediante el acceso a las numerosas colecciones de discos en soporte CD-ROM y DVD: sobre turismo, temas legales, datos económicos, enciclopedias generales y temáticas de todo tipo, películas y vídeos digitales, bases de datos fotográficas y todo aquello que desee ser resguardado y compartido.

- Canales de comunicación inmediata, como el *e-mail* y salas virtuales de *chat* en tiempo real. Asimismo, Facebook y Twitter son redes sociales que tienen como esencia principal la comunicación y el intercambio inmediato de información sin importar distancias.
- Almacenamiento de grandes cantidades de información en pequeños soportes de fácil transporte y toda una serie de avances en cualquiera de los campos que busquen aplicarse.

Los Estados contemporáneos han hecho suyo como política pública la introducción de las TIC como parte de los ejes articuladores del desarrollo; en este sentido quienes han tenido los desarrollos más destacados tienen como constante una gran inversión en el desarrollo y difusión de las nuevas tecnologías. Los neologismos como *gobernanza electrónica* nos recuerdan la idea del *Estado-aparato* que los alemanes utilizaban para buscar una mayor eficiencia en el ejercicio del poder. En este sentido la gobernanza busca incorporar los beneficios del mundo digital con la interacción no sólo de los entes públicos sino también privados.

Las TIC están llamadas a ser una nueva revolución industrial con importantes consecuencias para la vida común, y su inmersión en el ámbito estatal está generando nuevas dinámicas y retos. El miedo al cambio es una constante que recuerda cómo los obreros ingleses en el siglo XVIII destruían las máquinas por el miedo a ser sustituidos en sus puestos laborales.

VII. BIBLIOGRAFÍA

- CASTELLS, Manuel, *End of Millennium: The Information Age: Economy, Society, and Culture*, Wiley, Blackwell, 2010.
- CHADWICK, Andrew, *Internet Politics: State, Citizens and New Communication Technologies*, United Kingdom, OUP, 2006.
- DENNIS C. Mueller, *The Oxford Handbook of Capitalism*, United Kingdom, OUP, 2012.
- GEERTZ, Clifford, *The Interpretation of Cultures*, Basic books, Kindle Amazon, 1977.

- HARCOURT, C. y KRIESLER, Peter (eds.), *Oxford Handbook Post-Keynesian Economics*, vol. I, *Theory and Origins*, OUP, United Kingdom, *eBook*, 2011.
- HEEKS, Richard, *Implementing and Managing eGovernment: An International Text*, Londres, Sage, 2006.
- LANE, Erik Jane, *New Public Management: An Introduction*, United Kingdom, Routledge, 2011.
- LASSWELL, Harold, *Politics: Who gets What, When, How*, Nueva York, Peter Smith Pub (1971), 1991.
- LEVI-FAUR, David (ed.), *The Oxford Handbook of Governance*, United Kingdom, OUP, 2012.
- ORDÓÑEZ, Gonzalo, *Manual de análisis y diseño de política pública*, Bogotá, Universidad del Externado de Colombia, 2013.
- Privatization in the 21st Century: Recent Experiences of OECD Countries*, 2011.
- ROLAND, Gérard, *Privatization: Successes and Failures*, Columbia University Press, 2008.
- “State, Business and Training”, en Coen, David, Grant, Wyn y Wilson, Graham (eds.), *The Oxford Handbook of Business and Government*, United Kingdom, OUP, *eBook*, 2011.
- STEPHEN, Coleman y G. BLUMLER, Jay, *The Internet and Democratic Citizenship: Theory, Practice and Policy*, United Kingdom, CUP, 2011.
- VELÁZQUEZ RÍOS, Korina, *Gobierno electrónico en México*, México, Cámara de Diputados, Congreso de la Unión, 2009.
- WAI-FUNG, Lam, “Governing the Commons”, en BEVIR, Mark (ed.), *The Sage Handbook of Governance*, United Kingdom, Sage, *eBook*, 2011.

JUSTICIA ELECTRÓNICA: EN BUSCA DE LA INTEROPERABILIDAD

Myrna Elia GARCÍA BARRERA*

SUMARIO: I. *Introducción*. II. *Justicia electrónica*. III. *Interoperabilidad*.
IV. *Tribunal Virtual en Nuevo León*. V. *Conclusiones*. VI. *Bibliografía*.

I. INTRODUCCIÓN

En nuestra época es evidente que los avances tecnológicos han otorgado beneficios no sólo en el ámbito de las ciencias exactas sino también en el ámbito de la cibernética, de las comunicaciones y, por supuesto, en el derecho, provocando una serie de revoluciones que impactan en el gobierno electrónico y específicamente en la justicia electrónica.

El encuentro entre el derecho y la informática se da en la regulación de esta última. Además, debe preservarse entre ambas un equilibrio para la construcción de conocimientos, específicamente en la relación entre decisión judicial e informática decisional, para consolidar la llamada “justicia electrónica”. La justicia electrónica es modernización, ya que se utiliza la tecnología, las Tecnologías de Información y Comunicación, las llamadas TIC, al servicio del proceso de impartición de justicia, en otras palabras, gobierno electrónico en la impartición de justicia.

Por gobierno electrónico entendemos a los procesos y estructuras creados para la oferta electrónica de los servicios públicos. El gobierno electrónico depende funcionalmente de una política pública, clara, objetiva,

* Doctora en derecho egresada de la Facultad de Derecho y Criminología de la UANL. Investigadora en el Centro de Investigación de Tecnología Jurídica y Criminológica de la Facultad de Derecho y Criminología de la UANL. Catedrática de la propia Facultad de Derecho y Criminología de la UANL y de la Universidad de Monterrey. Directora de Equidad de Género y Protección a Grupos Vulnerables del Poder Judicial del Estado de Nuevo León. SNI nivel 1.

con etapas de avance, en los tres ámbitos: ejecutivo, legislativo y judicial, facilitando una transformación mucho más profunda: “hacia un modelo de gobierno relacional y orientado a los resultados”.¹ Ya que:

Uno de los pilares fundamentales de esta modernización tecnológica es la interoperabilidad en cuanto contribuye decisivamente a garantizar el funcionamiento armónico y cohesionado de los distintos sistemas, organizaciones, procesos y aplicaciones existentes que, en el ámbito de la justicia, son números dada la variedad de actores implicados: diferentes órganos judiciales, pero también administraciones distintas, como las responsables de los cuerpos y fuerzas de seguridad, y profesionales jurídicos.²

El proyecto de interoperabilidad busca conseguir que los sistemas y las aplicaciones informáticas, que actualmente manejan las diversas instituciones públicas, puedan conversar mutuamente, sean interoperables y contribuyan a mejorar y a minimizar los tiempos de atención al ciudadano, con especial énfasis en la administración de justicia.³

Es menester señalar que se requiere que el gobierno tenga apertura a un modelo de prestación de servicios bastante complejo, por la seguridad jurídica y tecnológica que debe cuidarse en todos los procesos o trámites del gobierno electrónico.

El “Estado de derecho” necesita crear la legislación que valide la transición del papel al documento electrónico en los diferentes trámites del llamado gobierno electrónico, no sólo abarcando los procesos de información en línea, sino también que el mismo trámite sea realizable en línea, incluyendo pagos, firma electrónica digital, etcétera.

Es claro que los principales beneficios son: el ahorro de tiempo, papel y dinero, con la gran ventaja de tener disponibilidad las 24 horas del día y los 365 días del año.

¹ Criado Grande, J. Ignacio, Ramilo Araujo, María Carmen *et al.*, “La necesidad de teoría(s) sobre gobierno electrónico. Una propuesta integradora”, XVI Concurso de Ensayos y Monografías del CLAD sobre Reforma del Estado y Modernización de la Administración Pública, “Gobierno Electrónico”, Caracas, 2002, p. 45, [http://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Comercio%20Electronico/la-necesidad-de-teoria\(s\) sobre-gobierno-electronico-una-propuesta-integradora.pdf](http://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Comercio%20Electronico/la-necesidad-de-teoria(s) sobre-gobierno-electronico-una-propuesta-integradora.pdf). Consultada el 6 de enero de 2015.

² Jiménez, Carlos E., *Interoperabilidad en la administración de justicia: experiencias y buenas prácticas en un ámbito complejo*, ponencia presentada en el XV Congreso Internacional del CLAD sobre las Reformas del Estado de la Administración Pública, p. 1, http://estratic.files.wordpress.com/2010/12/jimenez_io_justicia.pdf. Consultada el 12 de abril de 2014.

³ <http://pmsj-peru.org/wp-content/uploads/2012/05/balance-informativo-n1-enero-marzo-2012.pdf>. Consultada el 14 de abril de 2014.

Para la Organización de las Naciones Unidas,⁴ en el World Public Sector Report 2003 “E-government at the crossroads”, la letra “e” que se refiere al gobierno electrónico por el concepto en inglés “electronic government”, ayuda a reconocer que la administración pública se encuentra en un proceso de transformación de sus relaciones internas y externas con el uso de las nuevas TIC. Según el mismo documento, el concepto de gobierno electrónico abarca dos aspectos:

1. La capacidad o aptitud genérica del sector público para utilizar las TIC y así brindar servicios públicos y desplegar información de alta calidad (conocimiento explícito) al público, y proporcionar herramientas de comunicación efectivas que apoyen el desarrollo humano. Esta es la capacidad que tiene un gobierno para implementar el gobierno electrónico.
2. La voluntad, de parte del gobierno, para proveer información de alta calidad (conocimiento explícito) y herramientas de comunicación efectivas para el propósito específico de darle el poder a la gente para participar en consultas y en la toma de decisiones, dentro de sus capacidades como consumidores de servicios públicos y como ciudadanos. Este segundo aspecto define lo que es la *e-participation*.⁵

Ambas definiciones son muy útiles para la presente investigación, pues plantean dos etapas generales del desarrollo del gobierno electrónico:

1. Una primera etapa estática, en la cual predomina un gobierno electrónico utilizado como sistema de información.
2. Una etapa dinámica, identificada con valores democráticos como la participación ciudadana en las decisiones de gobierno.

Es conveniente considerar como válidos ambos aspectos del gobierno electrónico porque el segundo es complementario del primero. De acuerdo con el grado de desarrollo e implementación de los propios programas electrónicos, se espera que sea el gobierno quien ofrezca y proponga unilateralmente los contenidos que publica en sus páginas oficiales de Internet.⁶

⁴ “Gobierno electrónico: elementos de facilidad de uso y valor público de los portales de Internet local en México”, Sandoval Cervera, Sergio Alberto, tesis de maestría en gobierno y asuntos públicos, México, 2008, pp. 29 y 30, http://conocimientoabierto.flacso.edu.mx/medios/tesis/sandoval_sa.pdf. Consultada el 4 de mayo de 2014.

⁵ *Idem*.

⁶ Gobierno electrónico, *op cit.*, nota 4.

Ahora bien, en la segunda etapa se espera que los usuarios de esas páginas gubernamentales puedan interactuar con sus gobernantes y que sus opiniones sean consideradas en los programas públicos y en la toma de decisiones que la misma administración pública ponga a su consideración. Es decir, durante la primera etapa estática del gobierno electrónico, se espera que sea el propio gobierno quien ofrezca y proponga unilateralmente los contenidos que publique en sus páginas oficiales de Internet. En la segunda etapa, se espera que los usuarios de esas páginas gubernamentales puedan opinar, sugerir y, de forma ideal, votar y decidir, junto con los gobernantes, sobre programas públicos y toma de decisiones que la misma administración pública ponga a su consideración.⁷

Las experiencias de mejores prácticas a nivel nacional mexicano indican un nivel de desarrollo estático de los portales web oficiales. Lo anterior se debe fundamentalmente al predominio de las funciones informativas en las publicaciones de los sitios de Internet. De manera tal que se propone construir un instrumento que recoja los puntos de vista de expertos en gobierno electrónico, para identificar los objetivos ideales de los portales web; las características de construcción de los portales para facilitar su uso; las funciones dentro de un portal que tienen mayor relevancia para darle verdadera utilidad pública a los mismos y, finalmente, cuáles son los elementos que harían que un sitio web oficial de gobierno contribuya a mejorar las operaciones de la administración pública.⁸

La interacción con el sitio web se cumple cuando el usuario establece la relación o interacción con el mismo medio. Este tipo de interacción es posible cuando la relación con el ambiente de interfaz es de fácil comprensión para el usuario y cuando es sensible a cambios por este último, mismo que es empleado en muchos casos para facilitarle al navegante o usuario algún procedimiento automático.

El gobierno electrónico existe por la aplicación de las TIC en las actividades de los entes públicos, utilizando Internet; la interacción entre gobierno-gobernantes y entre gobierno-gobierno en la llamada justicia electrónica.

II. JUSTICIA ELECTRÓNICA

Los avances tecnológicos han otorgado beneficios no sólo en el ámbito de la cibernética, de las comunicaciones, o de las ciencias exactas, sino

⁷ *Ibidem*, p. 56.

⁸ *Idem*.

dichas innovaciones se han ido adoptando en varias materias o áreas del conocimiento, entre ellas se encuentra el derecho, en el cual se han encontrado tres tipos diferentes de informática jurídica: documental, de gestión y decisoria o decisional, siendo la primera aquella que se encarga de realizar el almacenamiento, clasificación y orden de los datos, resoluciones, fallos, documentos, ordenamientos legislativos, así como toda la información jurídica; de esta forma, la informática jurídica documental es una herramienta que facilita el almacenamiento y búsqueda de la información con mayor agilidad.

Mientras la tecnología avanza, Internet se ha convertido en un medio de comunicación mundial que ha abarcado ramas importantes como es el derecho y los sistemas de impartición de justicia. Para poder analizar el concepto de “justicia” electrónica, primero se tendrá que analizar lo que es la “justicia” en términos generales. La justicia proviene del latín “*iustitia*” y de acuerdo con el *Diccionario de la lengua española* es: “una de las cuatro virtudes cardinales, que inclina a dar a cada uno lo que le corresponde o pertenece/derecho, razón, equidad/conjunto de todas las virtudes, por el que es bueno quien las tiene y aquello que debe hacerse según derecho o razón”.⁹ “La justicia, más que cualquier otro aparato del Estado, debe funcionar y funcionar bien. De su forma de operación depende que haya paz y armonía entre los ciudadanos”.¹⁰

De lo anterior, y analizando lo que significa la justicia, podemos darnos una idea de que la “justicia” electrónica es un término que no existe tal y como se escucha. Puede variar el término o se puede interpretar en varios sentidos; se puede definir como las nuevas posibilidades que ofrecen las TIC, en el seno de la sociedad del conocimiento para garantizar una administración de justicia al servicio de los ciudadanos y ciudadanas. Se trata de un concepto que involucra cualquier transacción institucional efectuada por medios electrónicos, ya sean éstos teléfono, fax, Internet, télex,¹¹ Electronic Data Interchange (en adelante EDI),¹² etcétera, con el objeto de agilizar el proceso judicial por medio de la reducción de tiempos y de costos.

⁹ *Diccionario de la lengua española*, http://seminariodejusticia.blogspot.com/2012/11/justicia-en-el-diccionario-de-la-real.html?_sm_au_=iVVHsVSWZDbjF5WF. Consultada el 4 de mayo de 2014.

¹⁰ Jordán Flores, Fernando, *Las nuevas tecnologías y el derecho y la justicia*, Bogotá, Colombia, Servigraphic, LTDA, 2000, p. 15.

¹¹ El télex de la red es una red conmutada de teletipos similares a una red telefónica para los efectos de envío de mensajes de texto.

¹² Intercambio electrónico de datos en sus siglas en inglés: *Electronic data interchange*.

Por su parte, la informática jurídica de gestión tiene como objetivo la creación de documentos o datos nuevos a partir de unos ya existentes, satisfaciendo con mayor eficiencia y rapidez las necesidades de los abogados, tanto en el ámbito privado como en el público. Finalmente, la informática jurídica decisoria

...es el segmento de la informática jurídica que procura proponer o adoptar soluciones apropiadas para casos concretos que se le planteen, valorando los datos de cada problema por comparación con los criterios de decisión que se le hayan provisto. Con el debido respeto, trata de hacer por medio del ordenador lo que con su cerebro hacen hoy los encargados de adoptar decisiones jurídicas, especialmente cuando se trata de decisiones de rutina sujetas a modos de solución suficientemente conocidos.¹³

Al respecto, Guibourg, Alenda y Campanella, en su libro titulado *Manual de informática jurídica*, opinan: “La informática decisoria suele presentarse a sí misma como una colección de métodos, medios y propuestas para auxiliar al decidor humano en su tarea, antes que para reemplazarlo”.¹⁴

A pesar de las ventajas que dicha herramienta nos otorga, es importante mencionar que muchos juristas se oponen ante la idea del uso de la “justicia electrónica”, ya que creen que las computadoras, con la ayuda de la inteligencia artificial, van a reemplazar a los juzgadores humanos en la impartición de justicia, pero debemos aclarar que esa no es la misión ni el objetivo de dicha herramienta, sino el ayudar para que la tarea del juzgador sea más sencilla.

Para que esto sea posible, es necesario que se determinen los razonamientos lógicos que se deben seguir para realizar una tarea determinada, ya que las herramientas, como los diferentes programas computacionales, requieren necesariamente ser instruidos con las premisas hipotéticas y sus diferentes consecuencias, para lo cual se debe de cumplir con los siguientes requisitos:

- a) Tener claro cuáles son las condiciones que integran el Universo de Propiedades, en adelante UP, y cuándo ha de entenderse que cada una de ellas está presente o ausente en un caso concreto.
- b) Tener en claro cuáles son las soluciones que integran el Universo de Soluciones, en adelante US.

¹³ Guibourg, Ricardo A. *et al.*, *Manual de informática jurídica*, Argentina, Astrea, 1996, pp. 11 y 12.

¹⁴ *Ibidem*, p. 151.

- c) Cuidar que el sistema normativo esté libre de inconsistencias (dos normas que relacionen un mismo caso con soluciones incompatibles) y de lagunas indeseadas (casos pragmáticamente relevantes que no estén relacionados con una solución por norma alguna).¹⁵

En lo que respecta al inciso a), se debe establecer que se refiere al problema de la interpretación de la legislación y de la valoración de las pruebas. Por su parte, se considera que el inciso b), es la parte más sencilla, aun cuando limita las soluciones que se le pueden dar a los problemas planteados en el inciso anterior.

Finalmente, el inciso c), “choca con la habitual técnica legislativa, que no siempre permite discernir cuáles normas se hallan en vigencia y cuáles derogadas, no opone barreras políticas a la introducción de normas inconsistentes entre sí y depende, a la postre, del empleo de criterios de preferencia (*lex superior, lex posterior, lex specialis*) que a su vez no se hallan sujetos a un orden unívoco de preferencia o jerarquía”.¹⁶

De esta forma, podemos declarar que este tipo de informática jurídica no pretende modificar el proceso de decisión, ni introducir nuevos supuestos de resolución, ya que sólo “pone de manifiesto las condiciones de la decisión legal y reclamar (por razones estrictamente tecnológicas) un cumplimiento más estricto de ellas”,¹⁷ lo cual permite que las resoluciones estén libres de imprecisiones o valoraciones personales.

Sin embargo, se debe aclarar que el uso de las computadoras y de programas computacionales como auxiliares en el proceso de impartición o administración de justicia presenta la oportunidad de “adoptar en casos diferentes numerosas decisiones, de manera previsible, confiable y extremadamente rápida”,¹⁸ aun cuando implica la solución del gran problema de “determinar el tipo de problema a resolver, establecer los límites a la diversidad de los casos, explicitar todos los criterios a emplear en las decisiones y, al menos en principio, atenerse a los resultados”.¹⁹

La informática es un instrumento al servicio del derecho y debe contribuir a acelerar y hacer más eficientes las labores tradicionales del jurista.

¹⁵ Guibourg, Ricardo A., *op. cit.*, nota 13, pp. 155 y 156.

¹⁶ *Ibidem*, p. 156.

¹⁷ *Ibidem*, pp. 156 y 157.

¹⁸ *Ibidem*, p. 159.

¹⁹ *Idem*.

Pero es más que un instrumento en la medida que ofrece resultados que no sería posible obtener de otro modo.²⁰

Por lo anterior, en la actualidad es impensable el diseñar un programa que ejecute el procedimiento completamente, ya que es indispensable el razonamiento humano para valorar e interpretar una gran diversidad de hechos o situaciones que se pueden presentar; sin embargo, se han establecido criterios respecto a las funciones específicas en las que puede ser de gran utilidad para el juzgador, como lo es el establecimiento de la pena en materia penal, o la cuantificación de los daños y perjuicios solicitados en un caso específico.

En adición, es importante volver a recalcar que la informática jurídica decisoria no pretende sustituir al factor humano dentro del poder judicial, ya que éste aporta un gran valor, sino que sólo se desea que éste sea apoyado con diversas herramientas que ayuden a asegurar que la justicia es imparcial.

Es menester señalar que la máquina nunca podrá reemplazar totalmente al ser humano; sí puede sustituir trabajos, pero no reemplazarlo totalmente. Es difícil que un sistema tome decisiones jurídicas porque no tiene el mismo razonamiento que un ser humano. En informática se denomina sistema experto al programa capaz de actuar, al menos en cierta medida, como un experto para la solución de determinados problemas, lo que es llamada inteligencia artificial.

Asimismo, Guibourg, Alenda y Campanella opinan: “Un sistema informático para resolver casos de homicidio es poco probable ... para calcular el tiempo de prisión en función de las condiciones habitualmente consideradas por los jueces podría prestar gran utilidad”.²¹

La informática jurídica decisoria se basa en el principio de que las TIC faciliten la información adecuada al jurista para ayudarlo a tomar decisiones correctas. La gran cantidad de información existente constituye una explosión documental y es la que ha dado origen a esta nueva necesidad, de ordenar y sistematizar la misma, ya que se debe contar con procedimientos expeditos que nos permitan recuperar la información necesaria en el momento adecuado.

De esta necesidad han nacido los sistemas expertos legales que son programas capaces de efectuar análisis jurídico; vale decir, es aquel sistema mecanizado capaz de organizar procesos y analizar automáticamente un

²⁰ García Barrera, Myrna Elia, *Derecho de las nuevas tecnologías*, México, Instituto de Investigaciones Jurídicas, UNAM, 2011, p. 99.

²¹ Guibourg, Ricardo A., *op. cit.*, nota 13, p. 160.

cúmulo de información y conocimientos produciendo para el usuario una caracterización deontológica de la acción que debe ejecutar. En otras palabras, un consejo o una guía sobre la acción que debería realizar en forma pertinente y funcional.

Pero, además, más allá del propio proceso judicial y la integración de las figuras de la sentencia y el auto definitivo dentro del mismo, se identifican los elementos que pueden tener un impacto en el conocimiento y, específicamente, en el proceso judicial, respecto de las resoluciones y toma de decisiones como aspectos con alto impacto en las culturas organizacionales y sociales, en los que podrían intervenir elementos de análisis y generación de conocimiento –más que de información– como sistemas expertos, de inteligencia artificial o redes somáticas y neuronales, y que podrían implicar la intervención y control de decisiones de forma ciertamente automatizada con impacto social más allá de aspectos del proceso electrónico, requiriendo de una amplia colaboración y consenso multilateral, jurídico, técnico, semántico, organizacional y social.²²

Es claro el compromiso de las instituciones de sistemas de justicia a modernizarse, en cuanto al uso de las TIC, para dos objetivos, primordialmente: mejorar el acceso a la justicia, forjar un acercamiento con la comunidad a través del acceso a información legal y, en general, mejorar la organización del trabajo y productividad del sistema de impartición de justicia.

En otras palabras, se ha señalado que la “...e-justicia, es decir, el uso de las tecnologías de la información y el conocimiento en la administración de justicia (sic) puede suponer importantes beneficios en el funcionamiento de la administración de justicia: los profesionales de la justicia pueden ahorrar tiempo y trabajo; el gobierno y la administración de justicia pueden obtener mayor información y transparencia sobre el funcionamiento de la justicia, y ofrecerla de manera más eficaz y eficiente; los justiciables pueden relacionarse directamente con la justicia, lo que les puede facilitar el acceso a la misma; los usuarios de la justicia pueden suponer una mayor eficiencia en el tratamiento de los casos, un ahorro de tiempo, una disminución de los costos y un mejor acceso a una justicia de mayor calidad. En general, la e-justicia puede facilitar que los ciudadanos la tengan más cerca y que se pueda acercar también a determinados colectivos (inmigrantes, personas con bajo nivel cultural, discapacitados).²³

²² Cfr. Jiménez, Carlos E., *op. cit.*, nota 2, pp. 6 y 7.

²³ Lillo Lobos, Ricardo, *El uso de nuevas tecnologías en el sistema judicial: experiencias y precauciones*. Esta publicación se basa fundamentalmente en otra investigación realizada por el autor para el Centro de Estudios de Justicia de las Américas, y que fuera presentada durante el VIII Seminario de Gestión Judicial realizado en la ciudad de Brasilia, entre los días 29 a

III. INTEROPERABILIDAD

La noción de interoperabilidad refiere a la capacidad de los sistemas de información y, por ende, de los procedimientos a los que éstos dan soporte para compartir datos y posibilitar el intercambio de información y trámites eficaces vía electrónica.

La idea de la interoperabilidad domina hoy en día, si bien sólo para los servicios en que resulta útil. Su puesta en práctica es muy compleja y requiere la integración de numerosas actuaciones y medidas técnicas a fin de garantizar a los ciudadanos la seguridad de los intercambios.²⁴

La interoperabilidad es, según las redes temáticas, la habilidad de un sistema o producto para trabajar con otros sistemas o productos sin esfuerzo especial de parte del usuario, asegurando que el propio sistema se interrelacione con otros para llegar al objetivo previsto.

Es menester señalar que la implementación de iniciativas de interoperabilidad es muy compleja –pero necesaria–, y en el ámbito de justicia, lejos de ser una excepción, esta complejidad puede acentuarse debido a que entran en juego instituciones relacionadas con el Poder Legislativo, el Poder Ejecutivo y el propio Poder Judicial y, por lo tanto, la gobernanza de la interoperabilidad juega un papel aún más determinante por el principio de jerarquía normativa. Como no podía ser de otro modo, se necesita de cobertura legislativa específica y amplia que respalde adecuadamente los procesos electrónicos en el ámbito de la justicia electrónica.²⁵

La norma ISO 16100 define la interoperabilidad del *software* industrial como la habilidad de compartir información usando sintaxis y semánticas comunes

30 de noviembre de 2010, <http://www.ijjusticia.org/docs/LOBOS.pdf>. Consultada el 6 de enero de 2015.

²⁴ Dictamen del Comité Económico y Social Europeo sobre la “Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Plan de Acción Europeo sobre Administración Electrónica 2011-2015. Aprovechamiento de las TIC para promover una administración pública inteligente, sostenible e innovadora” y la “Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Hacia la interoperabilidad de los servicios públicos europeos. COM (2010) 744 final” (2011/C 376/17). Ponente: Raymond Hencks, *Diario Oficial de la Unión Europea*, p. C 376/93, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:376:0092:0096:ES:PDF>. Consultada el 15 de mayo de 2014.

²⁵ *Cfr.* Jiménez, Carlos E., *op. cit.*, nota 2, pp. 11 y 12.

para cumplir una relación funcional de una aplicación específica a través del uso de una interfaz común.²⁶

El real decreto español número 4/2010,²⁷ del 8 de enero de 2010, regula el esquema de interoperabilidad en el ámbito de la administración electrónica, en el propio país español y define a la interoperabilidad como: la capacidad de los sistemas de información y, por ende, de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

La interoperabilidad se entenderá contemplando sus dimensiones organizativa, semántica y técnica. La cadena de interoperabilidad se manifiesta en la práctica, en los acuerdos interadministrativos, en el despliegue de los sistemas y servicios, en la determinación y uso de estándares, en las infraestructuras y servicios básicos de las administraciones públicas y en la publicación y reutilización de las aplicaciones de las administraciones públicas, de la documentación asociada y de otros objetos de información. Todo ello sin olvidar la dimensión temporal que ha de garantizar el acceso a la información a lo largo del tiempo.

Interoperabilidad organizativa. Es aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.²⁸

Interoperabilidad semántica. Es aquella dimensión de la interoperabilidad relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.²⁹

Interoperabilidad técnica. Es aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración

²⁶ “La Interoperabilidad del software y aplicaciones en redes de empresas. La red de excelencia INTEROP”, *Revista del Instituto Tecnológico de Informática*, p. 19, <http://www.iti.es/media/about/docs/tic/11/articulo3.pdf>. Consultada el 20 de mayo de 2014.

²⁷ <http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf>. Consultada el 22 de mayo de 2014.

²⁸ Real decreto 4/2010, del 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. Boletín Oficial del Estado, núm. 25. De fecha 25 de enero de 2010. Sección I, p. 8155, <http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf>. Consultada el 25 de mayo de 2014.

²⁹ *Idem.*

de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.³⁰

Interoperabilidad en el tiempo. Es aquella dimensión de la interoperabilidad relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas; se manifiesta especialmente en la conservación de la información en soporte electrónico.³¹

Interoperabilidad de la web 3.0. Es fundamental para las exigencias de nuestros tiempos, ya que entre otras cosas ofrece: actualizaciones automáticas, trabajar y avanzar en los documentos electrónicos desde cualquier parte y resguardarlo en el cómputo en la nube.

En estos tiempos la interoperabilidad es una exigencia de la forma en que se obtiene información y se hacen los trámites en los ámbitos privados y lo que realizamos en la web 2.0 y 3.0 en donde, de manera rapidísima, obtenemos datos, información y conocimientos; esto nos obliga a tomar estas ventajas en lo que llamamos justicia electrónica, específicamente en el tribunal virtual del estado de Nuevo León.

IV. TRIBUNAL VIRTUAL EN NUEVO LEÓN

La administración de justicia en México requiere, por disposición constitucional, ser pronta y expedita, lo que puede lograrse mediante la incorporación de la tecnología en asuntos que por su naturaleza permitan el libre acceso a las partes en el proceso, a las autoridades o a terceros extraños que tiene que ver con el negocio, ya que las TIC facilitan el acceso a toda persona a los servicios en la administración de justicia y favorecen la comunicación bidireccional desde cualquier punto en donde se localice una computadora con acceso a Internet, eliminando los costos de traslado y permitiendo la comunicación vía correo electrónico, mensajes, etcétera, mediante:

- Una adecuada política en administración de justicia.
- Establecimiento de parámetros claros y precisos en el tratamiento de un caso concreto en comparación con otros similares.
- Celeridad en los procesos y procedimientos, mediante la opción de mecanismos alternativos de solución de conflictos diseñados y operados a través de una administración de justicia electrónica.

³⁰ *Idem.*

³¹ *Idem.*

- La disposición de los medios electrónicos y la tecnología para hacer eficientes los mecanismos de notificación y llamamientos a juicio, así como del desahogo de los asuntos jurisdiccionales.

Estos objetivos pueden ser llevados a cabo a través de:

1. El establecimiento de una comunicación eficaz entre los órganos jurisdiccionales, las partes involucradas en el proceso y los terceros involucrados en él.
2. Definir parámetros y criterios de evaluación y atención en el servicio de la administración de justicia, determinando y computando los plazos establecidos por la ley para la resolución de algunos asuntos de prioridad.
3. Implementar mecanismos de auxilio a la administración de justicia como órganos de solución alternativa de conflictos mediante su implementación en Internet.
4. Generar y crear un sistema de base de datos que permita las notificaciones, llamamientos a juicio, citaciones, resoluciones y recepción de probanzas en procesos de jurisdicción judicial.
5. Establecimiento de un sistema de disposición de información eficiente y eficaz.
6. Implementación de un sistema de Internet en materia de trámites.
7. Diseñar, implementar e instrumentar un sistema de administración de justicia electrónica en México, tanto a nivel federal como local.³²

En el estado de Nuevo León, en lo relativo al Tribunal Virtual, el Código de Procedimientos Civiles del mismo estado (CPCNL), establece esta figura jurídica en su artículo 44 del título especial, en la cual se define como: “el sistema de procesamiento de información, electrónico o virtual, que permite la sustanciación de asuntos jurisdiccionales ante el Poder Judicial del Estado, conforme a los lineamientos de operación establecidos por el Tribunal Superior de Justicia, a través del reglamento que para tal efecto se emita”.³³

El objeto de este Tribunal Virtual es que la población tenga la facilidad de consultar, desde cualquier lugar que tenga conexión a Internet, los

³² Ramos Salcedo, Irma, *La administración de justicia en línea en México. Una propuesta para su implementación*, pp. 80 a 83, <http://148.202.18.157/sitios/publicacionesite/ppperiod/jurjal/ano22no1/4.pdf>. Consultada el 27 de mayo de 2014.

³³ <http://www.pjenl.gob.mx/pdf/pjenl-codigo-procedimientos-civiles.pdf>. Consultada el 25 de mayo de 2014.

acuerdos, promociones y documentos de los expedientes que la o las personas autorizadas tengan acceso, de conformidad con las reglas que la ley establece para esos efectos.

Es así que el Tribunal Virtual es un sistema electrónico o virtual que permite llevar a cabo trámites y consulta relativos a un expediente o caso judicial en específico. Para que esto sea posible, es necesario que el demandante establezca dentro de su escrito de demanda su intención de utilizar dicho tribunal como medio para la sustanciación del procedimiento, lo cual también aplica para el demandado, quien efectuaría dicha solicitud en el escrito de contestación.

Dichas autorizaciones se encuentran condicionadas a la autorización a que se refiere el artículo 78 del mencionado CPCNL.³⁴ Es importante mencionar que esta solicitud se puede realizar en cualquier momento del procedimiento mediante un escrito a la autoridad que está estudiando el expediente.

La solicitud y autorización antes mencionadas no limitan a las partes a utilizar dicho medio como la única vía para presentar las promociones que crea conveniente al juzgado, sino que se reserva el derecho de entregar de forma personal los mismos en las instalaciones del juzgado respectivo.

Dentro de las facilidades que brinda esta herramienta se encuentra la consulta de un expediente, respecto de los acuerdos publicados, de las promociones e instructivos, entre otros. La única limitante que se establece para tener acceso al contenido de los documentos antes mencionados es que se tenga autorización para consultar dicho expediente.

Por su parte, el artículo 46 del ya mencionado código,³⁵ establece los requisitos que debe observar la solicitud que se efectúa para poder presentar

³⁴ Que a la letra señala: Artículo 78 (Reformado, P.O. 26 de diciembre de 2011). Las notificaciones personales realizadas electrónicamente a través del Tribunal Virtual se tendrán por legalmente practicadas y surtirán sus efectos en los términos de lo previsto por el artículo 76, ubicado en el Capítulo V, Título Primero del Libro Primero de este Código. Lo anterior se tendrá en cuenta para el cómputo de términos judiciales conforme a las leyes aplicables.

³⁵ Artículo 46 (Adicionado, P.O. 14 de enero de 2005). Para efectos de presentar cualquier tipo de promoción mediante el Tribunal Virtual se deberán observar los siguientes requisitos: I. Presentar escrito dirigido a la autoridad que conoce del asunto, debiendo señalar el nombre del usuario y nombre completo con el cual se registró en el Tribunal Virtual, firmada por el representante legal o por cualquiera de las partes; (Reformada, P.O. 26 de diciembre de 2011). II. Manifestar claramente su solicitud de presentar promociones vía electrónica, como lo indica el Artículo 78 de este Código. III. Hacer mención expresa del número de expediente en el cual solicita la autorización. IV. Tratándose de varios interesados se deberá señalar sus respectivos nombres de usuarios, siempre y cuando estén autorizados en el expediente para oír y recibir notificaciones. V. Deberá presentarse una solicitud por expediente.

cualquier promoción mediante el Tribunal Virtual. El primero de ellos es que se presente por escrito firmado por el representante legal o cualquiera de las partes ante la autoridad judicial que lleva el expediente, mencionando el nombre del usuario y nombre completo con el cual se registró en dicho Tribunal Virtual;³⁶ igualmente debe establecer de manera clara la solicitud para llevar a cabo promociones vía electrónica y que pueda ser notificado por la misma vía, de conformidad con el artículo 78 del CPCNL, así como mencionar el número de expediente para el cual se solicita esta autorización.

En caso de que se quiera autorizar a varias personas, se deben mencionar los nombres de dichas personas con sus respectivos nombres de usuarios, siempre y cuando estén autorizadas en el expediente respectivo señalado para oír y recibir notificaciones.

Tras la presentación de la solicitud, la autoridad judicial verificará la información, y actuará de conformidad con los artículos 34 y 52 del CPCNL, y en su caso autorizará el acceso.

Para esto se publicará el acuerdo correspondiente a la promoción. Este lo podrá consultar en la opción de “Acuerdos”. Después de hacer llegar la promoción al juzgado solicitando la autorización de un expediente ellos (los abogados o los justiciables, en su caso) tienen un lapso de 72 horas para generar el acuerdo correspondiente a esa promoción. En el acuerdo generado se menciona si se le autorizó o no la consulta del expediente a través de este portal. El acuerdo lo puede ver en la lista de acuerdos (opción “Acuerdos”).³⁷

Finalmente, el segundo título especial establece en su artículo 48, las siguientes definiciones:

Promoción electrónica: es una promoción redactada y enviada a través del sistema Tribunal Virtual.

Usuario: es una clave elegida por el interesado en el proceso de su registro para acceder e interactuar en el sistema Tribunal Virtual que será la identificación del interesado en el sistema.

Contraseña: es una clave elegida por el interesado en el proceso de su registro con la que, en combinación con el usuario, dará acceso a la información establecida y autorizada en el sistema Tribunal Virtual.

Firma electrónica: es la información en forma electrónica consignada en un mensaje de datos, adjuntados o lógicamente asociados al mismo por cual-

³⁶ Se debe hacer dicha mención de manera exacta de cómo se registró, mencionando cuándo se ha escrito con mayúsculas y minúsculas.

³⁷ <http://www.tribunalvirtual.nl.gob.mx>. Consultada el 24 de mayo de 2014.

quier tecnología, que son utilizados para identificar al firmante en relación con el mensaje y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Página electrónica: son las pantallas de acceso de los sistemas computacionales que mediante Internet publica el Poder Judicial del Estado.

Acción electrónica: es cualquier consulta, envío de información o interacción que se realicen en las páginas electrónicas del Tribunal Virtual del Poder Judicial del Estado.

Notificación electrónica: proceso mediante el cual se dan a conocer las actuaciones judiciales realizadas en los procesos civiles, familiares y de jurisdicción concurrente a los usuarios del Tribunal Virtual que así lo hayan solicitado.

Expediente electrónico: es el conjunto de documentos digitalizados, promociones electrónicas y resoluciones realizadas en los sistemas del Poder Judicial, almacenados en sus bases de datos siendo una copia fiel del expediente físico.

Administrador: persona u órgano que conforme a lo indicado en este título es encargado de realizar una función de servicio, control, monitoreo, estadística o de naturaleza análoga, dentro de la estructura del Tribunal Virtual, ya sea de orden administrativo o técnico.

Servicios: funciones del Tribunal Virtual que serán determinadas por el administrador del sistema, controlada por él y debidamente identificadas para beneficio de los usuarios.

Consulta electrónica: acto mediante el cual un usuario revisa la información que se encuentra en la base de datos del Tribunal Virtual a la cual se le ha permitido el acceso.

Recepción electrónica: momento en el cual queda registrado en el sistema la entrega electrónica de una o varias solicitudes generadas por un usuario previamente autorizado para ello, lo que se reflejará en una medida de tiempo de horas, minutos y segundos, indicando igualmente la fecha calendario.

Módulo: ventana o página electrónica, externa (para usuarios) o interna (para servidores públicos), que forma parte del Tribunal Virtual, permitiendo la realización o uso de un servicio, a través del usuario y contraseña adecuado.

Autorización: es el consentimiento explícito del administrador a través de una acción electrónica dentro del mismo sistema, que permite al usuario solicitante realizar una función determinada. Esta autorización será realizada por quien tiene facultades para ello.

Replicación: momento en el cual el sistema actualiza la información diaria para agregar las actuaciones judiciales que se han realizado en un periodo ordinario de tiempo.

Generación de resoluciones: es la producción de los proyectos de decretos, autos o sentencias, a través de los módulos internos del sistema para la revisión y firma del titular del tribunal correspondiente.³⁸

³⁸ <http://www.pjenl.gob.mx/pdf/pjenl-codigo-procedimientos-civiles.pdf>. Consultada el 25 de mayo de 2014.

Actualmente, debemos aceptar que la implementación del Tribunal Virtual en el Estado ha traído varios beneficios, tanto para el poder judicial, como para la población. Entre éstos se encuentran la reducción del número de las visitas a los juzgados, la cual se traduce en una disminución de tiempo para la consulta de uno o varios expedientes, ya que se realiza desde la comodidad de cualquier lugar del mundo y, en especial, del despacho del abogado o del domicilio del justiciable. Además, también se reflejan ventajas para el personal del juzgado, como un mejor manejo del tiempo, lo cual se traduce en la agilización de los procesos.

La justicia electrónica se podrá analizar desde la vertiente de la informática jurídica decisoria, debido a que la informática jurídica se ha ocupado también del campo de la decisión, no es necesario que el sistema se ocupe de la decisión, sino simplemente puede ser una ayuda a la decisión que se puede dar en varios planos y niveles, lo que le servirá al juzgador, al dictar su sentencia.

Todos estamos conscientes de que nuestro país ha cambiado debido a los avances tecnológicos que van incrementándose conforme el paso del tiempo y con la utilización de la TIC, pero ahora debemos conocer si se está cumpliendo con lo mencionado en el subtema de la interoperabilidad.

El derecho, la legislación y la tecnología deben ir evolucionando juntos. Por ello, debemos implementar la sustanciación de procesos judiciales, porque requerimos de un intercambio de documentación e información con distintas dependencias y entidades de gobierno y con empresas del sector privado, las cuales son requeridas por órganos jurisdiccionales a través de diferentes medios de comunicación. Uno de estos medios de comunicación es el llamado oficio.

En la gestión judicial, la generación, entrega y contestación de este medio, se realiza de manera impresa y con firma autógrafa, lo que hace que su trámite y ejecución sea indeterminado en tiempo. Además, es el beneficiario de la actividad jurisdiccional (abogado postulante) quien normalmente realiza la entrega de dicho documento a su destinatario.

Tomando como punto de partida las herramientas tecnológicas existentes y lineamientos del Código de Procedimientos Civiles (CPCNL) y el de Procesal Penal (CPPNL), el Pleno del Consejo de la Judicatura del Estado de Nuevo León ha considerado el desarrollo de un proyecto de mejora que optimice y acorte los tiempos de los procesos judiciales, autorizando al efecto la implementación de una nueva herramienta tecnológica que permita la generación y envío de oficios por medios electrónicos y autenticados a través de un mecanismo de firma electrónica, permitiendo además que la respuesta a dicho oficios se verifique de igual forma.

La implementación de este proyecto generará grandes beneficios ya que agilizará la administración de la justicia; además, tanto las instituciones de gobierno como el Poder Judicial contarán con un mecanismo para el mejor aprovechamiento y economía de sus recursos.

Sin perder el objetivo de que a través de los proyectos de Gobierno Electrónico se propone un nuevo modelo relacional e interactivo de gobierno cuyo reto consistirá en garantizar la gobernabilidad de las sociedades, esta gobernabilidad será posible en la medida que la acción política, social y económica sea capaz de formularse de manera consensuada teniendo presentes las necesidades y demandas del conjunto de la sociedad para ofrecer respuestas y resultados adecuados que permitan resolver los problemas, cada vez más complejos, de manera efectiva. Sólo así será posible recuperar la legitimidad y la confianza en las instituciones públicas, por lo que es menester enfatizar que las TIC son herramientas para lograr dicho modelo.³⁹ Los beneficios a considerar serán los siguientes:

- Eliminación de tiempos muertos o periodos de espera en el proceso judicial derivados de la solicitud, generación, envío y recepción de oficios.
- Eliminación de impresiones de oficios de petición y de oficios de respuesta.
- Eliminación de la gestión personal que realizan los abogados litigantes, actuarios o demás interesados en el proceso.
- Transparencia y certeza jurídica en la autenticación de los documentos.

Pero para la implementación de la presente interoperabilidad se requiere de seguridad jurídica y tecnológica. Por lo que respecta a la seguridad jurídica señalaremos que el mecanismo de comunicación electrónica oficial e intraprocesal está soportado en el CPCNL y el CPPNL, dado que su operación se contempla en esas codificaciones:

CPCNL. De los medios de comunicación en el proceso.

Artículo 79. Cuando se ordenen medios de comunicación en procesos llevados ante tribunales del Estado, podrán enviarse a través del sistema Tribunal Virtual. Estos documentos serán generados con la información contenida

³⁹ Criado Grande, J. Ignacio, Ramilo Araujo, María Carmen y Salvador Serna, Miquel, *op cit.*, p. 45. [http://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Comercio%20Electronico/la-necesidad-de-teoria\(s\)sobre-gobierno-electronico-una-propuesta-integradora.pdf](http://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Comercio%20Electronico/la-necesidad-de-teoria(s)sobre-gobierno-electronico-una-propuesta-integradora.pdf). Consultada el 6 de enero de 2015.

en la base de datos. Cuando se trate de exhortos o despachos se generará un expediente electrónico independiente al juicio de donde se derive.⁴⁰

CPPNL Comunicación entre autoridades.

Artículo 52. Los Tribunales, al dirigirse a las autoridades o funcionarios, lo harán a través de los medios que garanticen el conocimiento del acuerdo emitido.⁴¹

Ahora bien, para la implementación interpretativa el Tribunal Superior de Justicia y el Consejo de la Judicatura deberán celebrar convenios con dependencias públicas federales, estatales o municipales, a fin de determinar que las comunicaciones entre ellos, jueces o tribunales, se realicen a través de medios o métodos electrónicos que garanticen su autenticidad, conservación, integridad, así como la debida interoperabilidad entre sus tecnologías.

Para la materialización de este nuevo mecanismo de comunicación se ha diseñado un sistema donde los tribunales, al momento de dictar la resolución, puedan seleccionar las dependencias a las que se les ordena girar oficio, de modo que en forma automática al momento de terminar su lista de acuerdos y publicarla en el boletín judicial, se generen, firmen y envíen electrónicamente dichos oficios al portal de Internet donde las dependencias gestionarán su contestación.

Instalado el sistema, el proceso inicia cuando en el juzgado genera el acuerdo o resolución ordenando la comunicación por oficio a diferentes dependencias o entidades de gobierno y al enlistar el documento para su publicación.

El presente proyecto constituye un primer paso por parte del Poder Judicial del Estado de Nuevo León, en el establecimiento de esquemas de interoperabilidad con otras instituciones públicas y privadas, con sistemas y procesos que dan soporte y facilitan el intercambio de información con seguridad y agilidad.

Los beneficios de este proyecto representarán una disminución del tiempo en los procesos judiciales, mayor eficiencia en el personal que tramita los juicios, celeridad en la contestación de oficios y mayor certeza en la emisión y contestación de las comunicaciones procesales oficiales. Además, se considera que el proyecto será una garantía adicional del cumplimiento cabal al mandato constitucional que impone administrar justicia pronta y expedita, y así cumplir con las disposiciones constitucionales al respecto.

⁴⁰ <http://www.pjenl.gob.mx/pdf/pjenl-codigo-procedimientos-civiles.pdf>. Consultada el 25 de mayo de 2014.

⁴¹ <http://www.pjenl.gob.mx/pdf/pjenl-codigo-procesal-penal.pdf>. Consultada el 25 de mayo de 2014.

V. CONCLUSIONES

Primera. La informática y las TIC, en relación con el derecho, tienen el objetivo –entre otros– de facilitar que toda persona conozca las diversas legislaciones que regulan su conducta externa en la sociedad, y cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de señales digitalizadas, se infiltra –si bien con diversos ritmos e intensidad, pero de modo inexorable– en servicios, productos y procesos existentes, genera nuevos bienes y actividades; ocasiona cambios fundamentales, entre otros órdenes, en los patrones de producción y comercio internacionales, los métodos de gestión y la organización administrativa, y la defensa.

Segunda. El encuentro entre el derecho y las ciencias relacionadas con la TIC debe propiciar la evolución del gobierno electrónico a fin de facilitarle al usuario, el o los trámites que se prestan de manera presencial con la misma virtud de funcionar bien, para otorgar un servicio de calidad y acorde a los tiempos actuales y beneficiar a las personas que habitan nuestro estado y país.

Tercera. El Tribunal Virtual de Nuevo León es un sistema electrónico o virtual que permite consultar los expedientes, mandar promociones, realizar notificaciones, recibir en el teléfono móvil un mensaje si el expediente en cuestión ha tenido algún acuerdo. Esto es sólo el inicio de la utilización de las nuevas tecnologías en la impartición de justicia.

Cuarta. Son claros los beneficios de la interoperabilidad que están iniciando en el Tribunal Virtual, porque repercuten de forma directa e indirecta en la sociedad y en el cumplimiento de la responsabilidad de impartición de justicia pronta y expedita. La informática decisoria suele presentarse como una colección de métodos, medios y propuestas para auxiliar al juzgador en su tarea, antes que para reemplazarlo.

VI. BIBLIOGRAFÍA

- FALCÓN, Enrique M., *¿Qué es la informática jurídica? Del ábaco al derecho informático*, Abeledo-Perrot, Buenos Aires, 1992.
- FIX FIERRO, Héctor, “Informática y documentación jurídica”, *Revista de la Facultad de Derecho*, 1996.
- GARCÍA BARRERA, Myrna Elia, *Derecho de las nuevas tecnologías*, México, Instituto de Investigaciones Jurídicas, UNAM, 2011.

GUIBOURG, Ricardo A., ALENDE, Jorge O. *et al.*, *Manual de informática jurídica*, Argentina, Astrea, 1996.

JORDÁN FLORES, Fernando, *Las nuevas tecnologías y el derecho y la justicia*, Bogotá, Colombia, Servigraphic, LTDA, 2000.

LA PROTECCIÓN DE LOS DATOS DIGITALES. UNA LECTURA DE LA TENSIÓN DEL *HABEAS DATA* EN EL CONTEXTO DEL CAMBIO DE LAS RELACIONES SOCIALES QUE SUPONE INTERNET

Fredy Alexander PRADA V.*
Carolina VELANDIA H.**

SUMARIO: I. *¿Qué es la sociedad de la información y cuál es el rol del Estado, de los derechos humanos, especialmente del habeas data como mecanismo de protección de datos y de los usuarios en Internet.* II. *Las relaciones entre el Estado, los usuarios en el contexto de la Sociedad de la Información y los cambios tecnológicos. Una lectura desde Luhmann.* III. *Conclusiones.* IV. *Bibliografía.*

I. QUÉ ES LA SOCIEDAD DE LA INFORMACIÓN Y CUÁL ES EL ROL DEL ESTADO, DE LOS DERECHOS HUMANOS, ESPECIALMENTE DEL *HABEAS DATA* COMO MECANISMO DE PROTECCIÓN DE DATOS Y DE LOS USUARIOS EN INTERNET

La explicación de ciertos fenómenos sociales no debe desatender los fundamentos en virtud de los cuales tales fenómenos adquieren una relativa transparencia ante nuestros ojos; por el contrario, nuestro esfuerzo para llegar a tener una visión de mayor profundidad sobre ciertos fenómenos parece avocarnos constantemente a esta visión retrospectiva sobre el objeto de nuestra investigación.

* Abogado egresado de la Universidad Nacional de Colombia, investigador y escritor en temas de derecho, en la actualidad se desempeña como consultor independiente.

** Abogada egresada de la Universidad Nacional de Colombia, magister en negociaciones económicas internacionales de la Universidad Andina Simón Bolívar, especialista en derecho minero y petrolero de la Universidad Externado de Colombia, en la actualidad se desempeña como abogada en el sector petrolero.

Intentamos plantear brevemente los límites que demarcan nuestra discusión. Nuestro análisis tocará el problema del derecho, por tanto, deberá tomar en cuenta dos tipos de consideraciones que comprometen a la idea de derecho tal como la conocemos. De este modo hablaremos del derecho frente al Estado, pero también hablaremos del derecho como conjunto de comunicaciones sometidas a determinados protocolos que resultan propios de las ciencias jurídicas, que adquieren un poco de transparencia a la hora de pensar en la relación del Estado frente a sus pobladores. Por lo tanto, hablaremos de poder y de aquella parte del poder que, operando de un modo rutinario conforma el derecho, y al tiempo, contando con que son fenómenos en el mundo que se encuentran sometidos a un fenómeno particular que son las nuevas tecnologías de la comunicación. Así, terminaremos analizando fenómenos como los cambios en la comunicación que suponen las tecnologías imperantes para los Estados y para sus sistemas de regulación de la vida social, esto en el contexto del derecho de cada Estado.

Para comenzar presentamos algunas nociones de sociedad de la información, que brinden mayores enfoques académicos del horizonte sobre el cual se enmarca la discusión del presente escrito.

La Comisión Económica para América Latina y el Caribe (Cepal), en el texto *Los caminos hacia una sociedad de la información en América Latina y el Caribe*, define la sociedad de la información en los siguientes términos:

El concepto de la sociedad de la información hace referencia a un paradigma que está produciendo profundos cambios en nuestro mundo al comienzo de este nuevo milenio. Esta transformación está impulsada principalmente por los nuevos medios disponibles para crear y divulgar información mediante tecnologías digitales. Los flujos de información, las comunicaciones y los mecanismos de coordinación se están digitalizando en muchos sectores de la sociedad, proceso que se traduce en la aparición progresiva de nuevas formas de organización social y productiva. Esta “actividad digital”, que se va convirtiendo poco a poco en un fenómeno global, tiene su origen fundamental en las sociedades industrializadas más maduras. De hecho, la adopción de este paradigma, basado en la tecnología, está íntimamente relacionado con el grado de desarrollo de la sociedad. Sin embargo, la tecnología no es sólo un fruto del desarrollo (por ser consecuencia de éste), sino también, y en gran medida, uno de sus motores (por ser una herramienta de desarrollo).¹

¹ Comisión Económica para América Latina y el Caribe (Cepal), *Los caminos hacia una sociedad de la información en América Latina y el Caribe*, julio de 2003, Naciones Unidas, p. 1, http://repositorio.cepal.org/bitstream/handle/11362/1836/S0015K19_es.pdf?sequence=1. Fecha de consulta, 30 de diciembre de 2014.

Delia Cروي Druetta plantea en su publicación, *Sociedad de la información y el conocimiento. Entre el optimismo y la desesperanza*, lo siguiente:

De manera general entiendo por sociedad de la información, SI, a una sociedad caracterizada por un modo de ser comunicacional que atraviesa todas las actividades (industria, entretenimiento, educación, organización, servicios, comercio, etcétera). En este tipo de organización social la información ocupa un lugar sustantivo y se convierte en fuente de riqueza (Miége, 1998). Se produce un crecimiento rápido de las tecnologías de información y comunicación, TIC, las que repercuten en todos los sectores sociales. En efecto, a pesar de haber grandes diferencias en el acceso a estas nuevas tecnologías entre las naciones y entre los individuos, todos los países tienen al menos una franja de su sociedad que las han integrado a sus actividades. La mayoría de esos desarrollos tecnológicos (tanto su parte dura, *hardware*, como en su parte blanda o lógica, *software*) se producen en los países del primer mundo.²

La Cepal, en el texto *Report of the Round Table on Telecommunications and the Knowledge Society*, se encarga de analizar el caso de Trinidad y Tobago en la entrada a la sociedad de la información, y realiza un aporte importante para distinguir la sociedad de la información de la sociedad del conocimiento. Por su relevancia, se cita a continuación:

In differentiating a Knowledge Society from an Information Society, Dr. Kim Mallalieu posited that a knowledge society was one which placed value on knowledge as the means of realizing economic and social well-being. There was the recognition that in such a society, citizens had greater choice and opportunity, deeper social integration and longer life expectancy. Inquiry, research, creativity, the use of modern technology and entrepreneurial leadership were shown to be of great importance. As a result, the critical skills which must be harnessed include literacy, collaboration, innovation, communication, diversity and flexibility. In contrast, information-based innovations were featured as tools for productivity and entertainment in an Information Society, with little or no concern for assimilation, integration nor the application of understanding to innovations.³

² Cروي Druetta, Delia, “Sociedad de la información y el conocimiento. Entre el optimismo y la desesperanza”, *Revista Mexicana de Ciencias Políticas y Sociales*, México, año XLV, núm. 185, mayo-agosto de 2002. Disponible en http://www.miaulavirtual.com.mx/ciencias_sociales/Revista_UNAM/RevistaUnamPDF/RMCPYS%20NUM-185.pdf. Fecha de consulta, 30 de diciembre de 2014.

³ Cepal, “Report of the round table on telecommunications and the knowledge society”, mayo, 2006, Naciones Unidas, p. 3, http://repositorio.cepal.org/bitstream/handle/11362/24895/LCcarL96_en.pdf?sequence=1. Fecha de consulta, 30 de diciembre de 2014.

Aunque no es el objetivo de este documento profundizar en la noción de la sociedad de la información, puede decirse que no existe una única definición, por el contrario, existe una alta problematización de este concepto dados los cambios en el paradigma del conocimiento,⁴ razón por la cual, con el fin de cumplir con los objetivos del presente texto únicamente nos centraremos en resaltar algunos elementos que arrojan las definiciones que rescatamos con anterioridad. Primero, existe un nuevo paradigma en las relaciones económicas, sociales y culturales basado en la tecnología de la información y las comunicaciones. Segundo, este cambio genera procesos de digitalización donde el intercambio de la información es más ágil y adquiere una relevancia económica, social y política. Tercero, las relaciones entre los ciudadanos entre sí, entre los ciudadanos y las instituciones se desarrollan en el marco de este nuevo paradigma.

Por ende, sin importar las diversas concepciones de la sociedad de la información, lo relevante para el presente estudio sobre su noción es la manera en que el derecho busca proteger los elementos arquimédicos esenciales con los cuales se construye el sistema de la información. Es decir, cómo se protege el dato, el código, las centrales de datos y los sujetos como titulares del ejercicio del derecho, los usuarios de la información y las instituciones del Estado que se encargan de la vigilancia de los sujetos y que supuestamente garantizan la protección de los derechos.

Sin desconocer que la constitucionalización, es más, el reconocimiento de los derechos, está atravesado por escenarios de lucha de poder donde las conquistas políticas se traducen en el ejercicio mismo del derecho, es en esta parte inicial que queremos resaltar que introducir al *habeas data* como un derecho surge de la necesidad de la sociedad de proteger la información y de la pugna evidente entre el Estado y los ciudadanos, el primero estableciendo canales de control para garantizar la permanencia de las instituciones, y los segundos como un límite, lo cual plantea la noción de derecho como un límite al accionar del Estado, impone una carga a la administración de respetar los derechos, en este caso los derivados de la puesta en marcha de la sociedad de la información.

Es necesario aclarar de qué noción de derecho partimos. En este punto acogemos la teoría de Valencia Zea, quien explica que la ciencia jurídica define la palabra derecho en dos sentidos principales, recogiendo la escuela

⁴ En este sentido véase Hilbert, Martin y Cairó, Osvaldo, *¿Quo vadis, tecnología de la información y de las comunicaciones? Conceptos fundamentales, trayectorias y estado del arte en los sistemas digitales*, en http://Repositorio.Cepal.Org/Bitstream/Handle/11362/32830/S384q92009_Es.Pdf?Sequence=1. Fecha de consulta, 30 de diciembre de 2014.

positivista del derecho: derecho objetivo y derecho subjetivo. El autor plantea que el derecho en *sentido objetivo* indica el conjunto de normas y preceptos o reglas que gobiernan la vida de los hombres que viven en sociedad:

... Podemos decir, en consecuencia, que el derecho objetivo es el conjunto de códigos (civil, penal, administrativo, de procedimiento, de comercio, etcétera) y leyes no codificadas que rigen la vida social de las personas que forman un pueblo (nación o comunidad). ... En cambio, el derecho en *sentido subjetivo* está referido a las facultades o poderes de que son titulares las personas y que sirven para satisfacer sus necesidades. Siguiendo esta orientación, una persona dice: 'mi derecho de propiedad sobre esta casa', 'mis créditos', 'mi derecho de autor sobre determinada obra intelectual', etcétera.⁵

Ahora bien, el derecho colombiano ha consagrado dos normas principales desde donde se concibe el núcleo esencial del derecho de *habeas data*, las dos disposiciones son las contenidas en los artículos 15 y 20 de la Constitución Política de Colombia. Por su pertinencia, citamos las disposiciones:

Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

Éstos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

La naturaleza jurídica del *habeas data* como derecho autónomo se puede describir en tres facetas: la primera es sustancial, en Colombia corresponde

⁵ Valencia Zea, Arturo y Ortiz Monsalve, Álvaro, *Derecho civil. Parte general y personas*, Colombia, Temis, 2002, p. 7.

a un derecho humano fundamental derivado de la protección del derecho a la intimidad y al buen nombre; en la segunda, a nivel procesal, es un derecho procedimental en el sentido de que puede ser empleado como mecanismo de protección garantizar otros derechos como la dignidad, la libertad y la igualdad, obligando a los jueces y operadores jurídicos a salvaguardar la autodeterminación informativa. La última faceta, que puede considerarse el mayor aporte de la jurisprudencia colombiana, es la construcción del núcleo esencial del derecho de *habeas data*, que lo eleva a rango de derecho fundamental en el ordenamiento colombiano.

En el texto *Guía de mecanismos constitucionales de protección de derechos humanos*, la Oficina en Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, la Unión Europea y la Defensoría del Pueblo, plantean una tesis similar a la nuestra en el sentido de demostrar las dimensiones del derecho de *habeas data* en Colombia. En este sentido, afirman:

Se reitera entonces que la Carta política, en su artículo 15, incluye dentro de los varios conceptos que lo conforman el relativo al buen nombre y al *habeas data*, y que este derecho adquiere una doble dimensión, cuando se configura como derecho fundamental y, además, cuando es herramienta fundamental para la debida defensa por parte de los particulares en relación con la divulgación de informaciones que tengan relación con su buen nombre, su intimidad personal, familiar y su honra. Por ello, la información que se encuentra contenida en bases de datos, sin importar si quien maneja dicha información es una entidad pública o privada, deberá obedecer de manera estricta a la verdad, y los datos allí contenidos se caracterizarán también por su dinamismo, es decir, podrá ser actualizada, para ajustarse a la realidad y a la verdad en la cual se sustenta.⁶

Así las cosas, los casos en los cuales se ha materializado su protección en Colombia tienen una evolución histórica, puede decirse que comienzan con una protección del dato comercial y financiero, luego se extiende a datos sensibles como la información académica, sexual, social, entre otras. Esto ocurre en Colombia desde la década de los años noventa, cuando los instrumentos informáticos se hacen masivos, no sólo para acceder a servicios financieros informatizados sino que en adelante Internet y los sistemas computarizados dinamizaron el funcionamiento social en la relación ciudadanos-Estado, entre particulares como empresas y consumidores, universi-

⁶ Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Unión Europea, Defensoría del Pueblo, *Guía de mecanismos constitucionales de protección de derechos humanos*, Bogotá, 2003, <http://www.hchr.org.co/publicaciones/libros/mecanismos.pdf>. Fecha de consulta, 30 de diciembre de 2014.

dades y estudiantes y, además, se debe incluir que en estas décadas, Colombia inició un fuerte proceso de modernización donde uno de sus principales pilares fue incorporar la sociedad de la información al funcionamiento general del país.⁷

Este contexto permite comprender que la construcción del núcleo esencial del *derecho de habeas data* en Colombia, surge de las problemáticas y conflictos al interior del sistema financiero, donde los deudores morosos y los usuarios cumplidos fueron reportados en centrales de riesgo que penalizaban su incumplimiento, algunos de manera injusta (en el caso de los cumplidos), otros efectivamente habían incumplido sus obligaciones, pero la falta de regulación permitió que las entidades financieras, como los bancos, entre otras, reportaran en las centrales de riesgo sin límite de tiempo a los deudores, generando unas sanciones que aniquilaban la vida crediticia de las personas. Incluso en algunas acciones de tutela (conocida como acción de amparo constitucional en el resto del derecho latinoamericano) se expuso que estas penas o sanciones administrativas (como lo es en el derecho colombiano la inclusión en una central de riesgo) eran impuestas a perpetuidad, por esto las sentencias de la Corte Constitucional colombiana buscaron garantizar el buen nombre, la intimidad, y que los titulares de la información pudieran refutar y controvertir el contenido de la información, sobre todo cuando lo reportado no era veraz o era un error.

En este sentido, es necesario entender la noción de núcleo esencial, como aquella esfera del derecho a la cual el ordenamiento jurídico garantiza su protección e impone el límite hasta el cual puede ser regulado y restringido, una vez que se ingresa en esa esfera por parte del Estado como legislador o en ejercicio de su autoridad, el derecho se ve violentado y vulnerado, por esta razón para cada caso de derecho fundamental la Corte Constitucional colombiana ha definido el alcance del derecho y cuál es su núcleo esencial, dicho en los términos de la Corte:

La Corte ha indicado que respecto de los derechos fundamentales, la reserva de ley estatutaria no se predica de la regulación de todo evento ligado a los derechos fundamentales sino solamente los elementos estructurales esenciales de los derechos fundamentales, de modo que las leyes estatutarias no deben regular en detalle cada variante o cada manifestación de dichos derechos o

⁷ Un análisis del desarrollo de las telecomunicaciones y de la tecnologías de la información se puede observar en el estudio realizado por la Cepal, Serie Estudios y perspectivas, Colombia, núm. 22, “De las telecomunicaciones a las TIC: Ley de TIC de Colombia (L1341/09)”, http://repositorio.cepal.org/bitstream/handle/11362/4818/S110124_es.pdf?sequence=1, pp. 10 y ss. Fecha de consulta, 30 de diciembre de 2014.

todos aquellos aspectos que tengan que ver con su ejercicio; y para definir los elementos estructurales esenciales, la jurisprudencia constitucional se ha valido de la teoría del núcleo esencial, según la cual, los derechos fundamentales tienen: i) un núcleo o contenido básico que no puede ser limitado por las mayorías políticas ni desconocido en ningún caso, ni siquiera cuando un derecho fundamental colisiona con otro de la misma naturaleza o con otro principio constitucional; y ii) un contenido adyacente objeto de regulación. De conformidad con la jurisprudencia constitucional es competencia del legislador estatutario desarrollar aspectos importantes del núcleo esencial, siendo asuntos importantes del núcleo esencial propios de leyes estatutarias: i) la consagración de límites, restricciones, excepciones y prohibiciones de alcance general; y ii) los principios básicos que guían su ejercicio. Otro elemento que puede deducirse a partir de un examen de la estructura de los derechos fundamentales es la definición de las prerrogativas básicas que se desprenden del derecho para los titulares y que se convierten en obligaciones para los sujetos pasivos.⁸

En el caso específico del *habeas data*, la definición del núcleo esencial tuvo origen en los debates jurídicos suscitados en el escenario financiero, en este primer momento según el planteamiento de Diego López,⁹ los jueces afrontaron el problema jurídico de determinar bajo qué condiciones específicas puede una base de datos financiera poseer y divulgar información sobre un deudor sin violar las garantías constitucionales de intimidad y buen nombre. Según la metodología planteada por el autor, que puede sintetizarse en la búsqueda de una línea jurisprudencial donde los jueces construyen razones de derecho, *ratios decidenci*, que sustentan la razón por la cual responden de una manera u otra al problema jurídico. En este caso se presenta la tensión entre los deudores y las entidades financieras, frente a esta primera lectura, aporta López:

La sentencia T-022/92 es una sentencia-hito porque allí Angarita vira la línea más hacia la izquierda de la gráfica y se presenta preparado para afirmar que los deudores están protegidos no solamente por la garantía de intimidad, la cual impide la formación de ‘perfiles virtuales’ que los excluyen de las redes financieras, sino que incluso ‘el ciudadano no puede ser privado de su *derecho de acceso al crédito sin justa causa y observando la garantía del debido proceso*’. Esta

⁸ Corte Constitucional de Colombia, sentencia C-748/11, referencia: expediente PE-032, Control constitucional al Proyecto de Ley Estatutaria núm. 184 del 2010 Senado; 046 de 2010 Cámara, “por la cual se dictan disposiciones generales para la protección de datos personales”. Magistrado ponente: Jorge Ignacio Pretelt Chaljub, Bogotá D. C., 6 de octubre de 2011.

⁹ Cfr. Medina López, Diego Eduardo, *El derecho de los jueces*, 3a. ed., Colombia, Ediciones Uniandes, Legis, 2002.

radicalización no es bienvenida por la mayoría de la corte que ya empieza a desmontarla en la SU-528/93, donde se afirma que los jueces de tutela no pueden dedicarse a verificar por sí mismos la existencia o no de la prescripción de las obligaciones. La prescripción, incluso si no había sido declarada previamente por los jueces civiles, había sido una de las circunstancias en que la corte concedía *habeas data*. Finalmente, el giro hacia la “derecha” se consuma en las sentencias SU-082 y 089 de 1995, allí se insiste que la cuestión no es tanto la “intimidad” del deudor como el derecho a la información de que precisa el sistema financiero para poder asegurar a sus depositantes la calidad del crédito que conceden, los deudores, por tanto, no tienen derecho a la intimidad sino más bien a ‘un buen nombre’ que deben mantener mediante el cumplimiento de sus obligaciones.¹⁰

En razón de la ampliación de casos donde se evidenciaron diferentes formas de violación al *habeas data*, por ejemplo, la situación de los cotizantes al sistema de pensiones en donde el sistema no reporta sus pagos, casos de reportes a las centrales de riesgos con información no veraz o donde se reportan errores, casos de interceptaciones ilegales de comunicaciones, o reportes donde no media la voluntad del titular de la información, la Corte fue enfocando el ámbito de protección, obligando especialmente a los sujetos participantes en la comunicación de la información a una serie de acciones, especialmente ubicando roles de las autoridades, de los jueces y de los ciudadanos, y creando conceptos como la autodeterminación informática:

...La Corte ha afirmado que el principio de libertad en el manejo de datos tiene especial incidencia en la autodeterminación de la información. Al respecto, la Corte ha sostenido que el elemento esencial de la autodeterminación recae sobre el consentimiento. Sobre el particular esta Corporación en la sentencia SU-082 de 1995 se cuestionó: ¿Cuál es el núcleo esencial del *habeas data*? A juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica. La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales. ... En conclusión, compete a los jueces, en cada caso, analizar el contenido de la autodeterminación y el principio de libertad, así como el cumplimiento de los requisitos dispuestos en la ley y la jurisprudencia, a fin de no incurrir en alguna violación de derechos fundamentales. Dichos requisitos se pueden sintetizar en: i) obtener el consentimiento del titular de la información, ii) tal consentimiento deber ser calificado, es decir, expreso, informado y previo, iii) el tratamiento de la información se debe

¹⁰ *Ibidem*, p. 79.

realizar para las finalidades informadas y aceptadas por el titular del dato, iv) responsable del tratamiento le corresponde obtener y conservar la autorización del titular.¹¹

Siguiendo esta evolución en la jurisprudencia, en las sentencias del año 2013 la Corte tiene el suficiente bagaje y plantea una noción de *habeas data*. Para analizar estos cambios jurisprudenciales sobre la comprensión que tiene la Corte del núcleo esencial del *habeas data*, queremos presentar el caso de la sentencia T-058/13 anteriormente citada en la definición de autodeterminación informativa, si bien los efectos de las sentencias de tutela son *inter partes*, este es un ejemplo muy relevante donde se aplica la conexión del derecho de *habeas data* con otros derechos fundamentales como la educación, su aparición no es tan numerosa como los casos frente al sector financiero, a reclamaciones ante entidades del Estado que garantizan el acceso a la seguridad social, los registros de las condenas penales, la relación entre el buen nombre, el derecho a la intimidad y el *habeas data*.

Por esta razón, queremos presentar un caso atípico donde se evidencia la conexión entre el derecho de *habeas data* con el derecho a la educación. Además, en esta sentencia la Corte plantea en extenso la definición del núcleo esencial de *habeas data*, allí se analiza el caso de una estudiante que reclama la protección de sus derechos fundamentales al *habeas data*, a la educación y al buen nombre, presuntamente vulnerados por la “Universidad BB”, toda vez que en las certificaciones de estudio informó las sanciones disciplinarias que le fueron impuestas por plagio. Afirma la actora que al solicitar el ingreso a otra “Universidad CC”, le fue negado, a consecuencia de la expedición de las certificaciones de estudio mencionadas. En este caso la Corte hace una síntesis y explica que el núcleo esencial de derecho de *habeas data* se entiende al mismo tiempo como derecho autónomo y como garantía de derechos conexos, a continuación la explicación de la Corte:

El artículo 15 de la Constitución Política consagra el derecho al *habeas data* entendido como la facultad que tienen los individuos de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Asimismo, estipula la obligación de respetar la libertad y demás garantías constitucionales en el ejercicio de las actividades de recolección, tratamiento y circulación de datos.

¹¹ Sentencia T-058/13. Referencia: expediente T-3623403, Acción de tutela instaurada por AA contra la Universidad BB. Magistrado ponente: Alexei Julio Estrada, Bogotá D.C., 7 de febrero de 2013.

Para la Corte, el *habeas data* es un derecho de doble naturaleza. Por una parte, goza del reconocimiento constitucional de derecho autónomo, consagrado en el artículo 15 de la Constitución y, por otra, ha sido considerado como una garantía de otros derechos. Como derecho autónomo, el *habeas data* tiene un objeto protegido concreto: el poder de control que el titular de la información puede ejercer sobre quién (y cómo) administra la información que le concierne y el poder de su titular de conocer, actualizar, rectificar, autorizar, incluir y excluir información personal cuando ésta sea objeto de administración en una base de datos.

Ahora bien, como garantía de otros derechos puede operar en la medida en que los protege mediante la vigilancia y cumplimiento de las reglas y principios de la administración de datos. Por vía de ejemplo, el *habeas data* opera como garantía del derecho al buen nombre, cuando se emplea para rectificar el tratamiento de información falsa.¹² Opera como garantía del derecho a la seguridad social, cuando se emplea para incluir, en la base de datos, información personal necesaria para la prestación de los servicios de salud y de las prestaciones propias de la seguridad social.¹³ Opera como garantía del derecho de locomoción, cuando se solicita para actualizar información relacionada con la vigencia de órdenes de captura, cuando éstas, por ejemplo, han sido revocadas por la autoridad competente.¹⁴

Sin embargo, y pese a ser el *habeas data* un derecho autónomo, la infracción de este derecho puede acarrear la afectación de más de un derecho fundamental y, particularmente al derecho a la educación cuando se divulgan datos que se refieran a la disciplina, conducta, desempeño académico o aquellos relacionados con la vida del estudiante-titular sin la posibilidad de que éste modifique, conozca, actualice, rectifique o excluya, la información recogida en bases de datos o cualquier otro sistema de almacenamiento. En estos términos, el responsable del dato estudiantil tiene una responsabilidad concurrente frente a la finalidad, veracidad e integralidad del dato, pues a éste le corresponde la obligación de cerciorarse que se cumplan los requisitos para que un dato pueda ser objeto de tratamiento. De no ser así, se configura una violación al derecho a la educación del titular del mismo. Por consiguiente, divulgar al público en general de manera indiscriminada información del

¹² Sentencias T-455 de 1998 y T-949 de 2003. Casos en los cuales el *habeas data* funge como una garantía del derecho al buen nombre frente a situaciones de homonimia y suplantación.

¹³ Sentencia T-486 de 2003. Caso en el cual el *habeas data* funge como garantía de las prestaciones de la seguridad social, mediante la orden a una empresa prestadora del Servicio EPS (en adelante EPS) de incorporar información sobre la afiliación al sistema contributivo, de lo que dependía la concesión de dichas prestaciones.

¹⁴ Sentencia T-310 de 2003. Caso en el cual el *habeas data* funge como garantía del derecho a la libertad personal, mediante la orden de cancelación del registro de orden de captura vigente.

estudiante que el centro educativo haya conocido o conozca con ocasión de sus funciones educativas, constituye una barrera al acceso al derecho de la educación.

A nivel legal, ocurrieron unos cambios que aplicaron la protección de los datos y de la información, se promulgaron dos leyes estatutarias cuyo objeto es la regulación de los derechos y deberes fundamentales de las personas, los procedimientos y recursos para su protección (artículo 152 de la Constitución Política, en adelante CP). La primera de ellas es la Ley Estatutaria 1266 de 2008, cuyo objeto es desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la CP, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

II. LAS RELACIONES ENTRE EL ESTADO, LOS USUARIOS EN EL CONTEXTO DE LA SOCIEDAD DE LA INFORMACIÓN Y LOS CAMBIOS TECNOLÓGICOS. UNA LECTURA DESDE LUHMANN

El *habeas data* supone la existencia de la información como susceptible de afectar los derechos de los asociados. Estos derechos, para Luhmann, se determinan por un sistema social que depende de aportar una información a la sociedad.¹⁵ Esta acción, aquel procedimiento, esta o aquella consecuencia pueden ser jurídicos, acordes con el derecho o no. Con lo que define la perspectiva de Luhmann sobre el eje que permite realizar un conjunto de tareas al derecho: su código.

Por código entiende Luhmann una cierta pregunta que se interpreta en general como definitoria de un género; por ejemplo, en el caso del derecho, el discurso de lo jurídico busca averiguar la conformidad o no con el derecho de hechos, conductas o negocios. Analiza desde los medios de comunicación, la problematización sobre la distinción entre lo comunicable, y su opuesto, lo no comunicable. Desde el contexto del poder, es la posibilidad

¹⁵ Luhmann, Niklas, *Poder*, México, Antropos, Universidad Iberoamericana, 1995.

de generar en “el otro” incertidumbre como consecuencia de una decisión que pende en manos de un sujeto social.

Así las cosas, la teoría luhmanniana de hecho borra a los hombres del objeto mismo de la sociología, dado que ésta se describe como comunicación. En lo que se ha llegado a llamar la sociedad sin hombres, o en palabras de Javier Torres Nafarrete hablando de la teoría social de Luhmann como “cimentada sobre el fundamento de que la sociedad es pura comunicación”.¹⁶ En una perspectiva que, sin contravenir la teoría de la sociedad de la comunicación determinada por la aparición del fenómeno de la bidireccionalidad de la comunicación de Castells,¹⁷ plantearía que de fondo toda sociedad humana es comunicación.

Luhmann no niega la relativa importancia que puedan tener los cambios tecnológicos que introducen nuevas posibilidades comunicativas en la sociedad. Pero centra su atención siempre en el modo como la comunicación conforma, por así decirlo, sus protocolos. Los nuevos problemas jurídicos que introducen las nuevas tecnologías de la computación de la información dependen, no sólo de un cambio interno en el sistema de protocolos informativos, sino en parte como resultado de las ganancias comunicativas que atrae la tecnología. Si las comunicaciones en el entorno de la red generan nuevas formas de interactuar, depende de factores que, como se verá, afectan a la comunicación misma.

En un primer momento las distinciones jurídicas pueden ser descritas como aquellas en las que la intervención del Estado garantizaría determinadas consecuencias. Con lo que el discurso del derecho depende de la sanción del uso de la fuerza por parte del Estado que configura las expectativas legítimas que ocupan para Luhmann el papel de la función del derecho como un sistema de “expectativas de comportamiento contrafacticamente estabilizadas”.¹⁸

Un primer paso es descriptivo, comienza con anotar un conjunto de supuestos que orientan las reflexiones sobre los objetos que presentamos. En este orden de ideas, debiéramos decir que tanto el derecho como el Estado parten de un proceso social que les antecede lógicamente. A continuación presentamos una descripción de los elementos teóricos de Luhmann, evidenciando el impacto de esta teoría en los cambios sociales que supone la

¹⁶ En el *in memoriam* que prologa a Luhmann, Niklas, *La realidad de los medios de masas*, México, Antropos, Universidad Iberoamericana, 2007, p. XIII.

¹⁷ Castells, Manuel, *La era de la información: economía, sociedad y cultura*, vol. I, Madrid, Alianza Editorial, 1999, p. 13.

¹⁸ Luhmann, Niklas, *Sociología del derecho*, Bogotá, Universidad Libre, 2012, p. 56.

sociedad de la información y en el derecho como mecanismo de protección de los derechos informáticos.

1. *Son una suerte de efecto moderno
de un constante proceso de diferenciación social*

Esta diferenciación es comúnmente admitida como propia de un proceso *evolutivo* que fue tomado como punto de partida por las teorías que empezaron a analizar a las sociedades y culturas humanas, justo comenzando el análisis de sus propios procesos comunicativos. La conexión de estos conceptos nos es presentada del siguiente modo por Niklas Luhmann: “Los sistemas sociales surgen primero por la necesidad de selecciones convenidas, lo mismo que, por otro lado, tales necesidades se experimentan primero en los sistemas sociales. Las condiciones que hacen posible esta correlación son resultado de la evolución y cambian con ella”.¹⁹

Como se observa, independientemente de las “selecciones convenidas”, resultan condiciones necesarias de las sociedades mismas. Dicho en términos de la teoría de las obligaciones del derecho civil, requiere posibilidades para la existencia de las negociaciones, y el pacto es la elección de una de aquellas opciones.

Al tiempo la acción social se cifra en la selección. Una vez establecido el pacto, el pacto es ley para las partes y constituye una fuente de las obligaciones. Un poco lo que se nos propone es que si asumimos que lo social pasa por la coordinación de las acciones de los sujetos, tal coordinación se juega sobre un contexto de selección de unos determinados procesos de coordinación, frente a otros. La capacidad de pactar y los distintos caminos a seguir, de los que se terminará optando por alguno necesariamente, los conocimientos para la operación de estas “selecciones convenidas” tienden a pensarse como supuestos de carácter lingüístico, que muestran con su transformación los cambios evolutivos del sistema social mismo. Del mismo modo, la distinción entre las expectativas cognitivas, dependientes de la decepción por el camino de la confrontación con la realidad y las expectativas contrafactualmente estabilizadas devienen en el sistema jurídico logros evolutivos para evitar la complejidad interna del sistema social.²⁰

¹⁹ Luhmann, Niklas, *Poder*, *op. cit.*, nota 15, p. 9.

²⁰ *Ibidem*, nota 18, p. 57.

2. *Lo social es un sistema que “al seleccionar los propios estados”²¹ reproduce su existencia*

Cada comunicación puede dar paso, bien a la aceptación, bien a su rechazo, lo que hace hablar al autor de una “contingencia en ambos lados”.²² Es decir, el pacto depende de dos personas en la comunicación y la decisión de cada una de ellas supone un proceso contingente. De un lado hablaríamos de la opción seleccionada por el emisor, de otro del rechazo o aceptación de la opción del lado del receptor de la comunicación.

El rechazo de una selección “traducido en un tema dentro de los sistemas sociales, se identifica con el conflicto” para nuestro autor.²³ Tal conflicto es resuelto por la “experiencia vivida y compartida” en las sociedades “más simples”,²⁴ mientras las “sociedades más avanzadas desarrollan una necesidad de una diferenciación funcional entre el código del lenguaje en general y, en especial, los medios de comunicación simbólicamente generalizados tales como el poder o la verdad, que condicionan y regulan la motivación para aceptar las selecciones ofrecidas”.²⁵

La descripción del poder es expuesta por Luhmann como propia de un proceso comunicativo, pues, en sus palabras, “una suposición fundamental de todo poder es que la *inseguridad* que existe en relación con la selección del *alter* que tiene poder”²⁶ puede “*producir y quitar* inseguridad en su compañero cuando ejerce su elección”.²⁷

Tal circunstancia es introducida por Luhmann como una “precondición absoluta del poder”,²⁸ en una exposición que saca a la coerción del ámbito propio del poder, pues su centralización sólo es posible en sistemas muy simples.²⁹ En conclusión, bajo una estructura parecida la expectativa, la normativa, al no cumplirse, puede ser ampliada generando en las que entran conceptos como sanción.³⁰

²¹ Luhmann, Niklas, *op. cit.*, nota 15, p. 9.

²² *Idem.*

²³ *Idem.*

²⁴ *Ibidem.*, nota 15, p. 10.

²⁵ *Idem.*

²⁶ *Idem.*

²⁷ *Ibidem.*, nota 15, p. 13.

²⁸ *Idem.*

²⁹ *Ibidem.*, p. 14.

³⁰ *Ibidem.*, 13, p. 73.

En nuestra opinión, tanto las jerarquías como la historia política operan como “sustitutos” que permiten compensar las situaciones de poder,³¹ es decir, el poder tiende a convertirse en una cantidad que debe ser susceptible de ser medida para beneficiarse de la coordinación que aporta, labor que se sirve incluso de símbolos y acuerdos predeterminados que simplifican el proceso. El poder no es visto como un proceso de control absoluto sino como un proceso que en muchos sentidos es “catalizador”, dicho de otro modo, en un ingrediente que acelera o ralentiza ciertos procesos que de todos modos se darían.

Además, el poder se refiere a posibilidades de acción tanto como que su respaldo se encuentra en una suerte de sanción negativa, por lo que el grado de inseguridad resulta especificado para Luhmann,³² que se interesa crecientemente en el poder garantizado por normas dentro de su investigación. Tales consideraciones tienden a hacer la discusión abstracta pues generan las diferencias entre el uso del poder en atención o no, a su aumento, así como los efectos que se encuentren previstos en un sistema normativo, frente a su uso distinguiendo las circunstancias concretas.³³

De manera parecida las consideraciones sobre el poder, además de tender hacia su abstracción, tienden a poner al poder como prerequisite del poder mismo. Así, Luhmann nos dice que los sistemas “sociales organizados y en el nivel de los sistemas comprensivos existen equivalentes institucionalizados que abastecen esto, tales como competencias reconocidas o normas legales válidas a las que uno puede referirse”.³⁴ Falta la distinción entre una infraestructura del poder, es decir, la conformación de amenazas estandarizadas, y su uso por un personaje concreto, en lo que es denominado “modalización” del poder, que en términos de Luhmann se explica como el posible ejercicio del poder. Cuando hablamos del supuesto *ejercicio de poder* supone tomar al poder como objeto de un lenguaje, que tematiza el poder mismo, anticipando las posibles decisiones, lo que genera que el poder pueda ser efectivo, sin el uso siempre eficiente de sus instrumentos en principio centrados en la disuasión. En parte, las consideraciones que se vienen presentando dan para entender el proceso de desarrollo del poder desde la perspectiva de una cadena de comunicaciones, por lo que los resultados de la misma no siempre tendrían la posibilidad de hacer transparente el desarrollo de las decisiones en los distintos “niveles”.

³¹ *Ibidem*, p. 15.

³² *Ibidem*, p. 34.

³³ *Ibidem*, p. 37.

³⁴ *Ibidem*, p. 38.

El hecho de que se haga una interpretación de poder a partir de ciertas características que se hacen presentes en la comunicación, otorga especial importancia a los medios técnicos de tal comunicación. El hecho de que exista comunicación escrita supone, al tiempo, unas condiciones particulares del poder, al punto de que la comunicación puede convertirse en una suerte de programación de acciones, bajo ciertas condiciones. Tales condiciones del lenguaje se transparentan en un contexto, con una importancia propia, en lo que es denominado el código, la posibilidad dentro de las relaciones de poder de describir ciertos resultados o acciones como indeseables y que tales opciones indeseables se mantengan en el ámbito lingüístico de lo potencialmente realizable. Es decir: “En cada caso, da dos cursos a la situación, a favor o en contra del intento del portador del poder”.³⁵ En el caso del derecho el código está determinado por la función de la conformación de expectativas normativas que pueden mantenerse contra los hechos, con lo que, ante la aparición de expectativas contrapuestas y fundadas en la norma, se requiere algo más. Luhmann sostiene:

La evolución social rebasa este estadio mediante un acto de abstracción que se superpone a la forma obvia de bifurcación de toda expectativa (cumplimiento y desengaño), y lo hace mediante una distinción diversa. Igual que antes, ahora se trata de si las expectativas normativas se cumplen o se frustran. Esta observación inmediata de las circunstancias bajo exactamente este punto de vista soporta la función del derecho y no puede ser eliminada. Pero –y por ello hablamos de suponer–, se le completa con una operación de segundo orden que se orienta por el código jurídico diferenciado para ello, y que se reserva el derecho de comprobar, si la expectativa o la conducta decepcionante es (fue, será) de conformidad (o de no-conformidad) con el derecho.³⁶

Como método para facilitar la comunicación sobre el poder puede darse que aquel que esté sujeto al poder anticipe las acciones que pueden llegar a ser requeridas y las ejecute aun sin una comunicación en cada caso, con lo que ganaría a su vez relativamente algo de poder.³⁷ De otro lado, transformaciones en el código hacen posible las distinciones entre las alternativas indeseables y el código como estructura que las señala o no, de modo que la toma de las decisiones puntuales no afecte la estructura del poder, por ejemplo, cuando se delega la solución de un problema concreto a alguien o

³⁵ *Ibidem*, p. 50.

³⁶ Luhmann, Niklas, *El derecho de la sociedad*, México, 2a. ed., Herder, Universidad Iberoamericana, 2005, p. 225.

³⁷ *Ibidem*, p. 52.

en virtud de cargos o aptitudes, distinguiéndose por esta vía el poder de su ejercicio.

El código captura la atención del autor, es decir, la manera como el código empieza a abandonar su papel meramente lógico y empieza a ser compuesto por “la simbolización de las fuentes de poder, de las limitaciones sobre el poder, etcétera; sólo (por oposición) no lo están las selecciones particulares del portador del poder, sus deseos y sus órdenes”.³⁸ La diferencia pasa a ser en cómo el modelo realiza las distinciones fundamentales, mientras que las decisiones particulares ocupan otro lugar en el contexto del poder. En este punto, el código se relaciona con el cargo de la persona que lo ocupa y “sirve como catalizador para la construcción de cadenas de acción”.³⁹ ¿El modo como el sujeto portador de poder lo ejerce, no sería tematizable también como parte del estudio del poder?

Por ejemplo: ¿Las diferencias entre las decisiones de un presidente y las de su sucesor no podrían ser preguntas sobre el poder?

Luhmann sostiene en el fondo que el poder personal admite que el poder fluya en dirección contraria cuando “el poder del sistema excede la capacidad de selección potencial de un solo portador de poder y la capacidad de eslabones medios para intervenir les sirve como una fuente de poder personal”.⁴⁰ Las opciones que exige el sistema superan la capacidad de una fuente de poder, las decisiones deben seguir tomándose, el subordinado puede cambiar la cadena de poder, en la medida en que pueda generar acciones en beneficio de otro. Se separa por oposición la capacidad de generar decisiones de la capacidad de un “administrador”. El centro de creación de decisiones necesita de ayuda, en el fondo el poder supone la competencia para generar ideas para la acción. La competencia se esconde detrás de una incapacidad de cálculo que se asume como hipótesis, tanto como sería admisible, como hipótesis, que nunca hay diferencia entre las opciones de acción del sistema y la capacidad de toma de decisión, estableciendo una armonía entre el tamaño del poder reconocido como tal y la posibilidad de ejercicio de tal poder. Cabe preguntarse, como una vuelta atrás ¿Las cadenas de acciones sociales sólo operan por obra del poder? ¿El diferencial de orden-castigo, como esquema de comunicación, qué grado de la cooperación social puede explicar? Pero Luhmann suma más al asunto con la generación de subcódigos, en caso de que el sistema genere demanda de selecciones.

³⁸ *Ibidem*, p. 54.

³⁹ *Ibidem*, p. 53.

⁴⁰ *Ibidem*, p. 59.

Para ejemplificar la existencia de los subcódigos, Luhmann presenta los casos del “trueque cuando hablamos de crisis económicas o de las historias personales cuando nos referimos a las relaciones afectivas”.⁴¹ El código pasa a ser una distinción fundamental que permite al sistema social cumplir con ciertas funciones que vienen con su configuración previa. Las comprensiones propias de un sistema cultural, en este ejemplo, suponen unas vías de cooperación que no parecen ser problemáticas para Luhmann a la hora de presentarnos el fenómeno del poder. Ciertamente tampoco el concepto genérico de medios de comunicación, como un conjunto de comprensiones que tendrían los mismos efectos resulta problematizado por las mismas razones. El conjunto de distinciones que afectan al ejercicio del poder tiene una cierta configuración lógica determinada por la posibilidad de la negación del lenguaje. Lo que configura una constante en el modo de tratar los objetos de estudio de parte de Luhmann, el código es entendido como susceptible de tramitar nuevos casos, para los que el sistema no cuenta con experiencia, o bien se divide y se sirve de programas con el mismo fin.

En el contexto del derecho, Luhmann nos presenta ciertos casos en los que las distinciones jurídicas son sometidas a una pregunta que puede ser entendida como una paradoja. Por ejemplo, la pregunta sobre si la distinción, conforme a derecho, no conforme a derecho, es conforme a derecho; o, dicho de otro modo, si tal distinción puede ser tratada como tema del género “derecho”. Luhmann nos dice: “[e]n este nivel de programación (autoestructuración), el sistema puede exponerse a variaciones temporales e independizarse de la casualidad de la existencia de conflictos, determinando él mismo lo que puede ser tratado como conflicto sujeto a decisiones. De esta manera el sistema actúa como ‘atractor’ evolutivo de los casos jurídicos”.⁴² Es difícil determinar si la comprensión que tiene Luhmann en este contexto de exposición es la misma que guarda frente a los casos de conflicto en los que interviene el poder. La resistencia a continuar con una orden, independientemente de las consecuencias, en todo caso parece orientarse nuevamente, en el contexto, en sentido de la atención de conflictos sociales, mientras que el código aparece como protagonista en evolución del sistema. El autor también nos dice que en estos casos:

No se trata de pasos empíricos en la constitución de un sistema, ni tampoco históricos del sistema jurídico. Se trata de una reconstrucción lógica de la autopoiesis del sistema, y más exactamente, de una reconstrucción que ha de

⁴¹ *Ibidem*, p. 60.

⁴² Luhmann, Niklas, *op. cit.*, nota 15, p. 227.

puntualizar la imposibilidad de una derivación lógica y a la vez la improbabilidad empírica de la conformación del sistema. La posibilidad de un sistema no se lleva a efecto porque pueda ser deducido de axiomas que se deben a una exigencia lógica, sino porque la autopoiesis del sistema se inicia bajo condiciones históricas excepcionales.⁴³

Ejemplificando se plantea que “una de las categorías más importantes del derecho civil romano, al *obligatio*, parece haber surgido porque alguien, o bien *ex delictu*, o bien *ex contractu*, estaba colocado en-el-no-derecho, y que había que conferirle forma jurídica a esa situación para someterla a un *tratamiento jurídico*”.⁴⁴ Aun cuando la distinción para nosotros es más clara en la reflexión que aumenta las fuentes de la obligación del contrato y el delito, se ve forzada a postular el cuasicontrato y el cuasidelito.

El centro de nuestra atención es, sin embargo, el papel que para Luhmann ocupa el código en la producción y la reproducción evolutiva del derecho. De algún modo el replanteamiento que supone una transformación del derecho, aun cuando es representable lógicamente y es ambientada por el momento histórico, supone un salto creativo que no es explicado por sus antecedentes. En la formación de obligaciones nacidas por un cuasicontrato o por un cuasidelito, debe admitirse el evento del nacimiento de una obligación aun cuando su fuente no puede identificarse, en tanto que no es el contrato ni el delito. En un movimiento regresivo, se construye desde las frases que parecieran *derivadas*, nuevas fuentes de las obligaciones, a una altura que sería en principio más del nivel de lo *axiomático*.

La *causa sui* parece ser la primera aproximación que pudo haberse realizado sobre esa condición particular de fundar la propia existencia. En su *Ética*, Spinoza, además nos dice que es “aquello cuya esencia implica la existencia, o, lo que es lo mismo, aquello cuya naturaleza sólo puede concebirse como existente”.⁴⁵ La tradición ha definido la asimilación de la palabra Dios y la palabra naturaleza en Spinoza.⁴⁶ Así, podría afirmarse que aquella condición de ser *causa de sí*, pudo haber tenido una temprana relación con el mundo natural como un todo, mucho antes de que fuera adjudicable tal condición para los sistemas biológicos por la teoría de sistemas, aun cuando tal condición podría ser observable, si se tiene en cuenta el concepto de *sistema* como directivo de nuevas reflexiones. Valga traer a estas consideraciones un aporte de Marx que roza con nuestro tema:

⁴³ *Idem.*

⁴⁴ Luhmann, Niklas, *op. cit.*, nota 15, p. 228.

⁴⁵ Spinoza, Baruch, *Ética demostrada según el orden geométrico*, Madrid, Orbis, 1980, p. 47.

⁴⁶ *Ibidem*, p. 60.

Que el producto del siervo tiene necesariamente que bastar para reponer, además de su subsistencia, sus condiciones de trabajo, es una circunstancia invariable de todos los sistemas de producción, puesto que no se trata de un resultado de su forma específica, sino una condición natural de todo trabajo continuo y reproductivo en general de toda producción continuada, que es siempre, al mismo tiempo, reproducción y también, por tanto, reproducción de sus propias condiciones de eficacia.⁴⁷

Mientras que en el pensamiento de Luhmann el cambio social se ve determinado por una transformación de la perspectiva en función de ciertas *definiciones fundantes* (el código) de un sistema social, es decir, en el sistema comunicativo, y se orienta a la evolución, entendido como división y proliferación en subsistemas o de sus partes; en Marx, el trabajo sobrante y cedido es condición de la reproducción de *cualquier* sistema social, pero los cambios del sistema están determinados por su contexto económico que incluye las condiciones tecnológicas propias. Con cada descubrimiento productivo, impulso para generar valores de uso, las relaciones sociales se tambalean, pues hay una relación entre la administración de la fuerza de trabajo y los poderes relativos de los sectores de la sociedad.

La relación directa existente entre los propietarios de las condiciones de producción y los productores directos —relación cuya forma corresponde siempre de un modo natural a una determinada fase de desarrollo social— es la que nos revela el secreto más recóndito, la base oculta de toda la construcción social y también, por consiguiente, de la forma política de la relación de soberanía y dependencia, en una palabra, de cada forma específica de Estado.⁴⁸

Este sector de la realidad tecnológica quedará en la consideración de Luhmann, más o menos a las espaldas del objeto de investigación “sociedad”, mientras que para Marx es condición de análisis de un cierto sistema económico y, más aún, de su producción, reproducción y cambio. En el ámbito de las relaciones de los sujetos jurídicos con un determinado dato, es posible ver tal relación existente entre la información y el sustrato tecnológico, formato o infraestructura, si, por ejemplo, observamos el actual estado del mercado discográfico. Si de un lado las nuevas tecnologías, en lo tocante a los formatos de las producciones culturales, se han orientado a generar una mayor portabilidad de los productos musicales, la industria de las

⁴⁷ Marx, Carlos, *El capital. Crítica de la economía política*, México, Fondo de Cultura Económica, 2000, p. 732.

⁴⁸ *Ibidem*, p. 733.

computadoras personales ha abierto la posibilidad de reproducir contenidos indefinidamente. Como consecuencia los vendedores de formatos como el de CD han registrado descensos aquí y allá, forzando incluso a la disminución de los competidores dentro del mercado.⁴⁹ Todo el proceso que se describe para Marx en el esquema cambio de condiciones de producción-cambio de las relaciones sociales, podría ser descrito como un evento comunicativo, sin embargo, queremos señalar que el hecho de que la tecnología sea *disponible* determina una condición concreta de las relaciones de poder. Tal disposición está definida por condiciones en el mundo físico de cercanía y control de objetos.

En un sentido parecido, pero dentro del ámbito biológico que sirve de condición para el sistema social se encuentra el tratamiento luhmanniano de la violencia. En el contexto del poder, denominado “medio de comunicación” por Luhmann, es ajena la violencia, por lo que se nos dirá: “La violencia física ejercida intencionalmente contra la gente tiene una conexión con el medio del poder orientado por la acción, en que *elimina la acción por medio de la acción* y, con esto, excluye la *transmisión comunicativa de premisas reducidas de toma de decisiones*”.⁵⁰ En este esquema la acción pasa a ser meramente comunicativa y su efecto, en el fondo, únicamente es visible en la transmisión de mensajes. Por esta vía Luhmann nos aclara que la “violencia física no puede ser poder, pero conforma el caso extremo inevitable de una alternativa de evitación que forma poder”,⁵¹ con lo que la violencia queda más allá del velo que encierra la sociedad, excluido en el contexto del “acoplamiento estructural”. Esto no significa que Luhmann no considere las condiciones tecnológicas:

La técnica toma la forma de hacer automático y calculable al procesamiento de la información de operar con entidades idealizadas sin, al mismo tiempo, tener que considerar sus implicaciones más amplias. El desarrollo técnico de este tipo posibilita procesar selectivamente situaciones muy complejas y, con esto, reorganizar aquellas posibilidades que siguen siendo compatibles con los límites de la conciencia y con el estatus del mundo que experimentamos comúnmente.⁵²

⁴⁹ Tahiri, Javier, “La compra de EMI por Universal dibuja un mercado con cada vez menos negocio y competidores”, *Periódico ABC*, del 29 de octubre de 2012, <http://www.abc.es/20121015/economia/abci-crisis-discograficas-201210122003.html>.

⁵⁰ Luhmann, Niklas, *op. cit.*, nota 15, p. 91.

⁵¹ *Idem.*

⁵² *Ibidem*, nota 15, p. 101.

Así las cosas, la relación de la técnica con el entorno de un sistema social ilumina el cambio de condiciones de comunicación, pero Luhmann se cuida de no relacionarse con el pensamiento materialista al decirnos que tal circunstancia: “No contiene la sugerencia inmediata de que la organización laboral, el control del entorno, las relaciones de la producción, el estado de la economía y el dominio de clases sean factores primarios en el cambio social, aunque no los excluye”.⁵³

Habría que hacer una presentación conceptual del término luhmanniano “alternativa de evitación”, como una suerte de consecuencia desagradable que sustenta las relaciones de poder, esto no necesariamente cambia con las distintas relaciones de poder. Así, si se trata de influencia: “Ego acepta la influencia porque otros también la aceptan. Con el objeto de poder denominar claramente estos tipos de generalización, los llamaremos autoridad a la influencia temporalmente generalizada, y liderazgo a la influencia circunstancialmente generalizada”.⁵⁴

Es claro que el autor ve al poder como un medio de comunicación, algo relacionado de algún modo con la posibilidad de extender las comunicaciones, como el aparato lingüístico sobre el que funciona el proceso de toma de decisiones social que “generan una distinción entre lo que el sistema social admite como posible y lo que su relación con el tiempo puede hacer posible”.⁵⁵ De este modo la crisis se ve como un cierto momento en donde el medio de comunicación del poder funciona incorrectamente, bien por falta en la alternativa que se intenta evitar (el castigo implícito), o por falta en la perspectiva que orienta las acciones, lo que vendría a ser un problema cognoscitivo.

Incluso Luhmann llega a plantear la idea de la no transformación de las relaciones de riqueza y de poder por la no existencia en el comercio de la producción de leyes o la imposibilidad legal de confiscar los bienes, con la idea final de que el poder político no debe enriquecer a sus portadores.⁵⁶ Plantea una circunstancia teórica del modo como debiera ser entendido el poder o las condiciones en las que es comprensible que funcione, pero dejando de lado la infinidad de casos en los que las condiciones de poder fortalecen posiciones por razones de prestigio o riqueza. Esta circunstancia será, a lo sumo, para él, una contingencia más o menos reiterada que no

⁵³ *Idem.*

⁵⁴ *Ibidem*, p. 107.

⁵⁵ *Ibidem*, p. 123.

⁵⁶ Luhmann, Niklas, *op. cit.*, nota 15, p. 143.

demuestra una condición profunda de ligazón, al no presentarse dentro de las consideraciones de un contexto de vínculos indelebles entre sí.

III. CONCLUSIONES

Así vistas las cosas, la generalidad de la descripción hace equivalente la amenaza de invasión de una nación a otra, independientemente de que el origen de la intimidación sea una superpotencia nuclear o un país retrasado del tercer mundo. Con este comentario se quiere subrayar que la posibilidad de disposición sobre la tecnología de la guerra de los sujetos sociales se hace necesaria para explicar sus relaciones, no bastando así los efectos sobre los protocolos de la comunicación social de la tecnología. En tanto que hay casos en los que esos réditos de la tecnología se ven mermados para estos efectos, se puede pensar en las consecuencias en los protocolos de la comunicación social que puede aportar un misil o un fusil y se verá los límites de la explicación de la tecnología en estos estrechos márgenes.

Un análisis que no toma en cuenta las consideraciones propias del sustrato tecnológico de la sociedad, deja ver la necesidad de proteger los datos de los ciudadanos en el momento, en medio del cambio del contexto del fordismo a la sociedad de la información. El cambio de contexto genera las siguientes consecuencias: primero, su elevación a grado de derecho, entendido el contenido del derecho como una facultad del ciudadano de oponerle al Estado la protección de sus datos; segundo, imprimiendo un valor probatorio a las transacciones económicas que garantizan el comercio y la celebración de negocios en ámbitos virtuales o en plataformas altamente tecnológicas de transacción; tercero, es un canal de comunicación del ejercicio del poder y de la gobernabilidad, es decir, desde las elecciones hasta la propaganda y la oposición se efectúan por canales de comunicación altamente tecnológicos que transmiten mensajes de datos que en su contenido permiten el ejercicio de la democracia y el funcionamiento de otros sistemas, como el político, el económico, el sociológico y el cultural.

De este modo, son tres esferas las que constantemente se hacen presentes en la consideración de los derechos vinculados a los datos. El Estado, como forma social, pero también como poseedor de tecnología de coerción y control de las acciones en la sociedad. Es decir, primero por ser el depositario del monopolio de la violencia y la vigilancia por efecto de la renuncia de sus asociados a tales prácticas como garantía de la paz común o el Estado como poseedor exclusivo de los medios de coacción. En segundo lugar los sujetos vinculados a ese Estado, tanto como los sujetos en una cierta

relación con los medios tecnológicos de la sociedad. Y en tercer lugar, la capacidad tecnológica de la sociedad y su lugar dentro de un determinado mercado. Estas tres áreas se encuentran relacionadas y se transforman con la tecnología misma. Los Estados pueden presentarse como oferentes de seguridad, pero las condiciones concretas de tal oferta dependen de su capacidad tecnológica. Sectores de la población de un Estado pueden tener ciertos medios técnicos que definen sus relaciones de poder frente a su propio Estado. Bastará recordar en este contexto el cambio en la forma como se configuró la voluntad de las masas en la era de la televisión, como modelo de comunicación unidireccional y los cambios en los movimientos sociales en la era de Internet.

Desde el punto de vista tecnológico la infraestructura comunicativa de la red global de información está distribuida por todo el globo en cables oceánicos y todo tipo de señales para antena, sea este de un satélite, o un poblado de la tierra, transportado por ondas electromagnéticas. Toda esa infraestructura, con su enorme inversión, su sofisticación, se acompaña de los lugares de procesamiento de información, que van desde los propios satélites hasta una variedad de infraestructuras de gran tamaño como los servidores de Internet (grandes edificios en las que se apilan multitud de computadoras en constante comunicación). Gran parte de esta estructura depende de grandes Estados y empresas de gran calado.

La permanencia de la infraestructura empieza a ser un factor de seguridad nacional,⁵⁷ al punto que se clama desde Brasil por su regulación desde un organismo internacional a causa de informaciones de prensa que sostenían que el país había sido víctima de espionaje masivo.⁵⁸ En ese contexto internacional. ¿En qué medida una legislación sobre Internet tiene que partir de las capacidades reales de los Estados para llevarlas a cabo? Pues la capacidad tecnológica en cada Estado es diferente, además, vale la pena tomar en cuenta las posteriores definiciones sobre las políticas públicas que intentaran determinar qué tanto actuar o qué tanto fijar unos principios sobre el grado de protección de los datos en la red.

El reverso de la pregunta es si los ciudadanos pueden recurrir a programas que encripten sus comunicaciones cuando el Estado no pueda garantizar la reserva que acoja el derecho a la intimidad. Este proceso adquiere

⁵⁷ “Internet surgió como un proyecto de la CIA: Putin”, *Plano informativo*, consultado el 14 de mayo de 2014, http://planoinformativo.com/nota_voz_2014.php?id=321408.

⁵⁸ “Rousseff liderará movimiento internacional de regulación de Internet”, *Diario de Yucatán*, 23 de abril de 2012, <http://yucatan.com.mx/tecnologia/internet/rousseff-liderara-movimiento-internacional-de-regulacion-de-internet>.

cada vez más importancia, al punto que las propuestas sobre una moneda virtual dependen también para su eficacia de la criptografía, con lo que cubrimos las dos caras del control de la comunicación y la información, es decir, el tener el sustrato tecnológico en el que descansa o tener escondido su sentido en virtud de un proceso de encriptación.

Ciertamente operan otras condiciones para que no en todos los procesos de negociación se requiera la amenaza de la intervención del Estado mediante un proceso judicial y, sin embargo, se cumpla el contenido de sus acuerdos. A su vez, no todo conflicto es susceptible de ser conocido por un juez. Las mismas normas escogen, mediante los escenarios que proponen, el tratamiento de ciertas conductas y no el de otras. Los intentos de descripción para el difícil problema del contorno de los derechos por parte de los Estados, nos hacen pensar que los cambios materiales también atraen consecuencias en la ciencia jurídica por medio de la introducción de descripciones. Cuando hablamos de un proceso donde está en juego la responsabilidad administrativa de un particular. ¿Se debe mantener la regla de la inviolabilidad del correo sin orden judicial?

El caso que se presentó recientemente en Colombia, con el alcalde mayor de Bogotá y los procesos en su contra en búsqueda de su destitución,⁵⁹ muestra otro de los eventos en que los actores sociales pueden tener interpretaciones disímiles sobre el alcance de los derechos en el contexto de las nuevas tecnologías. Así, además de los dos extremos de protección, la posesión del sustrato material de la información y la encriptación, quedan un conjunto de usos de la información prohibidos de acuerdo con el contexto institucional de una discusión social. En este contexto de protección lo que se regula es el uso de la información, su papel como prueba judicial frente a los procesos, o las consecuencias del mismo uso en el derecho a la intimidad o el buen nombre. La discusión judicial ha avanzado sobre la información generando un sistema de garantía débil, en tanto que otros usos de la información podrían generar daños que los propios estrados judiciales no podrían subsanar.

Un ejemplo de cómo la regulación colombiana no es eficaz a la hora de proteger el derecho fundamental del *habeas data*, se constata con la expedición de las dos leyes estatutarias la de 1266 de 2008 y la 1581 de 2012, y el Decreto 1377 de 2013, reglamentario de esta última hacen evidente la tensión entre el Estado y el sujeto de derecho. La regulación del derecho por

⁵⁹ “Los magistrados que restituyeron a Petro habían tumbado pruebas en proceso”, *El Tiempo*, redacción justicia, 23 de abril de 2014, http://www.eltiempo.com/justicia/ARTICULO-WEB-NEW_NOTA_INTERIOR-13870476.html.

parte del Estado le otorga el alcance, limita la información protegida y establece la relación entre el sujeto y las instituciones, sean públicas o privadas, regulando obligaciones de los actores participantes en la comunicación de la información.

En la primera ley no se puede distinguir la importancia de la protección al *habeas data*, su conexión con los derechos humanos y no es claro que la intención del legislador sea proteger derechos fundamentales como la intimidad, el buen nombre, evitar la discriminación o la persecución en razón de la afiliación política, el sexo, o la raza, entre otros. La Ley 1266 surge como una respuesta del sector financiero y de sus usuarios que presentaron conflictos profundos y complicados en los reportes a las centrales de riesgo por incumplimiento de sus obligaciones crediticias.

Con la expedición de la Ley 1581 en 2012 el ámbito de protección se amplió, no solamente se extendió la protección a otras formas de información distinta a la comercial y crediticia, enmarcadas dentro de un concepto más amplio de los datos personales, sino que la ley definió un nuevo objeto:

Artículo 1. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información consagrado en el artículo 20 de la misma.

En consecuencia, es un derecho que permite oponer limitaciones al Estado, y el Estado, al mismo tiempo, puede hacer nugatorio el derecho o ser el principal violador del mismo, y más bien, la legislación se constituye en una nueva forma de control desde el dominio y manejo de los datos de las personas. El derecho cambia la descripción del dato que se protege, lo anterior se puede comprobar en la evolución del tipo de dato que fue protegido por la legislación. En la Ley 1266 de 2008 se define el dato personal, el público, el semiprivado y el privado en términos generales, y siempre con una finalidad de protección del sector comercial y financiero, por otra parte, lo interesante es que en 2012 la Ley 1581 se ocupa de definir qué es el dato sensible explicando que se trata de aquel dato que al usarlo indebidamente puede generar discriminación en términos raciales, políticos, sociales y culturales. Por ello, el Decreto Reglamentario de esta última, el 1377 de 2013 repite las definiciones sin ahondar en discusiones de fondo sobre el tema. Lo que brilla por su ausencia es qué ocurre cuando las violaciones a la protección de estos datos las comete el mismo Estado colombiano, es decir,

cuando esta información se emplea en desmedro de los ciudadanos, caso de las chuzadas en medio de los diálogos de paz en La Habana, o cuando los correos privados de los ciudadanos son intervenidos por una potencia internacional, o cuando la omisión de las autoridades no garantiza con la debida diligencia la protección del contenido de los datos sensibles como es el caso de los pensionados que han perdido sus semanas de cotización de la pensión y, por lo tanto, el derecho a pensionarse, porque en el sistema se borran o se pierden las semanas cotizadas. A continuación un cuadro comparativo del concepto de dato y sus diversas acepciones, en las normas vigentes en Colombia:

<i>Ley 1266 de 2008</i>	<i>Ley 1581 de 2012</i>	<i>Decreto 1377 de 2013</i>
<p>Artículo 3o. <i>Definiciones.</i> Para los efectos de la presente ley, se entiende por:</p> <p>...</p> <p>e) Dato personal. Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos personales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados.</p> <p>f) Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son</p>	<p>Artículo 3o. <i>Definiciones.</i> ...</p> <p>c) Dato personal. Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.</p> <p>Artículo 5o. <i>Datos sensibles.</i> Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los</p>	<p>Artículo 3o. <i>Definiciones.</i> Además de las definiciones establecidas en el artículo 3 de la Ley 1581 de 2012, para los efectos del presente decreto se entenderá por:</p> <p>...</p> <p>2. Dato público. Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.</p> <p>3. Datos sensibles. Se entiende por datos sensibles aquellos que afectan la in-</p>

<i>Ley 1266 de 2008</i>	<i>Ley 1581 de 2012</i>	<i>Decreto 1377 de 2013</i>
<p>públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.</p> <p>g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.</p> <p>h) Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.</p>	<p>datos relativos a la salud, a la vida sexual y los datos biométricos.</p> <p>Artículo 6o. <i>Tratamiento de datos sensibles.</i> Se prohíbe el Tratamiento de datos sensibles, excepto cuando:</p> <p>a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;</p> <p>b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.</p> <p>c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no</p>	<p>timidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.</p>

<i>Ley 1266 de 2008</i>	<i>Ley 1581 de 2012</i>	<i>Decreto 1377 de 2013</i>
	se podrán suministrar a terceros sin la autorización del Titular. d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.	

Sin embargo, el Estado no ha tenido el mismo tratamiento para todos los derechos en juego en el contexto de la sociedad de la información, mientras las filtraciones por la intromisión masiva de algunos Estados en la intimidad de las comunicaciones de miles de habitantes del globo se da, los intentos más serios de regular este ámbito se libran en el tema de los derechos de autor y sobre todo del *copyright*, es decir, fundamentalmente asegurando y extendiendo los derechos económicos involucrados con el derecho de autor, dejando de lado los derechos morales y otras áreas susceptibles de regulación. Estos intentos se centran en el uso de la información, más que en las posibilidades reales para garantizar su control, y del uso de la información destinada a conocerse por efecto de la industria cultural, mientras que los derechos a la intimidad no tienen el mismo grado de protección. El último intento de regular el tema, y atado a la firma del Tratado de Libre Comercio con Estados Unidos, fue declarado inconstitucional por la sentencia C-011/13,⁶⁰ que controló la constitucionalidad de la Ley 1520/13, para desmedro del debate, no por razones sustanciales, sino fundamentalmente

⁶⁰ Corte Constitucional, sentencia de constitucionalidad C- 011/13, demanda de inconstitucionalidad contra la Ley 1520 de 2012 “por medio de la cual se implementan compromisos adquiridos por virtud del Acuerdo de Promoción Comercial suscrito entre la República de Colombia y los Estados Unidos de América, y su Protocolo Modificatorio, en el marco de la política de comercio exterior e integración económica”. Referencia: expediente D- 9107, 23 de enero de 2013, p. 50.

por razones de orden procedimental. En este caso la Corte definió que la norma había sido tramitada por una comisión errada (la comisión 2a., tanto de la cámara como del Senado cuando las correctas eran las comisiones primeras). Se dejaba ver, en todo caso, en la legislación frustrada una exención de los derechos comerciales en general, su ejemplo más claro era extender la vigencia de los derechos patrimoniales de 50 a 70 años en el caso de que las propietarias fueran personas jurídicas, con lo que se estaban ampliando derechos en últimas derivados, pues los autores, como personas naturales ya tenían esa protección.

IV. BIBLIOGRAFÍA

CASTELLS, Manuel, *La era de la información: economía sociedad y cultura*, vol. I, Madrid, Alianza Editorial, 1999.

CORTE CONSTITUCIONAL DE COLOMBIA, sentencia C-748/11, referencia: expediente PE-032, control constitucional al Proyecto de Ley Estatutaria núm. 184 de 2010 Senado; 046 de 2010 Cámara, “por la cual se dictan disposiciones generales para la protección de datos personales”, Bogotá D. C., 6 de octubre de 2011.

———, Sentencia T-058/13. Referencia: expediente T-3623403, Acción de tutela instaurada por AA contra la Universidad BB. Bogotá D.C., 7 de febrero de 2013.

———, Sentencias T-455 de 1998 y T-949 de 2003. Casos en los cuales el *habeas data* funge como garantía del derecho al buen nombre frente a situaciones de homonimia y suplantación.

———, Sentencia T-486 de 2003. Caso en el cual el *habeas data* funge como garantía de las prestaciones de la seguridad social, mediante la orden a una EPS de incorporar información sobre la afiliación al sistema contributivo, de lo que dependía la concesión de dichas prestaciones.

———, Sentencia T-310 de 2003. Caso en el cual el *habeas data* funge como garantía del derecho a la libertad personal, mediante la orden de cancelación del registro de orden de captura vigente.

———, Sentencia de Constitucionalidad C-011/13. Demanda de inconstitucionalidad contra la Ley 1520 de 2012 “por medio de la cual se implementan compromisos adquiridos por virtud del Acuerdo de Promoción Comercial suscrito entre la República de Colombia y los Estados Unidos de América y su Protocolo Modificatorio, en el marco de la política

de comercio exterior e integración económica”. Referencia: expediente D-9107, 23 de enero de 2013.

CROVI DRUETTA, Delia, “Sociedad de la Información y el Conocimiento. Entre el optimismo y la desesperanza”, *Revista Mexicana de Ciencias Políticas y Sociales*, México, UNAM, año XLV, núm. 185, mayo-agosto de 2002, http://www.miaulavirtual.com.mx/ciencias_sociales/Revista_UNAM/RevistaUnamPDF/RMCPYS%20NUM-185.pdf.

Diario de Yucatán, “Rousseff liderará movimiento internacional de regulación de Internet”, <http://yucatan.com.mx/tecnologia/internet/rousseff-liderara-movimiento-internacional-de-regulacion-de-internet>.

MARX, Carlos, *El Capital. Crítica de la economía política*, Fondo de Cultura Económica, México, 2000.

MEDINA LÓPEZ, Diego Eduardo, *El derecho de los jueces*, 3a. ed., Colombia, Ediciones Uniandes, Legis, 2002.

NIKLAS, Luhmann, *Sociología del derecho*, Universidad Libre, Bogotá, 2012.

———, *Poder*, Antropos, Universidad Iberoamericana, México, 1995.

———, *El derecho de la sociedad*, Herder, Universidad Iberoamericana, 2a. ed., México, 2005.

SPINOZA, Baruch, *Ética demostrada según el orden geométrico*, Orbis, Madrid, 1980, Parte I, Definición I.

———, *Ética demostrada según el orden geométrico*, Orbis, Madrid, 1980, Parte I, Definición XIV.

PLANO INFORMATIVO, Internet surgió como un proyecto de la CIA: Putin, <http://www.planoinformativo.com/nota/id/321408#.U1q6vVXa6so>.

VALENCIA ZEA, Arturo y ORTIZ MONSALVE, Álvaro, *Derecho civil. Parte general y personas*, Colombia, Temis, 2002.

ALGUNOS ASPECTOS DE LA PROPIEDAD INTELECTUAL EN EL ENTORNO DIGITAL

Carlos Alberto ORTIZ LÓPEZ*

SUMARIO: I. *Generalidades del derecho de autor.* II. *Generalidades de la propiedad industrial.* III. *La propiedad intelectual en el entorno digital.* IV. *Conclusiones.* V. *Bibliografía.*

I. GENERALIDADES DEL DERECHO DE AUTOR

La propiedad intelectual es la rama del derecho que se encarga de la protección de las diferentes creaciones del intelecto. Se divide principalmente en dos ramas denominadas, derecho de autor y propiedad industrial. El derecho de autor tiene como objeto de protección las obras literarias y artísticas, entre las cuales encontramos los libros, las canciones, las fotografías, las esculturas, la arquitectura, los dibujos, el *software*, los artículos de investigación, la música, el cine, el teatro, las obras coreográficas, entre otros.

Cuando el autor crea una obra literaria o artística, la legislación en la materia les otorga una serie de prerrogativas a su favor, llamadas derechos morales y derechos patrimoniales, sin embargo, antes de entrar a explicar la naturaleza y contenido de estos derechos, es preciso señalar algunos de los principios que rigen esta materia.

* Abogado de la Universidad Católica de Colombia, especialista en derecho de autor, propiedad industrial y nuevas tecnologías, de la Universidad Externado de Colombia. Actual docente e investigador en propiedad intelectual en la Facultad de Derecho de la Universidad Cooperativa de Colombia.

1. *Principios del derecho de autor*

A. *La no protección de las ideas*

El derecho de autor protege exclusivamente la forma literaria o artística en que las ideas son descritas, ilustradas o incorporadas en las obras. Este principio permite que las ideas fluyan de generación en generación, sin que su utilización requiera de la autorización de alguna persona natural o jurídica, o del mismo Estado. En tal sentido, se protegerá la obra literaria y artística *per se*, mas no las ideas contenidas en ellas.

B. *Ausencia de formalidades*

La protección que el derecho de autor otorga a los autores de obras literarias o artísticas iniciará desde el mismo momento en que la obra es creada, sin requerir el cumplimiento de alguna formalidad.

Al respecto, el Convenio de Berna en su artículo 5.2 señala: “El goce y el ejercicio de estos derechos no estarán subordinados a ninguna formalidad y ambos son independientes de la existencia de protección en el país de origen de la obra”.¹

En este sentido, desde el mismo instante en que una persona escribe un texto, toma una fotografía, desarrolla un *software*, realiza una escultura, etcétera, las obras están protegidas por el derecho de autor. Sin embargo, en la mayoría de los países, existe un sistema de registro de obras, el cual tiene un carácter meramente declarativo y no constitutivo de derechos, es decir, que el registro no se realiza para obtener la protección de la obra, ya que ésta se protege desde su creación, sino para obtener un medio probatorio que me acredite como el respectivo autor de mi creación.

C. *Destino y mérito*

El derecho de autor protege las obras literarias y artísticas sin importar sus calidades o el propósito con el que fue creada. De esta forma, el derecho de autor protege por igual a las obras que se crean con fines comerciales, a las que se crean con fines académicos o sencillamente por una actividad lú-

¹ Convenio de Berna, artículo 5.2.

dica, aun sin importar si son largas, cortas, si gustaron o no, o si son creadas por un experto o un principiante.

D. *Originalidad*

Todas las obras literarias o artísticas deben cumplir con el requisito de originalidad, es decir, que no deben ser una copia de una obra ya existente, en donde el autor le imprime su sello personal, sus características, su talento propio que lo diferencia de otros autores.

E. *Soporte material*

En relación con el soporte material de las obras, hay que señalar dos aspectos que, aunque sencillos, son muy importantes. En primer lugar, el derecho de autor protege las obras en cualquier formato en el que se encuentren, sea papel, arcilla, madera, o sea un archivo digital. Sea un formato analógico o digital, el derecho de autor otorga la misma protección.

En segundo lugar, es importante diferenciar entre el formato que contiene una obra y los derechos de la obra incluida en dicho formato. Es decir, que cuando se adquiere una obra en cualquier lugar de expendio, como un libro, se compra el formato que contiene una obra, mas no los derechos que posee el autor sobre la misma.

Por ejemplo, existen muchos casos en los que algunas personas compran el disco compacto de música, pero en vez de utilizarlo para su disfrute dentro de su ámbito o domicilio privado, le dan un uso comercial argumentando que ellos lo compraron legalmente. En tal sentido, es claro que no se puede utilizar una obra con fines comerciales por el solo hecho de comprar un ejemplar, ya que por dicha compra no se están adquiriendo los derechos que posee el autor sobre la obra respectiva.

Una vez conocidos los principios regulatorios del derecho de autor, es importante conocer los derechos que la ley le otorga al creador de una obra desde el mismo instante en que ésta es creada.

2. *Los derechos morales*

Los derechos morales son derechos que se caracterizan por ser inalienables, perpetuos, imprescriptibles e inembargables, y no son derechos de explotación económica. Entre los derechos morales en favor del autor

se encuentra el derecho de paternidad, el cual hace relación al derecho de ser reconocido como autor de su propia creación. Asimismo, se encuentra el derecho de integridad, el cual le permite al autor impedir cualquier modificación de su obra que afecte el decoro de la misma o su personalidad y reputación; el autor también ostenta el derecho de ineditud, en donde el autor podrá oponerse a la publicación no autorizada de su obra y a mantenerla inédita si es su deseo. Finalmente, se encuentran los derechos de modificación, en el cual el autor puede modificar su propia obra en cualquier momento, y el derecho de retracto o arrepentimiento, en donde un autor que ya haya autorizado la publicación de su obra podrá retractarse de dicha autorización y ordenar la recolección de todos los ejemplares que se encuentran al público, so pena de pagar los perjuicios ocasionados.

3. *Los derechos patrimoniales*

Por su parte, los derechos patrimoniales son derechos exclusivos de autorizar o prohibir cualquier uso de la obra y se caracterizan por ser transferibles, embargables y temporales.

En primer lugar, encontramos el derecho de reproducción, derecho que le permite al autor autorizar o prohibir que multipliquen o reproduzcan su obra a través de cualquier formato, medio o procedimiento. Por otro lado, encontramos el derecho de comunicación pública, en el cual el creador puede autorizar o prohibir que su obra llegue al público a través de algún medio impreso o tecnológico, como la televisión, Internet o la radio.

Igualmente, encontramos el derecho de transformación, en el cual el creador podrá autorizar o prohibir cualquier modificación a su obra, tales como adaptaciones o traducciones; finalmente, se encuentra el derecho de distribución, el cual se refiere al derecho de autor de autorizar o prohibir que su obra se venda, se preste o se alquile. En la mayoría de las legislaciones, se encuentran estipulados estos derechos patrimoniales, pero no debe entenderse como los únicos, ya que cualquier acto que constituya una explotación económica de la obra fuera de los anteriormente enunciados, debe requerir de la autorización previa y expresa del titular de los derechos patrimoniales.

II. GENERALIDADES DE LA PROPIEDAD INDUSTRIAL

La otra rama de la propiedad intelectual, es la denominada propiedad industrial, la cual, como su nombre lo indica, se refiere a creaciones que

tienen un fin más comercial o industrial. En la propiedad industrial se encuentra la protección de los siguientes tipos de creaciones:

1. *Las nuevas creaciones*

Dentro de las nuevas creaciones se hallan principalmente las patentes de invención, las patentes de modelos de utilidad y los diseños industriales.

Las patentes de invención tienen como objeto de protección los inventos en los distintos campos de la tecnología, por ejemplo, los avances electrónicos, los farmacéuticos o las fórmulas, entre otros. Para que una invención obtenga la protección vía patentes, deberá cumplir con los siguientes requisitos:

- **Novedad:** que la invención no se encuentre en el estado de la técnica, es decir, que no exista en ninguna parte del mundo algo igual o semejante.
- **Nivel inventivo:** que el invento no sea obvio para un experto medio en el campo tecnológico al que haga parte el mismo.
- **Aplicación industrial:** que el invento pueda ser producido o utilizado en cualquier tipo de industria.

Las patentes de modelo de utilidad tienen que ver con aquellas nuevas formas o configuraciones de algún artefacto, instrumento u objeto, que permita un mejor o diferente funcionamiento o que le proporcione alguna utilidad, ventaja o efecto técnico que antes no tenía.

En relación con los diseños industriales, la Decisión Andina 486 de 2000, norma principal en propiedad industrial para los países de la CAN, los define como “la apariencia particular de un producto que resulte de cualquier reunión de líneas o combinación de colores, o de cualquier forma externa bidimensional o tridimensional, línea, contorno, configuración, textura o material, sin que cambie el destino o finalidad de dicho producto”.²

Por ejemplo, la botella de Coca Cola, al tener una forma diferente a lo usual en el mercado, logró obtener el registro de diseño industrial. El requisito de novedad es el único que se exige para que un diseño industrial sea protegido por cada una de las legislaciones.

² Decisión Andina 486 de 2000, artículo 113.

2. *Signos distintivos*

Dentro de los signos distintivos, encontramos principalmente las marcas, las cuales son signos que identifican productos o servicios en el mercado. Estos signos pueden ser constituidos por palabras, letras, números, colores, dibujos, sonidos, o la mezcla de éstos.

Las marcas son de las creaciones intelectuales que más se han desarrollado y explotado por el uso de las nuevas tecnologías, pues están presentes en cualquier página web o en la publicidad que aparece en la red. Hoy en día ya se hacen estudios específicos del valor de las marcas solamente en redes sociales o en una página web particular, lo que evidencia un uso predominante para el comercio digital.

Por otro lado, como signos distintivos se encuentran los nombres comerciales, relacionados con el nombre por medio del cual las empresas se dan a conocer en el mercado, los lemas comerciales, los cuales son aquellas palabras o leyendas que acompañan una marca, y las enseñas comerciales, las cuales otorgan protección al aviso o letrero del establecimiento de comercio.

De igual forma, dentro de los signos distintivos encontramos las indicaciones geográficas, entendidos como aquellos signos que identifican un producto con un origen determinado, como el tequila de México, el café de Colombia, o el queso parmesano de Italia, entre muchos otros.

Finalmente, encontramos los nombres de dominio, es decir, la dirección electrónica de las páginas web. Muchos doctrinantes ubican a los nombres de dominio dentro de los signos distintivos, mientras que otros la consideran como una nueva rama de la propiedad intelectual.

3. *Secretos empresariales*

Se considerará como secreto empresarial aquella información no divulgada o no conocida que tiene un valor comercial o económico para una determinada persona natural o jurídica.

III. LA PROPIEDAD INTELECTUAL EN EL ENTORNO DIGITAL

Al profundizar en el panorama tecnológico actual y en la utilización de contenidos protegidos por el derecho el autor en Internet, nos damos cuenta que los distintos tratados internacionales y las normas nacionales o supranacionales se quedan cortos frente a la necesidad, por una parte, de los autores

de hacer respetar sus derechos y, por otra, de los usuarios, quienes, frente a sus derechos a la educación, cultura, libertad de expresión e información solicitan un mejor manejo de la propiedad intelectual en el entorno digital.

En consecuencia, frente a los nuevos retos que las tecnologías le impusieron a los diferentes derechos de propiedad intelectual, la Organización Mundial de la Propiedad Intelectual (OMPI), organismo especializado de las Naciones Unidas, inició la construcción de unos tratados cuyo propósito era actualizar la normatividad existente en materia de derecho de autor para su desarrollo en Internet. De dichos esfuerzos nacieron los denominados “Tratados Internet”, es decir, el Tratado de la OMPI sobre Derecho de Autor (TODA) y el Tratado de la OMPI sobre Interpretaciones o Ejecuciones y Fonogramas (TOIEF).

Los “Tratados Internet” establecieron principalmente algunos parámetros relacionados con los derechos patrimoniales de autor, las limitaciones y excepciones, obligaciones relativas de las medidas tecnológicas de protección y a la información sobre la gestión de los derechos, disposiciones sobre observancia de los derechos, entre otros.

Asimismo, pero en el marco de la Organización Mundial del Comercio (OMC), se desarrolló el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), el cual invitó a los países miembros a reforzar la protección de la propiedad intelectual como impulso económico y social de los países. Al respecto la doctrina ha señalado:

Internet inicialmente fue concebido como una red científica y de información, pero ha evolucionado hacia un modo de hacer negocios y un espacio de carácter comercial, donde el mercadeo de bienes y servicios a través de Internet, entre ellos bienes intelectuales, ha convertido en tema fundamental al del valor y la protección de los contenidos que se encuentran en la red.

Con las tecnologías de digitalización de obras, y la difusión y transmisión de éstos a través de Internet a grandes velocidades y con facilidades de cobertura universal, ha resultado ser muy interesante para los autores y titulares de derechos como vehículo de explotación de las creaciones, pero a la vez ha generado preocupación sobre la manera de proteger legalmente esos contenidos disponibles en Internet. En tal sentido, con los Tratados de la OMPI de 1996 sobre Derecho de Autor, y sobre Interpretaciones o Ejecuciones y Fonogramas, se ha pretendido conceder una protección adecuada y suficiente a los titulares de derecho de autor y derechos conexos por los usos en el ámbito digital.

Dos aspectos principales deben considerarse sobre el tema de Internet y el derecho de autor. En primer lugar, Internet como medio de difusión y

utilización de las obras, así como los derechos exclusivos que tal utilización afecta. Las páginas de Internet o sitios web como elementos protegibles por el derecho de autor, es el segundo aspecto.³

De igual forma, los países constantemente firman tratados de libre comercio, en donde se establecen obligaciones para la protección de la propiedad intelectual en general, pero específicamente en Internet.

Es evidente que las legislaciones a nivel mundial reconocen la problemática que actualmente se suscita en Internet y están buscando mecanismos que les permitan mantener principalmente el equilibrio económico que generan las industrias protegidas por el derecho de autor.

Estos derechos le permiten al autor o titular tener un control sobre su obra o creación, decidiendo cualquier uso que un tercero pretenda realizar sin importar su finalidad. Dichas normas fueron desarrolladas con un pensamiento analógico, es decir, teniendo en cuenta únicamente el uso, comercialización y necesidades de las obras en formato físico, sin considerar que a futuro, todas las personas tendríamos acceso a obras de forma legal e ilegal, masivamente y a tan solo un click de distancia.

Sin embargo, a pesar de la aplicación de la normatividad existente al entorno digital, se continúan presentando diferentes vacíos jurídicos en relación con la interpretación de las normas, la responsabilidad de los diferentes actores y las tendencias contractuales para el manejo de las obras.

1. *Proveedores de servicios de Internet (PSI)*

En el manejo de las obras en Internet, se ha hablado mucho de la responsabilidad de los diferentes actores, tales como los autores, los usuarios de los derechos, las empresas que distribuyen o comercializan las obras y la responsabilidad de quienes prestan el servicio de Internet.

En cuanto a los últimos, qué responsabilidad pueden tener por las acciones ilegales, como la piratería que realice uno de sus usuarios. La respuesta es clara; obviamente los proveedores de servicios de Internet no pueden asegurar que sus usuarios usen las obras legalmente, pero sí pueden establecer acciones que mitiguen el mal uso, y que ayuden a los autores y titulares a tomar acciones efectivas en contra de quienes vulneran sus derechos. En consecuencia, los proveedores de servicio de Internet podrían actuar de la siguiente manera:

³ Vega, Alfredo, *Manual de derecho de autor*, Bogotá, Dirección Nacional de Derecho de Autor, 2010, pp. 45 y 46.

- Detectar el uso ilegal de obras reiterativo que uno de sus usuarios realice, y así iniciar un proceso de notificación de la acción ilegal.
- Dar de baja de una página web, por ejemplo, una obra que está colgada en la red de manera ilegal, cuando el autor o titular les notifique debidamente.

Al respecto, la doctrinante Gina Spin, señala:

Internet ha sido una de las innovaciones más importantes del siglo XX. La rápida, segura y económica capacidad para la distribución de la información digital, lleva a que casi todas las personas puedan recibir y enviar textos, imágenes, sonidos, datos o *software* con sólo tocar un botón.

Es allí donde el papel de los proveedores de servicios de Internet, o ISP, vienen a jugar un papel determinante, al ser éstos, quienes, haciendo posible la conexión entre los usuarios de Internet y los contenidos incorporados a los sitios de la red, vienen a ser también los que tienen un control más próximo a los materiales alojados.⁴

En muchos países aún no se ha regulado el actuar de los proveedores de servicios de Internet a pesar que ya es una necesidad. Para enfrentar la actual cultura de ilegalidad que existe en el entorno digital, deben unirse todas las instituciones y actores pertenecientes al uso de obras, por lo que se hace necesario que en cada país se establezca una acción efectiva no judicial de protección de los autores y titulares, que tenga su fundamento en los proveedores de servicios respectivos.

Frente a la responsabilidad de los Proveedores de Servicios de Internet (PSI o ISP por sus siglas en inglés), y a las acciones que éstos deberían tomar en función de la protección de los autores, el doctor Rafael Gamboa señala:

Respecto a si debe haber un procedimiento administrativo o judicial previo, coercitivamente debe haberlo, pero si el ISP sabe de un material ilícito y no lo baja esperando la orden judicial o administrativa, la responsabilidad se le puede ir incrementando. Si por el contrario, notifican al ISP por cierto material ilícito y el ISP mira y no lo hay, entonces como prueba, fotocopie la página web, día, hora, para demostrar que ese día No había tal material ilícito. Pueden los ISP, por razones políticas, bajar la información sin haber recibido la orden administrativa o judicial. Es el ejemplo de los códigos de conducta. En conclusión, lo mejor es que los mismos ISP sean los que regulen su responsabilidad a través de regulaciones fundamentadas en sus posiciones

⁴ Spin, Gina Paola, *Revista El Derecho de Autor*, 2006, p. 77.

políticas, o sea, aun sin notificación el ISP puede por sí mismo bloquear el acceso a ciertas páginas, como las de las autodefensas o las guerrillas, o de pornografía, para protegerse ellos mismos. Es una posición derechista. Todo se restringe a una decisión política para salvaguardarse de responsabilidad.⁵

Es evidente que los ISP deben tener una responsabilidad sobre los actos ilegales que realicen sus usuarios o, por lo menos, colaborar para ser parte de un proceso efectivo que permita evitar un perjuicio para los autores. Será responsabilidad de cada Estado establecer las reglas de juego para los procesos de protección de los autores en Internet, a través de los proveedores de servicio de Internet.

2. *Derechos de los usuarios*

Otro tema importante del desarrollo de los derechos de propiedad intelectual en Internet, es el relacionado con los derechos de los usuarios frente a los derechos de los diferentes titulares de propiedad intelectual. Actualmente, el principal fundamento para argumentar el uso ilegal de obras en Internet, increíblemente, es la pelea por el respeto de derechos de primera importancia como la educación, la cultura o la libertad de expresión. Suena un poco incoherente que en virtud del respeto a la educación se deba vulnerar los derechos de los autores, pero es la realidad social. ¿La protección del derecho de autor impide el desarrollo de la sociedad? No es posible considerar que en el momento de la historia de la humanidad en el que más acceso a información se tiene de forma masiva, se establezca que la educación o la información se vean afectadas por los derechos que hacen los creadores sobre sus obras.

Tampoco es admisible que las personas justifiquen su ilegalidad en el manejo de las obras, bajo la excusa de compartir, es decir, que, culturalmente, las personas piratean, pues señalan, que no poseen un ánimo de lucro. Frente al autor, el uso ilegal de una obra no depende del ánimo de lucro, sino de la ilegalidad misma, ya que cualquier uso indebido genera perjuicios al titular y a la economía de los países directamente.

Sin duda, deben generarse mecanismos que permitan a la sociedad gozar del uso de las obras literarias y artísticas, siempre y cuando no afecte la denominada regla de los tres pasos, la cual expresa lo siguiente: i) las formas de utilización libre de las obras deben ser taxativas; ii) no debe causarse un

⁵ *Ibidem*, p. 92.

perjuicio injustificado al autor, y iii) no debe afectarse la normal explotación de la obra.

Para crear un equilibrio entre los derechos de la sociedad y los derechos de los autores y titulares, se han estipulado las siguientes figuras:

i) Protección limitada en el tiempo: Los autores gozan de los derechos morales y derechos patrimoniales. Estos últimos son derechos de autorizar o prohibir las diferentes formas de explotación de una obra o prestación. Con el fin de generar este equilibrio, las legislaciones decidieron que la protección de estos derechos sea limitada en el tiempo, para que, una vez que finalice dicho término, las obras entren al denominado dominio público, es decir, que las obras se podrán utilizar libremente sin requerir la autorización del autor.

Por ejemplo, en países como Perú, Ecuador o Estados Unidos, la protección de los derechos patrimoniales tiene una duración de la vida del autor y setenta años después de su muerte, en México son cien años después de la muerte del autor, y en Colombia son ochenta años. Una vez que se cumpla dicho término las obras entran al dominio público.

ii) En segundo lugar, tenemos uno de los principales principios del derecho de autor a nivel mundial, el cual expresa que las ideas no se protegen. El derecho de autor protege las obras literarias y artísticas, es decir, la materialización de las ideas a través de esta forma de expresión, pero no las ideas por sí solas.

Por ejemplo, en la ley colombiana se estipula lo siguiente en relación con la no protección de las ideas:

Artículo 6o. Los inventos o descubrimientos científicos con aplicación práctica explotable en la industria, y los escritos que los describen, sólo son materia de privilegio temporal, con arreglo al artículo 120, numeral 18, de la Constitución.

Las ideas o contenido conceptual de las obras literarias, artísticas y científicas no son objeto de apropiación. Esta ley protege exclusivamente la forma literaria, plástica o sonora, como las ideas del autor son descritas, explicadas, ilustradas o incorporadas en las obras literarias, científicas y artísticas.

Las obras de arte aplicadas a la industria sólo son protegidas en la medida en que su valor artístico pueda ser separado del carácter industrial del objeto u objetos en las que ellas puedan ser aplicadas.⁶

⁶ Congreso de la República de Colombia, Ley 23 de 1982, artículo 6o.

iii) Por último, la ley contempla las denominadas limitaciones y excepciones al derecho de autor, las cuales son aquellos usos de obras que no requieren de la autorización del autor o titular del derecho para su utilización, cuando la obra todavía se encuentra dentro del término de protección. Sobre este punto profundizaremos a continuación.

3. Limitaciones y excepciones al derecho de autor

Son los usos libres de una obra durante su término de protección, siempre y cuando no afecten al autor o a la explotación misma de la obra.

El Tratado de la OMPI de 1996, para la protección de las obras literarias y artísticas, señala en su artículo 10 lo siguiente:

1) Las Partes Contratantes podrán prever, en sus legislaciones nacionales, limitaciones o excepciones impuestas a los derechos concedidos a los autores de obras literarias y artísticas en virtud del presente Tratado en ciertos casos especiales que no atenten a la explotación normal de la obra ni causen un perjuicio injustificado a los intereses legítimos del autor.

2) Al aplicar el Convenio de Berna, las Partes Contratantes restringirán cualquier limitación o excepción impuesta a los derechos previstos en dicho Convenio a ciertos casos especiales que no atenten a la explotación normal de la obra ni causen un perjuicio injustificado a los intereses legítimos del autor.⁷

Cada legislación tiene la facultad de establecer las limitaciones y excepciones que considere pertinentes, siempre y cuando no vaya en contra de los principios establecidos en los principales tratados internacionales en la materia. Al respecto, podemos encontrar como limitaciones y excepciones al derecho de autor, el derecho de cita, los fines educativos, los fines informativos, la copia privada, el uso para las bibliotecas, entre otras.

Son varios los usos que se otorgan de manera libre, con el fin de crear un equilibrio entre los derechos de los autores y la sociedad. Sin embargo, la aplicación de las limitaciones y excepciones en Internet no parece tan clara, ya que por ejemplo, en el entorno analógico hablar de la copia privada sin fines de lucro es legal, pero implementar la copia privada en el entorno digital con la posibilidad de que una persona descargue cualquier cantidad de obras, no parece legal, ni justo para los autores.

Durante los últimos años se han hecho varios llamados de atención para que las entidades públicas encargadas de la materia actualicen el catálogo

⁷ Tratado de la OMPI, para la protección de las obras literarias y artísticas, artículo 10.

existente de limitaciones y excepciones o, en su defecto, se cree uno nuevo destinado únicamente al entorno digital.

4. *Contratos y licencias*

Dentro del uso de obras en Internet se han desarrollado algunos aspectos contractuales que es importante mencionar. En primer lugar, tenemos los contratos de cesión de derechos; son aquellos en los que el autor o el titular de los derechos patrimoniales ceden algunos o la totalidad de los mencionados derechos sobre las obras a un tercero.

Por otro lado, tenemos las licencias de uso, las cuales son contratos en donde el autor no transfiere los derechos patrimoniales de su obra, sino que únicamente autoriza el uso de la misma a un tercero.

Es habitual encontrar en Internet este tipo de contratos, por ejemplo, existen bases de datos con miles de fotografías, quienes otorgan licencias de uso a agencias de publicidad, para que pueda utilizar dichas fotos, pagando una suma anual o mensual dependiendo del caso. Otro ejemplo es el uso del *software* Office, en donde cada persona debe comprar la licencia respectiva y así utilizar la obra con las restricciones que el mismo contrato establezca.

Otro tipo de licencias que han tomado fuerza en la red, son las denominadas licencias libres, en donde el autor manifiesta su intención de dejar que cualquier persona utilice libremente una obra colocando algunos parámetros para su uso. Por ejemplo, un autor podrá manifestar su deseo del uso libre de una obra pero sin fines comerciales; a otro sólo le interesará dejar libre la comunicación pública de la obra, y así, cada autor determinará qué tanta libertad otorga a las personas interesadas en utilizar una obra.

5. *Los nombres de dominio*

El doctrinante Wilson Ríos, en relación con los nombres de dominio, establece:

El Servicio de Nombres de Dominio (DNS, por sus siglas en inglés) ha sido administrado por la Autoridad de Asignación de Números en Internet (Internet Assigned Numbers Authority, IANA), teniendo en cuenta para ello la norma 3166 de la Organización Internacional de Normalización (International Standard Organization, ISO). Las direcciones o dominios en internet son simplemente una referencia o transmutación que se hace de una dirección IP,

constituida por una secuencia de números, a su correspondiente referencia en letras o nombre entendibles y de fácil recordación y comprensión.⁸

El nombre de dominio es la dirección electrónica de un sitio web para darse a conocer en Internet, y que a cada titular debe otorgársele una protección para evitar confusión en los consumidores. Precisamente, esta protección buscó que se considerarán las denominadas causales de ciber-ocupación o registro abusivo, donde una persona natural o jurídica, perjudicada por la adquisición y puesta en funcionamiento de un nombre de dominio, pudiera tomar las acciones correspondientes para la defensa de sus intereses. Las causales de registro abusivo son las siguientes.

a. Que el nombre de dominio sea igual o semejante a una marca

En el caso en que una persona natural o jurídica adquiriera un nombre de dominio que sea igual o semejante a una marca ya registrada, el afectado y titular legítimo de la marca podrá tomar las acciones correspondientes para solicitar la cancelación del nombre de dominio al infractor o, en su defecto, que el mismo sea transferido a él. Es preciso señalar que la protección de los nombres de dominio busca principalmente proteger al consumidor para que no caiga en error o confusión, y a los titulares marcarios por su derecho sobre la marca.

b. Que el titular del nombre de dominio no tenga un derecho o interés legítimo sobre el mismo

En caso de un conflicto por el uso de un nombre de dominio, el titular del mismo deberá probar que él tiene un legítimo interés sobre dicho nombre, ya sea porque es el nombre de su empresa, su propio nombre, alguna referencia a la labor que desempeña, entre otros.

Con esta causal se pretende evitar que la adquisición de un nombre de dominio se haga sin un interés particular, fundado en el deseo de perjudicar a una persona o a una empresa.

⁸ Ríos, Wilson, *La propiedad intelectual en la era de las tecnologías de información y comunicaciones*, Bogotá, Uniandes, 2009, p. 443.

c. Que el nombre de dominio haya sido registrado o se utilice de mala fe

La adquisición de un nombre de dominio puede constituir un acto de mala fe y generarle perjuicios a una persona o a una empresa. Podrá constituir mala fe, por ejemplo, cuando una persona pretende vender o alquilar al titular legítimo de una marca un dominio igual o semejante a la misma, o cuando se obtiene un nombre de dominio con el fin de perturbar los negocios de un competidor.

Además de las mencionadas causales, existe un conflicto relacionado entre el derecho marcario y la regulación de los nombres de dominio, toda vez que en principio la protección marcaria es territorial, es decir, solamente se protege en el país donde se registra, mientras que el nombre de dominio rompe las fronteras territoriales. Cómo podría protegerse un titular marcario en un determinado país, cuando una persona, al otro lado del mundo, obtiene un nombre de dominio igual al de su marca. Es una situación que actualmente se encuentra en debate, pues no existe un registro internacional de marcas que abarque cada uno de los países del mundo y que le permita al titular tener una cobertura total con un solo registro, por lo que es necesario llegar al registro de la marca país por país como actualmente se debe realizar.

Al respecto, la Organización Mundial de la Propiedad Intelectual, en su primer Informe sobre Nombres de Dominio, manifestó lo siguiente:

A medida que ha ido expandiéndose la red Internet, los nombres de dominio han entrado en un creciente conflicto con las marcas comerciales. Esa posibilidad de conflicto surge por la falta de conexión entre el sistema de registro de las marcas, por un lado, y el sistema de registro de los nombres de dominio, por el otro. El primer sistema (marcas) lo administra una autoridad pública (gubernamental) sobre una base territorial (nacional o regional) que da lugar a derechos que el titular de la marca puede ejercer en el territorio pertinente. El segundo sistema (nombres de dominio) lo administra generalmente una organización no gubernamental sin ninguna limitación funcional: los nombres de dominio se registran por orden de llegada y ofrecen una presencia mundial en Internet.⁹

Por lo pronto, la obtención de un nombre de dominio es un proceso bastante sencillo y económico, por el cual se le otorga una titularidad

⁹ Organización Mundial de la Propiedad Intelectual, Primer Informe sobre Nombres de Dominio, www.wipo.int, consulta: enero de 2014.

y monopolio a una persona natural o jurídica sobre una dirección web que se compone de los siguientes elementos. En primer lugar, tienen las letras `http://` iniciales de Hyper Text Transfer Protocol (Protocolo de transferencia de hipertexto), seguido de las letras `www`, las cuales significan World Wide Web o Red Mundial de Información en español. Acto seguido, se indica el nombre que la persona o el empresario escoja, el cual puede ser su marca, su propio nombre o cualquier otra referencia, siempre y cuando no exista como nombre de dominio en el momento del registro. Finalmente, se estipulan las siglas relacionadas con la naturaleza de la página, por ejemplo, `.com` en relación con actividades comerciales, `.gov` o `gob` para páginas gubernamentales, `.edu` para instituciones de educación, entre muchas otras. En algunos casos, se estipula la sigla correspondiente al área local, como `.co` para Colombia, `.mx` para México, `.uk` para el Reino Unido o `.jp` para Japón.

En el momento de la compra de un nombre de dominio, quien lo obtiene acepta unas condiciones contractuales con el registrador, dentro de las cuales se encuentra la obligación de someterse al procedimiento alternativo para la solución de conflictos. Actualmente, es la Organización Mundial de la Propiedad Intelectual la que, dentro de sus funciones, ostenta el manejo del Centro de Arbitraje y Conciliación en Materia de Propiedad Intelectual de la OMPI, para la solución de controversias en materia de nombres de dominio, proceso que busca la anulación, cancelación o transferencia del registro de nombre de dominio infractor.

6. *El impacto de las marcas en Internet*

Las marcas son el bien intangible que más ha tomado una fuerza económica gracias a su interacción dentro del mundo digital. La marca, como signo que identifica un producto o servicio en el mercado, antes estaba limitada a las barreras análogas para su difusión e impacto, tales como periódicos, carteles, radio o televisión, entre otras. Sin embargo, con la llegada de Internet, y como principal medio de intercambio de información, creó un camino, un espacio para que de una manera sencilla, una marca pudiera llegar a todos los rincones del planeta, generando innumerables ganancias para sus titulares.

Si bien, Internet es un mecanismo que permite que los internautas puedan utilizar las marcas, es también un blanco fácil de quienes pretenden aprovecharse de la reputación de ellas y sacar un provecho económico, ya

sea utilizando una marca sin la debida autorización, copiándola o explotando una semejante que podría generar confusión en los consumidores.

En primer lugar, debemos recordar que las marcas son territoriales, es decir, solamente se protegen en el país donde se registran y por un término determinado, renovable por el mismo término sucesivamente mediante el pago de una tasa oficial. Además, las marcas están sujetas al denominado principio de especialidad, el cual hace relación a la unión de un signo con un producto o servicio determinado de conformidad con la Clasificación Internacional de Niza, la cual constituye un listado enumerado del 1 al 45, donde se organizan todos los productos y servicios existentes.

Teniendo en cuenta que las marcas son territoriales y están ligadas a un producto o servicio en particular, existen formas de utilizarlas y explotarlas sin vulnerar los derechos de los titulares, sin embargo, lo más común actualmente es apropiarse de una marca protegida y darle un uso indebido a través de los medios digitales.

Las acciones para la protección de las marcas son de dos tipos principalmente. En primer lugar, encontramos las acciones penales en aquellos Estados donde su legislación ha contemplado que la usurpación o uso indebido de las marcas constituye un delito. Por otra parte, otra acción judicial es a través de un procedimiento civil, en donde se busca detener la acción ilegal y obtener una indemnización por los perjuicios causados.

Hoy en día, la valoración del impacto económico de las marcas no se hace de forma general, sino de forma específica teniendo en cuenta páginas web, redes sociales o publicidad a través de medios digitales, es decir, que es tal el impacto de una marca, que por ejemplo, existen estudios de las mismas sólo frente a su valor en páginas de redes sociales como Facebook o Twitter. Por ejemplo, la Interactive Advertising Bureau realizó un estudio sobre el impacto de las marcas referentes a los equipos de fútbol españoles en Facebook, dando como resultado que el valor de la marca Real Madrid en esta red social tiene un valor aproximado de 30 millones de euros, frente a 13 millones del Barcelona y 262 000 del Valencia.¹⁰

Frente a este evidente crecimiento económico de las marcas por su interacción en Internet, y el aumento en los delitos de infracción marcaria registrados por la misma razón, no son pocos los titulares que solicitan una adecuación frente a la territorialidad de las marcas, para que se creen mecanismos que faciliten el registro internacional de las mismas. Si bien existe el denominado Tratado de Madrid, el cual es un procedimiento que facilita el registro internacional de las marcas, éste no es suficiente frente a la

¹⁰ La Vanguardia.com, *Estudio de las Interactive Advertising Bureau*, 28 de julio de 2011.

necesidad de romper fronteras, tal como lo hace el entorno digital. Es muy difícil que los países accedan a crear un registro único internacional de marcas y que pierdan su autonomía frente a la decisión de conceder o no una de ellas, no sólo por cuestión de soberanía, sino porque el registro de marcas representa una gran tasa anual que entra a las arcas de los Estados.

IV. CONCLUSIONES

El uso de las tecnologías se ha convertido en el principal reto de la protección que la propiedad intelectual otorga a las diferentes creaciones del intelecto, no sólo por los nuevos usos y alcances que les ha brindado sino por la masiva cultura de vulneración de estos derechos. Los Estados se han quedado atrás en los intentos de regular la protección de la propiedad intelectual en Internet, toda vez que simplemente han creado pequeñas disposiciones que pretenden actualizar las normas ya existentes en la materia, sin entender la necesidad de hacer un alto en el camino y crear una norma completa, que permita visualizar cada uno de los aspectos del uso de creaciones en el ambiente analógico y digital.

En el marco del derecho de autor, temáticas como la responsabilidad de los proveedores de servicios de Internet, los mecanismos no judiciales para la protección de las obras o las limitaciones y excepciones, requieren de una pronta regulación, y así fortalecer la protección de las obras literarias y artísticas por sus usos ilegales en la red sin importar su país de origen.

Es indispensable que la legislación en materia de derecho de autor establezca nuevos modelos de negocio que faciliten a los usuarios la adquisición de obras de forma legal, fácil y a un precio cómodo. Buscar estos mecanismos permitiría volver a una cultura de legalidad por el derecho de autor, lo que traería incentivos al creador y beneficios económicos para los países.

En relación con los nombres de dominio, al estudiar su funcionamiento, desarrollo y mecanismos de protección y registro, podemos llegar a la conclusión que una de las tareas más importantes que tienen las autoridades al respecto, es la de relacionar el registro de marcas con el registro de nombres de dominio, y así brindarle más garantías no sólo a los diferentes titulares marcarios, sino al consumidor mismo, quien es el directamente afectado por la confusión y el uso ilegal o indebido de marcas y nombres de dominio.

Finalmente, en relación con las marcas, debe resaltarse la importancia que las mismas han tenido como motor económico de las empresas y países, pues su utilización dentro del medio digital es indispensable para todas aquellas labores de publicidad y promoción comercial de productos y servi-

cios. En tal sentido, una protección marcaria eficaz defendería los intereses de la sociedad, la cual podrá identificar claramente los productos y servicios de su preferencia sin caer en engaño o confusión con otros signos que puedan ser iguales o semejantes. De conformidad con todo lo anterior, más importante aun que una nueva regulación en la materia, es generar una cultura de respeto por los derechos de propiedad intelectual, y la necesidad de que la sociedad reconozca la importancia de los creadores y de brindarles incentivos que motiven la creación.

V. BIBLIOGRAFÍA

- RÍOS, Wilson, *La propiedad intelectual en la era de las tecnologías de información y comunicaciones*, Bogotá, Uniandes, 2009.
- SPIN, Gina Paola, *Revista El Derecho de Autor*, 2006.
- VEGA, Alfredo, *Manual de derecho de autor*, Bogotá, Dirección Nacional de Derecho de Autor, 2010.
- LIPSYC, Delia, *Derecho de autor y derechos conexos*, CERLALC, Zabalía, UNESCO, 2006.
- RODRÍGUEZ, Sofía, *La era digital y las excepciones y limitaciones al derecho de autor*, Universidad Externado, 2004.

EL DERECHO DE AUTOR EN INTERNET Y LAS RESPONSABILIDADES DE LOS PROVEEDORES DE SERVICIOS DE INTERNET

Jonathan Gabriel GARZÓN GALVÁN*

SUMARIO: I. *Introducción*. II. *Derechos de autor*. III. *Responsabilidad de los proveedores de Servicios de Internet (PSI)*. IV. *Sistemas de protección*. V. *Conclusiones*. VI. *Bibliografía*.

I. INTRODUCCIÓN

La red de Internet ha sido un motor de desarrollo para diversos sectores e industrias, permitiéndoles alcanzar nuevos clientes y mercados de forma ágil y a menor costo.¹ Estos beneficios también se han permeado dentro de la industria autoral, donde los autores tienen plataformas para dar a conocer y explotar sus obras a una audiencia a nivel global sin requerir de fuertes cantidades de inversión. Inclusive los usuarios de la red, al realizar videos o

* Especialista en temas de derecho y tecnología, con experiencia en la implementación de soluciones y herramientas legales relacionadas con la protección de datos personales, firma electrónica avanzada, factura electrónica, protección de propiedad intelectual y derechos de autor en Internet, contratación electrónica, etcétera. Es licenciado en derecho con mención honorífica por la Barra Nacional de Abogados, licenciado en ciencia política y administración pública con mención honorífica por la UNAM y cuenta con los grados de maestro en derecho de la empresa con mención honorífica emitido por la Universidad Panamericana y maestro en comercio electrónico por el Instituto Tecnológico de Estudios Superiores de Monterrey. Actualmente, es gerente de proyectos y productos de tecnología en Cecoban, S.A. de C.V., y profesor de posgrado en el ITAM, La Salle, Universidad Panamericana y el ITESM. Fungió como miembro del Consejo Directivo y Vicepresidente Jurídico de la Asociación Mexicana de Internet (AMIPCI) durante los periodos 2011 y 2012.

¹ *Cfr.* Organisation for Economic Co-operation and Development (OECD), *The Seoul Declaration, the Future of Internet Economy*, Korea 2008 pp. 5-7. Recuperado de <http://www.oecd.org/internet/consumer/40839436.pdf>, fecha de consulta 4 de marzo de 2014.

audios y escribir blogs o diferentes textos en las redes sociales, podrían convertirse en autores de obras protegidas por derechos de autor sin conocerlo.

Con la red de Internet, la industria autoral percibe que sus derechos están siendo vulnerados cuando los materiales digitales de su creación son compartidos, visualizados y descargados de forma viral. Hoy una obra puede ser reproducida, compartida y descargada por miles de usuarios sin la autorización del autor.

Esta industria ha señalado que la piratería generalizada es el principal culpable del debilitamiento del negocio de la música digital. Los servicios de contenido legítimos en Internet, sea cual sea su modelo, deben adquirir las licencias y remunerar a los titulares de los derechos de autor, además de invertir en infraestructura segura y soporte de calidad, lo cual se torna insostenible cuando se compite con sitios ilegales que no remuneran a los titulares de los derechos de autor y evaden la normativa.

Para los autores proteger sus obras de forma individual y colegiada significa enfrentar la búsqueda, identificación y seguimiento de un gran número de posibles infracciones en una red global como lo es Internet, mientras que el contenido de sus creaciones se sigue descargando y compartiendo sin restricción alguna, lo cual genera una carga adicional y desproporcionada para ellos. El hecho que dicha protección se vea afectada, y que sea bastante complejo evitar que un contenido continúe siendo descargado o compartido, así como la dificultad para conocer la identidad de quién lo está realizando, ocasiona la reducción del incentivo para producir nuevas obras y tecnologías.

Con estos criterios la industria autoral ha considerado que los Proveedores de Servicios de Internet (PSI o ISP por sus siglas en inglés, *Internet Service Providers*), podrían ser parcialmente responsables de los contenidos que comparten y descargan los usuarios de forma ilegal a través de sus redes y servicios.

En este tenor, juicios y controversias se han analizado a lo largo del mundo sin resoluciones o criterios homogéneos. Por ello, algunos países buscaron hacer adecuaciones regulatorias para contemplar puertos seguros a los PSI, y elementos para proteger a los titulares de derechos de autor: EUA con la *Digital Millennium Act*, la Unión Europea con la Directiva 98/34/CE, así como Canadá, Chile y Francia, todos ellos contando con modelos de protección diferente.

Estos modelos tienen por objeto una mayor protección, pero también pueden ser modelos donde se llegan a generar abusos que encarecen los servicios de Internet o que obligan a los proveedores de servicios a desconectar

personas, o afectar derechos de los usuarios como su privacidad, libertad de expresión, entre otros derechos.²

Al momento de la redacción del presente artículo, México se encuentra en negociación y ratificación de tratados internacionales como el Acuerdo Estratégico Trans-Pacífico de Asociación Económica (en inglés: *Trans-Pacific Strategic Economic Partnership* o *Trans-Pacific Partnership*, o TPP) y el Acuerdo Comercial Anti-falsificación (en inglés: *Anti-Counterfeiting Trade Agreement*, o ACTA), así como reformas nacionales en materia de telecomunicaciones y derechos de autor, que con base en la protección del derecho de autor podrían llegar a responsabilizar de manera indirecta a los PSI en caso de que no monitoreen las comunicaciones realizadas en Internet, afectando el funcionamiento actual de Internet con la posibilidad de repercutir en calidad o costo del servicio a los usuarios, lo cual afectaría los esfuerzos nacionales e internacionales de reducir la brecha digital y aumentar el acceso a la red en mayor medida, así como perturbar derechos humanos de los usuarios de los servicios de Internet.

El objetivo del presente artículo es proporcionar un documento explicativo y de análisis a los diferentes interesados en el tema que sirva para orientar y entablar discusiones futuras en los diferentes foros que al respecto se lleven a cabo. Analizando de inicio las generalidades respecto de los derechos de autor y las principales problemáticas que el abuso de algunos usuarios en red de Internet ha provocado a los intereses de los titulares de dichos derechos. Posteriormente se analizarán los marcos de responsabilidad que pudieran llegar a aplicárseles a los PSI, y finalmente los modelos que se han implementado en otros países para solventar estos conflictos.

II. DERECHOS DE AUTOR

La Organización Mundial del Comercio (OMC) establece que el principal objetivo de la protección del derecho de autor y los derechos conexos es fomentar y recompensar la labor creativa, es decir, si un autor está protegido se ve estimulado para crear obras, enriqueciendo la literatura, el teatro, la música, e incluso los programas de cómputo de su país.³

² Zucchini, Clara, *La responsabilidad de los ISPs por los contenidos generados y transmitidos por los usuarios*, Certamen IP 2008: mentes innovadoras para el desarrollo, 2a. ed., Argentina, 2008, pp. 7-11. Recuperado de https://www.u-cursos.cl/derecho/2011/2/D124T07237/35/material_docente/bajar?id_material=411759, fecha de consulta, 4 de marzo de 2014.

³ Rangel Medina, David, *Derecho de la propiedad industrial e intelectual*, UNAM, Instituto de Investigaciones Jurídicas, México, 1992, p. 91.

El derecho autoral siempre ha sido un derecho que cada país otorga dentro de sus fronteras, es decir, es un derecho territorial, lo cual era funcional derivado del carácter relativamente limitado de la circulación de las obras.⁴ Sin embargo, a raíz de un mayor flujo internacional de productos y servicios, se requirió de acuerdos bilaterales y posteriormente multilaterales, los cuales, en general, establecen que el autor tiene dos tipos de prerrogativas respecto de sus obras: los derechos morales y los derechos patrimoniales, los primeros son aquellos que le permiten al autor tomar ciertas medidas para preservar un vínculo entre él y su obra, destacan: a) el derecho de paternidad (aparecer como autor de la obra, y la salida al comercio de la misma), y b) el derecho de integridad (autorizar su traducción, adaptación, interpretación o cualquier tipo de modificación). Este tipo de derechos están íntimamente unidos al autor por lo que son inalienables, imprescriptibles, irrenunciables e inembargables, e incluso le permite que después de la muerte del autor los herederos salvaguarden los intereses morales del autor, al ser la obra como un reflejo de su personalidad.⁵

Los derechos patrimoniales son aquellas facultades que tiene el autor de autorizar o prohibir la explotación de sus obras u obtener una retribución económica por su uso.⁶ Entre las formas de explotación existen varias, pero sólo se ahondará en aquellas que por su relación la forma en que se prestan los servicios a través de la red de Internet sean relevantes.

1. *Reproducción*. Se refiere a la realización de uno o varios ejemplares de una obra en cualquier forma. Es el derecho fundamental de los derechos patrimoniales, el cual permite a su titular autorizar o prohibir que se creen copias de su obra. Aquí, cabe señalar que derivado del funcionamiento de Internet, los PSI requieren para guiar los paquetes de información hasta su destino final, almacenar temporalmente el contenido de la transmisión (que pudiera ser una obra protegida), en la memoria temporal de un enrutador. Por tanto, si esta copia se considera como reproducción, el PSI, el dueño

⁴ Comisión de las Comunidades Europeas (CCE), *Libro verde: los derechos de autor y los derechos afines en la Sociedad de la Información*, Bélgica, 1995, p. 24.

⁵ Rangel Medina, David, *op. cit.*, nota 3, p. 102.

⁶ Cfr. Organización Mundial de Propiedad Intelectual (OMPI), *Principios básicos del derecho de autor y los derechos conexos*, p. 8. Recuperado de: http://www.wipo.int/export/sites/www/freepublications/es/intproperty/909/wipo_pub_909.pdf, fecha de consulta, 6 de marzo de 2014.

o usuarios de la computadora o servidor que realiza esta copia transitoria podría estar cometiendo una infracción.⁷

Otra copia que se realiza debido a funciones informáticas que buscan la optimización de las aplicaciones, es la que se queda en la memoria *caché*. Ésta se genera debido a que cuando a través de una computadora o servidor se accede por primera vez a algún contenido dentro de la red, se hace una copia en la memoria *caché* de dicho equipo; los futuros accesos se realizan a dicha copia, haciendo que el tiempo de acceso al contenido sea menor.

Cuando el equipo necesita leer o escribir en una ubicación en memoria principal, primero verifica si una copia de los datos está en el *caché*. Si es así, el procesador de inmediato lee o escribe en la memoria *caché*, que es mucho más rápido que la lectura o la escritura a la memoria principal. Por lo anterior esta función también podría considerarse una infracción.

La LFDA, en la definición de reproducción, incluye cualquier almacenamiento permanente o temporal por medios electrónicos, y no hace excepción en la facultad del titular de autorizar y prohibir la reproducción cuando sea en memoria temporal o *caché*, por lo que en México los escenarios antes señalados sí se considerarían infracciones, si es que no se llega a comprobar que está dentro de alguna excepción enmarcada por la ley.⁸

2. *Publicación*. La reproducción de la obra en forma tangible y su puesta a disposición del público mediante ejemplares, o su almacenamiento permanente o provisional por medios electrónicos, que permitan al público leerla o conocerla visual, táctil o auditivamente.

3. *Comunicación pública*. Acto mediante el cual la obra se pone al alcance general, por cualquier medio o procedimiento que la difunda y que no consista en la distribución de ejemplares. Esta facultad viene recogida por el artículo 8o. del WCT, y se amplía a que el público pueda acceder a las obras desde el lugar y en el momento que cada uno de ellos elija.

Con la definición anterior podría interpretarse que si un usuario pone al alcance de una pluralidad de personas, a través de las plataformas de servicios de los PSI, alguna obra protegida, podría estar infringiendo los derechos de autor, siempre que no exista una excepción aplicable a esa comunicación.

4. *Ejecución o representación pública*. Presentación de una obra, por cualquier medio, a oyentes o espectadores, sin restringirla a un grupo privado o

⁷ Cfr. Piñeiro Ugarte, Lorena, “Responsabilidad de los ISPs por violación a la propiedad intelectual: Estados Unidos, Europa y Chile”, *Revista Chilena de Derecho Informático*, Chile, 2011, pp. 173 y 174.

⁸ Artículos 16 y 27 de la LFDA.

círculo familiar. En este caso no se considera pública la ejecución o representación que se hace de la obra dentro del círculo de una escuela o una institución de asistencia pública o privada, siempre y cuando no se realice con fines de lucro.

5. *Distribución al público*. Es la puesta a disposición del público del original o copia de la obra mediante venta, arrendamiento y, en general, cualquier otra forma.

Los derechos patrimoniales tienen un periodo de vigencia reconocido, el Convenio de Berna establece un mínimo de 50 años después de la muerte del autor, siendo México el único país que actualmente lo protege por más de 100 años después de la muerte del autor. Estados Unidos y la Unión Europea tienen un plazo de 70 años posteriores a la vida del autor.⁹

Estas prerrogativas tienen ciertas limitaciones, es decir, pueden utilizarse sin autorización del titular y sin remuneración, en casos muy específicos, siempre que no se afecte la explotación normal de la obra, se cite la fuente y no se altere la obra. Estos casos específicos quedan determinados por cada país conforme al artículo 9.2 del Convenio de Berna. En México, en el artículo 148 de la LFDA se establecen los casos específicos.¹⁰

Antes de continuar con el análisis, es importante recordar que la legislación mexicana ofrece una amplia protección en materia de derechos

⁹ Cfr. Xalabarder, Raquel, “Copyright y derecho de autor: ¿convergencia internacional en un mundo digital?”, *IDP Revista de Internet, Derecho y Política*, núm. 1, España, 2005, pp. 3 y 4. Recuperado de <http://www.uoc.edu/idp/1/dt/esp/xalabarder02.pdf>, fecha de consulta, 12 de febrero de 2014.

¹⁰ Los supuestos establecidos son:

I. Cita de textos, siempre que la cantidad tomada no pueda considerarse como una reproducción simulada y sustancial del contenido de la obra.

II. Reproducción de artículos, fotografías, ilustraciones y comentarios referentes a acontecimientos de actualidad, publicados por la prensa o difundidos por la radio o la televisión, o cualquier otro medio de difusión, si esto no hubiere sido expresamente prohibido por el titular de derechos de autor.

III. Reproducción de partes de la obra, para la crítica e investigación científica, literaria o artística.

IV. Reproducción por una sola vez, y en un solo ejemplar, de una obra literaria o artística, para uso personal y privado de quien la hace y sin fines de lucro. Las personas morales no aplican esta excepción salvo que se trate de una institución educativa, de investigación, o que no esté dedicada a actividades mercantiles.

V. Reproducción de una sola copia, por parte de un archivo o biblioteca, por razones de seguridad y preservación, y que se encuentre agotada, descatalogada y en peligro de desaparecer.

VI. Reproducción para constancia en un procedimiento judicial o administrativo.

VII. Reproducción, comunicación y distribución por medio de dibujos, pinturas, fotografías y procedimientos audiovisuales de las obras que sean visibles desde lugares públicos.

de autor, en la vía penal, al constituir como delito grave, perseguido de oficio y con sanción personal y patrimonial la comisión de delitos contrarios al derecho de autor (artículos 424 y 424 bis del Código Penal Federal). La LFDA establece como infracción la reproducción de obras y fonogramas no autorizada, sea con ánimo de lucro directo o indirecto. En forma adicional para ambos casos se establece la posibilidad de la reparación del daño.

En adición, el artículo 234 de la LFDA y 199 bis de la Ley de la Propiedad Industrial establecen las medidas precautorias que el Instituto Mexicano de la Propiedad Industrial (IMPI) puede realizar para la protección de la propiedad intelectual, independientemente de los medios en que estas actividades se cometan y dichas leyes establecen las garantías que se otorgan al presunto infractor para mantener a salvo sus derechos en caso de que no se dicte declaración administrativa de infracción.

III. RESPONSABILIDAD DE LOS PROVEEDORES DE SERVICIOS DE INTERNET (PSI)

Actualmente, Internet es de vital importancia para las personas, los gobiernos e inclusive para los autores de la nueva generación, y esta red requiere de los PSI para funcionar y continuar desarrollándose. Pero los PSI sólo se verán impulsados a mantener estos servicios e incluso invertir en su crecimiento, si el régimen jurídico es sencillo, fiable y no impone cargas innecesarias y onerosas para ellos, contando con garantías de que no serán imputados de alguna responsabilidad por actividades que no pueden, ni deben controlar.

En el manejo de contenido protegido por derechos de autor a través de Internet existen varios roles que deben analizarse: 1) el titular de derechos de autor, que es aquella persona que tiene algún derecho moral o patrimonial sobre la obra que está dentro del contenido controvertido; 2) el PSI; 3) el proveedor del contenido, que es la persona o empresa que sube el contenido a la red, y 4) el usuario que usa o descarga el contenido. Algunos de estos roles pueden ser llevados a cabo por una misma persona al mismo tiempo, es decir el autor o productor de una canción puede ser quien también la suba a la red, en este caso es al mismo tiempo titular de derechos de autor y proveedor del contenido; o como el caso de Netflix, quien con sus series originales, es PSI, titular de derechos de autor y proveedor de contenido. Aquí comienza la problemática de si es que el titular de derechos de autor pierde sus derechos por el simple hecho de que el contenido ha sido subido a la red.

Lo primero que habría que señalar es que un usuario es responsable de los usos que hace de los diversos contenidos/obras que encuentran en Internet; de acuerdo con las condiciones que le imponga la legislación nacional sobre derecho de autor o el titular de derechos de autor. El problema radica en que en muchas ocasiones es difícil identificar en la red a una persona para hacerla responsable de la comisión de un ilícito.¹¹

Los usuarios y los proveedores de contenido son identificados con un *nickname*, del cual resulta complejo determinar su identificación real, ya que sólo el PSI podría contar con datos que logren identificar el origen de la comunicación, sobre todo si se tiene en cuenta el acelerado ritmo con que los usuarios acceden a las redes informáticas.¹²

En el caso del proveedor del contenido, es quien realmente decide compartir, subir o poner a disposición, una película, serie, canción, libro, artículo o cualquier otro contenido en la red. Este proveedor podría ser al mismo tiempo titular de derechos de autor y no existiría problema alguno; sin embargo, cuando no lo es, esta persona es responsable de los derechos relacionados, en cada caso, con un contenido determinado; pues al ponerlo en la red a disposición de los usuarios, favorece la explotación de tal contenido en forma indiscriminada.¹³

Por otro lado, es entendible, en primera instancia, el porqué de la interpretación o tendencia de responsabilizar al PSI de las actividades realizadas por los usuarios en la red de Internet, ya que sin la existencia de los servicios brindados por los PSI no podrían cargarse, descargarse, visualizarse, copiarse, compartirse y transmitirse sin autorización, con la misma calidad, de manera fácil y con costos reducidos, contenido protegido por derechos de autor, lo cual en el mundo de reproducciones físicas no era sencillo o era fácilmente diferenciable un original de una copia.¹⁴ Este argumento, si bien es real, también es engañoso. Ya que también sin la existencia de estos servicios no se obtendrían tampoco los beneficios de la Sociedad de la Información, los cuales se suponen mayores, como para limitar la existencia de los mismos.¹⁵

¹¹ Cfr. Álvarez Amézquita, David *et al.*, “Proveedores de servicios de Internet y de contenidos, responsabilidad civil y derechos de autor”, *Revista Studiositas*, Colombia, 2009, núm. 4, vol. 3, p. 53.

¹² *Idem.*

¹³ *Idem.*

¹⁴ Smedinghoff, Tomas J., *Online law: the SPA's legal guide to doing business on the Internet*, EUA, Software Publishers Association, 1996, p. 138.

¹⁵ Viviana Sarra, Andrea, *Comercio electrónico y derecho*, Argentina, Astrea de Alfredo y Ricardo Depalma, 2000, p. 242.

Su situación sería similar a la de una compañía carretera o un proveedor de servicios telefónicos, donde no es posible sostener que dichas compañías deben responder por los actos ilegales que realicen las personas en la carretera construida por ella o vía telefónica, respectivamente. Inclusive, este ejemplo podría verse aún más claro con empresas vendedoras de armas de fuego, donde en ningún momento se responsabiliza a las mismas por los actos que los compradores llegaren a realizar con ellas.

Retomando las razones para la interpretación de responsabilizar a los PSI, éstas descansan en la idea errónea de que ellos conocen, controlan o pueden conocer o controlar el contenido que fluye o está almacenado en sus servicios. Lo anterior es tecnológicamente imposible ya que el monitorear o revisar todos los contenidos e información que viaja por la red requeriría de inversiones multimillonarias donde casi se requeriría del mismo número de personas que están cargando e intercambiando contenido, para revisarlos e interpretar su legalidad.

Adicional a esto, el obligar a auditar y revisar los contenidos de las comunicaciones enviadas por Internet, se encuentra expresamente prohibido en el marco constitucional mexicano, dentro del artículo 16 constitucional, al señalar: “Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas”. Lo anterior está ratificado por el artículo 177 del Código Penal Federal que sanciona hasta con 12 años de prisión a quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente. En este último artículo, se prevé que exclusivamente sea la autoridad judicial quien pueda autorizar y ordenar la intervención de comunicaciones privadas.

Finalmente, suponiendo que fuera tecnológicamente viable y no existiera restricción legal, al permitirle un monitoreo del contenido compartido y bloquear o impedir el acceso de aquel que el PSI considere, se está usando o compartiendo sin autorización, constituye un acto de molestia originado por la simple presunción de la comisión de una infracción, lo cual sería violatorio de garantías de debido proceso, convirtiendo al PSI en una autoridad de decisión, sobre qué material infringe o no derechos de autor para llevar a cabo alguna actividad que impidiera su libre flujo.

1. Responsabilidad contractual y extracontractual (objetiva y subjetiva)

La responsabilidad civil es la obligación de indemnizar o reparar los daños y perjuicios causados a una persona en su integridad física o en su patrimonio fundamentándose en el principio de no causar daño a los demás, y

por consecuencia en el deber de reparar el daño injustamente causado. Se divide en dos categorías, la responsabilidad civil contractual y la responsabilidad civil extracontractual.¹⁶

La responsabilidad civil contractual procede de un determinado acto jurídico, de un acuerdo de voluntades –generalmente un contrato– que le da la facultad a los sujetos involucrados en dicho acto, para reclamar los daños causados. Este tipo de responsabilidad se deriva de conductas lícitas dentro de actos jurídicos, los cuales no fueron cumplidos por las personas que lo acordaron. Este tipo de responsabilidad está contenida en el artículo 2104 del Código Civil Federal (CCF).

En este tipo de responsabilidad debe considerarse que no basta que haya un contrato entre las partes, sino que se requiere que la actividad causante del daño se encuentre incluida dentro de la esfera de lo pactado y como desarrollo del contenido contractual.¹⁷

En esta situación se encuentra el PSI con los proveedores de contenido y los usuarios de la red, quienes aceptan los términos y condiciones de uso de los servicios, y donde se establecen las responsabilidades que adquieren las partes por el uso de contenido protegido por derechos de autor, y donde también se establecen mecanismos para apoyar a los autores en caso de que se esté utilizando de forma no autorizada material sobre el cual tengan derechos.¹⁸

En cuanto a la responsabilidad civil extracontractual, ésta se materializa en cualquier otro supuesto en que el daño o afectación sean causados por circunstancias ajenas a alguna relación contractual previa entre los involucrados, debiéndose acreditar culpa o negligencia por parte del sujeto a quien se le demanda. Es un derecho distinto del que nace por el incumplimiento a un contrato, pero que causa un daño.¹⁹

Esta es la responsabilidad generalmente atribuida de forma errónea a los PSI, dado que se interpreta que por una omisión de debido cuidado, al permitir el paso de contenido protegido, el PSI causa un daño al titular de derechos de autor, lo cual es incorrecto ya que está impedido por la propia ley para conocer la naturaleza de lo que pasa por sus redes y servicios.

¹⁶ Ángel, Ricardo de, *Tratado de responsabilidad civil*, Madrid, Civitas, 1993, p. 26.

¹⁷ *Ibidem*, p. 28.

¹⁸ El maestro Joel Gómez Treviño hace un análisis detallado de las políticas de algunas redes sociales como Facebook, Twitter y Youtube. Cfr. Gómez Treviño, Joel, “Retos legales para proteger los derechos de propiedad intelectual en el entorno digital”, en Pérez-Alonso, Rodrigo y Piedras Fera, Ernesto (coord.), *Una agenda digital: telecomunicaciones y tecnologías de la información en México*, México, Cámara de Diputados, LXI Legislatura, 2012, pp. 453-461.

¹⁹ Cfr. Ángel, Ricardo de, *op. cit.*, nota 16, p. 28.

La responsabilidad extracontractual se basa en la existencia de un régimen subjetivo u objetivo. El primero se encuentra fundamentado en el marco legal mexicano en el artículo 1910 del CCF y se enfoca en la persona que ha causado el daño y en el efecto que por su acción u omisión se lo causó a otro. La responsabilidad objetiva implica que se debe reparar el daño con base en el perjuicio efectivamente causado, se atribuye a la actividad humana, no a la culpa.²⁰ Bajo la óptica de este sistema, el PSI sería responsable de la reparación del daño que ha causado si es que, estando en posibilidad razonable de hacerlo, omitió conducirse con el especial cuidado que las circunstancias ameritaban para prevenir el daño a los titulares de derechos de autor, lo que se traduce en un deber de diligencia frente al titular de derechos de autor.

Por tanto, el PSI sería responsable siempre que haya culpa o negligencia de su parte. Este tipo de régimen subjetivo se basa en la teoría de la culpa donde el eje central no es el daño ni la víctima, sino el agente y su conducta frente al daño, bajo la premisa de que “no hay responsabilidad sin culpa”.²¹ En este caso, al estar impedido técnica y legalmente para controlar el contenido y los materiales que fluyen o se almacenan al prestar los servicios, es complejo dictaminar este tipo de responsabilidad que debiera imputárseles.

En el caso de la responsabilidad objetiva la cual se encuentra fundamentada en el marco legal mexicano en el artículo 1913 del CCF, no requiere que la actividad sea ilícita. Esta responsabilidad, también catalogada de riesgo creado, no requiere de negligencia o culpa, se apoya en el hecho de que se usa un objeto peligroso que requiere de cuidados especiales, lo cual genera un estado de riesgo para otros.

En este caso la simple existencia del daño reputaría la responsabilidad del PSI como causante del mismo y, por consiguiente, sería responsable de la reparación de los daños y perjuicios causados, toda vez que no es necesario que el afectado acredite la culpa del causante, sino el daño y la causa de éste. Sin embargo, interpretar que el PSI es responsable por ofrecer el servicio de Internet o hacer uso de la tecnología e infraestructura que permite su existencia, requiere al mismo tiempo interpretar que Internet y la infraestructura que le dan vida, son mecanismos, instrumentos, o aparatos peligrosos, o la actividad llevada a cabo por el PSI es una actividad peligrosa.

²⁰ Álvarez Amézquita, David *et al.*, *op. cit.*, nota 11, p. 60.

²¹ Cfr. Aguilar, Jorge, *La responsabilidad civil objetiva por daños al medio ambiente y su regulación en México*, México, Cámara de Diputados, Congreso de la Unión, 2010. Recuperado de <http://www.diputados.gob.mx/cedia/sia/redipal/redipal-02-10.pdf>. Fecha de consulta, 11 de febrero de 2014.

De estos puntos es posible concluir que en los marcos normativos de origen romano como el mexicano no es posible establecer ningún grado de responsabilidad al PSI, cuando su actuar es neutral es decir, cuando no es quien provee, elige o modifica el contenido o sus destinatarios.

2. *Responsabilidad vicaria, contributiva y directa*

En Estados Unidos existen tres tipos de responsabilidad general por daños, las cuales se han aplicado en materia de copyright para obtener la responsabilidad de los PSI por hechos realizados por terceros, utilizando sus servicios.²²

Responsabilidad directa (Direct infringement). Implica que alguien está realizando directamente la infracción a los derechos patrimoniales de autor. En este caso quien reproduce, distribuye o comunica una obra protegida sin previa y expresa autorización de su autor o titular de derecho es responsable directo de la infracción.²³ Este tipo de responsabilidad se les ha asignado a los PSI dado que al subir el usuario sus contenidos a Internet, la infraestructura del PSI automáticamente los conserva para verificar la transmisión o para facilitar futuras descargas del contenido, lo cual es considerado como reproducción no autorizada. Sin embargo, se creó una excepción en los marcos legales norteamericano y europeo, pero este tipo de responsabilidad por reproducción temporal sigue vigente en el marco normativo mexicano.

Responsabilidad contributiva (Contributory infringement). No requiere la comisión personal de la infracción aunque sí el conocimiento de la misma y la inducción, causación o contribución material en la actividad del tercero infractor.²⁴ Ahora bien, el PSI desconoce el contenido de las comunicaciones o información almacenada, pero qué sucede cuando el PSI es avisado por quien supone ser el titular de derechos de autor de una infracción y el PSI no baja los contenidos y no hace imposible su acceso.

²² Cfr. Piñeiro Ugarte, Lorena, *op. cit.*, nota, 7, p. 174.

²³ Ramírez, Mónica Andrea, “La responsabilidad de los ISPs desde el punto de vista de los contenidos”, *Revista la Propiedad Inmaterial*, núm. 13, Colombia, 2009, p. 291. Recuperado de http://portal.uexternado.edu.co/pdf/5_revistaPropiedadInmaterial/rpi%2013/MonicaRamirez.pdf. Fecha de consulta, 13 de febrero de 2014.

²⁴ *Religious Technology Center vs. Netcom On-Line Communications Services*, 907 F. Supp. 1361 (N.D. Cal 1995), donde se indica: “quien, con conocimiento de la actividad infractora, la induce, causa o materialmente contribuye a la conducta infractora de otro, puede ser considerado responsable como un infractor contributivo”, http://www.law.cornell.edu/copyright/cases/907_FSupp_1361.htm. Fecha de consulta, 10 de septiembre de 2014.

Responsabilidad vicaria (Vicarius liability). Sucede cuando aquél que tenía el derecho y la posibilidad de controlar el acto del tercero infractor, no lo hace, y además recibe un beneficio económico al suceder la infracción, en este caso se responsabiliza a quien debió controlar la acción del tercero.²⁵ Para que exista responsabilidad vicaria deben satisfacerse dos requisitos: i) que el demandado tenga el derecho y capacidad de controlar los actos del infractor, y ii) que el demandado reciba beneficio financiero directo de la infracción.²⁶

Cabe concluir que es totalmente imposible la aplicación de este último tipo de responsabilidades en México al estar basadas en una doctrina extranjera, incompatible con el ordenamiento jurídico mexicano.

En atención a la aplicación de toda esta gama de posibles responsabilidades, la normativa de ciertos países buscó atender las preocupaciones anteriormente plasmadas, establecido puertos seguros (*safe harbors*) para ciertas funciones de los PSI, delimitando una serie de supuestos y garantizando que, si se cumplen las condiciones previstas en los mismos, el PSI no podrá ser declarado responsable por sus servicios.

Estos puertos seguros no deben interpretarse que en caso de no cumplirse los requisitos, suponga que automáticamente los PSI se vuelven responsables. Tienen el objetivo de excluirlos directamente, pero en caso de incumplir el juzgador deberá evaluar el caso en concreto para decidir si se les debe imputar alguna responsabilidad, estando en posibilidad de que, a pesar de no cumplir con estos requisitos, no sean declarados responsables por las circunstancias específicas del caso y la regulación aplicable.

Los requisitos del puerto seguro no son obligaciones o deberes que la regulación de otros países impone a los PSI, son tan sólo elementos que permiten considerar su actividad como neutra o pasiva en relación con los contenidos alojados o transmitidos. Por tanto, el hecho de que el PSI no satisfaga los requisitos no se debe interpretar como un incumplimiento de un deber legal.

IV. SISTEMAS DE PROTECCIÓN

Habiendo revisado la problemática existente y los esquemas de responsabilidad que en ocasiones se ha interpretado le aplican a los PSI, se revisa-

²⁵ Piñeiro Ugarte, Lorena, *op. cit.*, nota 7, p. 174.

²⁶ Maza, Íñigo de la, *Responsabilidad de los proveedores de servicios de Internet por infracción de los derechos de autor*, 2003, p. 5. Recuperado de http://www.fundacionfuego.udp.cl/articulos/inigo_de_la_maza/responsabilidad%20isp.pdf. Fecha de consulta, 7 de marzo de 2014.

rán también los esquemas que otros países han implementado en búsqueda de equilibrar los intereses de la industria autoral y los PSI.

1. *Estados Unidos de Norteamérica (vertical)*

En Estados Unidos la *Digital Millennium Copyright Act* de 1998 (en lo sucesivo la DMCA),²⁷ define según la limitación de la que se trate de aplicar. En el caso de las comunicaciones transitorias es: “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received”.²⁸ Respecto de cualquier otra limitación se define en términos más amplios como “a provider of online services or network access, or the operator of facilities therefor”.²⁹

El PSI debe cumplir con dos requisitos generales para que le puedan aplicar las exenciones. El primero de ellos es adoptar e implementar una política de terminación de las cuentas de los usuarios reincidentes de infracciones de derechos de autor (respuesta gradual); el segundo es que el PSI debe abstenerse de interferir con las medidas técnicas estándares (*standard technical measures*), en la medida que éstas no le impongan costos o cargas excesivas sobre sus servicios o sistemas.

El DMCA establece cuatro tipos de actividades o servicios que están cubiertos dentro de los puertos seguros, siempre que el PSI cumpla con los dos requisitos previos generales y los requisitos particulares de cada actividad.

²⁷ Es posible consultar la Digital Millennium Act en <http://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf>.

²⁸ DMCA sección 512(k)(1)(A) y (B).

(k) DEFINITIONS.

(1) SERVICE PROVIDER.

(A) As used in subsection (a), the term “service provider” means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term “service provider” means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

²⁹ *Idem*.

A. *Comunicaciones transitorias, sección 512 (a) DMCA*

Es cuando el PSI únicamente transmite, enruta o provee las conexiones de datos desde un punto a otro a solicitud de otra persona. Dentro de esta excepción se incluye el almacenamiento intermediario y temporal. Esta exención será aplicable si se cumplen cinco requisitos particulares: 1) el PSI no haya iniciado la transmisión; 2) el proceso de transmisión sea automatizado; 3) el PSI no seleccione los destinatarios; 4) no se almacene copia de la información en los sistemas del PSI más allá del tiempo necesario para lograr la comunicación, y 5) el PSI no modifique o seleccione el contenido de la comunicación.

B. *Almacenamiento temporal en cacheo caching sección 512 (b) DMCA*

Este tipo de almacenamiento es el que es necesario como consecuencia de la fragmentación en paquetes para transmitir la información vía Internet, para que, en caso de que un paquete de información no llegue o llegue incompleto a su destino, el PSI puede acudir a esta copia para completar la información y completar la transmisión.³⁰ La DMCA establece que para ser sujeto de esta exención es necesario: 1) el contenido o la información no hayan sido modificados; 2) que el PSI actualice los contenidos que conserva en caché; 3) que no interfiera en las medidas que permiten al titular del sitio obtener información sobre quienes acceden a sus contenidos, y 4) que mantenga las condiciones de acceso.³¹

Esta normativa contiene un requisito adicional para ser sujeto de esta y la siguiente exención (alojamiento-*hosting*): el PSI tiene la obligación de retirar o hacer inaccesibles aquel material que haya sido subido a la red sin autorización de su titular, siempre que sea notificado por una persona que declare bajo protesta de decir verdad que es titular de los derechos sobre el contenido en controversia. Esta obligación es conocida como *Notice and Take Down*, la cual se especifica en la sección 512 c (1)(C), (2) y (3).

C. *Alojamiento (hosting-web housing) sección 512 (c) DMCA*

Aplica para la información que reside en los sistemas o redes del PSI en sitios, páginas y direcciones de terceros. Para encuadrarse en esta causal de

³⁰ Cfr. Piñeiro Ugarte, Lorena, *op. cit.*, nota 7, p. 176.

³¹ Cfr. Maza, Íñigo de la, *op. cit.*, nota 26, p. 13.

exención se requiere: 1) el PSI no tenga conocimiento de que la actividad o el disponible en su sistema infringe derechos de autor, incluyendo el conocimiento de hechos o circunstancias que hagan presumirlo; 2) en caso de obtener el conocimiento, actúe expeditamente para retirar o deshabilitar el acceso al material, y 3) no reciba beneficio económico directo por la actividad infractora del usuario.

En relación con el segundo requisito y muy similar al mismo, se agrega un cuarto requisito, para el PSI para que en caso de una notificación de vulneración de derechos (*notification of claimed infringement*) responda de manera expedita removiendo o haciendo inaccesible el contenido. La principal diferencia se encuentra en que en el segundo requisito, donde el PSI pudo haber obtenido el conocimiento por cualquier medio y en este caso debe “actuar”; en contraste del cuarto requisito, donde el PSI recibe una notificación específica con elementos y un procedimiento establecido, en este caso el PSI debe “responder”.

Dentro del cuarto requisito se establecen los elementos de la notificación de vulneración de derechos (sección 512 (c) (3)) y la designación de un agente responsable de la atención a las notificaciones (sección 512 (c) (2)). El procedimiento de *Notice and Take Down* que debe cumplir el PSI al recibir una notificación consta de cuatro pasos fundamentales:

- a) Remover o inhabilitar el contenido.
- b) Notificar prontamente al usuario respecto a quién removió o inhabilitó el acceso a su contenido.
- c) En caso de recibir una contra-notificación, enviar rápidamente copia al quejoso e informarle que en 10 días repondrá el material o restablecerá su acceso. Los requisitos para la contra-notificación son iguales a los anteriormente descritos.
- d) Reponer el material o restablecer su acceso entre el día 10 al 14 de haber recibido la contra-notificación, a menos que el quejoso le haya hecho saber que presentó el caso en tribunales.

En cuanto a la designación de un agente responsable, la DMCA señala que el PSI deberá poner a disposición de los posibles quejosos la información de su delegado (nombre, dirección, número de teléfono, y correo electrónico) a través de un aviso en su sitio web y registrándolo en la *Copyrights Office*.

D. Herramientas para la localización de información sección 512 (d) DMCA

Son aquellos servicios de búsqueda, referencia o enlace (*linking*) de usuarios con sitios o direcciones web, como: motores de búsqueda, hipervíncu-

los, directorios en línea, y otras herramientas de búsqueda semejantes. Las condiciones para la aplicación de la exención son las mismas que para la actividad anterior (alojamiento).

En este caso PSI se exime de responsabilidad si: teniendo conocimiento, remueve el contenido o material presuntamente infractor o, sin tener conocimiento, y sin recibir beneficio económico de la infracción, al recibir una notificación (independientemente de su estado de conocimiento) remueve o inhabilita el acceso. Adicional a lo anterior, la DMCA establece que el PSI no está autorizado a monitorear o vigilar el contenido que se transmite o almacena en sus redes.³²

2. *Europa (horizontal)*

En el sistema europeo, a través del artículo 1o. de la Directiva 98/34/CE, la cual fue modificada por la Directiva 98/48/CE, y en relación con la Directiva 2000/31/CE (DCE), define al PSI como cualquier proveedor de un servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios. La DCE regula tres funciones dentro de estas exenciones.

A. *Mera transmisión de datos o acceso a la red (artículo 12, DCE)*

Donde se requiere que el PSI no haya originado él mismo la transmisión, no haya seleccionado al destinatario de la transmisión ni haya seleccionado o modificado los datos o contenidos transmitidos. La exención opera únicamente si la transmisión ha sido pasiva y automática. Por lo mismo la selección del destinatario de la transmisión y los datos transmitidos deben haber sido realizados por el usuario y el PSI no debe haber modificado los datos.³³

En este punto se requiere que la información no sea almacenada por un periodo más largo de lo razonablemente necesario. Este punto resulta relevante, ya que en la normatividad mexicana este tipo de almacenamiento, al igual que el almacenamiento en memoria caché, están dentro de la

³² Cfr. Maza, Íñigo de la, *op. cit.*, nota 26, p. 16.

³³ *Ibidem*, p. 9.

definición de reproducción y, por lo tanto, podría resultar en una infracción por parte de los PSI.

*B. Almacenamiento de datos en memoria caché o catching
(artículo 13, DCE)*

La DCE no difiere en el fondo con lo establecido por la DMCA, pues reconoce que se puede llevar a cabo esta función con el solo propósito de hacer más eficiente la transmisión, cumpliendo con los requisitos de no modificar o actualizar la información y con las condiciones de acceso a la información, así como no interferir en las tecnologías de control de visitas.

*C. Almacenamiento de información cargada por el usuario
o hosting (artículo 14, DCE)*

Como en la DMCA, esta acción es aquella donde el usuario carga información a una plataforma administrada por un PSI para su alojamiento. En este caso, para brindar la exención, la DCE requiere que el PSI no tenga conocimiento efectivo de que la actividad es ilícita, ni tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito o, en caso de tenerlos, actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible, así como que el PSI no tenga un rol de control sobre el destinatario del servicio.

Esta exención se establece para el PSI a modo de doble nivel de ausencia de conocimiento, respecto de la ilicitud de la información almacenada: “conocimiento efectivo” y “conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito”. La DMCA (sec.512 c A ii) también recoge este doble nivel de conocimiento. Pero en el segundo nivel –circunstancias revelen carácter ilícito– la problemática de este punto es que si se realiza la inhabilitación del contenido y no existió violación al derecho de autor, el PSI podría ser sujeto a una demanda por incumplimiento de contrato, o incluso un transgresor de la libertad de expresión.

En este punto también existe debate ya que, como la DCE no define “conocimiento efectivo”, no hay claridad en que si una notificación por parte de un particular puede o no generar elementos para que se considere que un PSI tiene conocimiento efectivo o conocimiento de hechos que revelen el carácter ilícito del contenido y, por lo tanto, la obligación de reaccionar ante

la notificación de una supuesta infracción.³⁴ En algunos casos, la legislación de los países miembros de la Unión Europea establece esta definición, como en el caso español, que en el artículo 16.1.b) de la Ley de Servicios de la Sociedad de la Información (LSSI) señala que será cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos.

La normativa europea y la norteamericana cuentan con diferencias relevantes, las cuales resumimos a continuación:

- I. La normativa europea no incluye al día de hoy, dentro de su alcance, las funciones de motores de búsqueda o localizadores, sí incluidos en la DMCA. Cabe señalar que los Estados miembros de la Unión Europea pueden incorporarlo, como ejemplo está España dentro de la LSSI (artículo 17).
- II. La normativa europea no establece ningún tipo obligación adicional de carácter permanente al PSI, como la exigencia de una política de terminación anticipada de servicio a sus usuarios por reincidir en las infracciones en materia de *copyright*, o la designación de una persona o agente para atender las notificaciones.
- III. La normativa americana únicamente requiere de una notificación por parte de un particular para retirar o imposibilitar el acceso a algún contenido, mientras que la europea requiere de la participación de una autoridad.
- IV. La DCE, en su artículo 15, establece la prohibición expresa dirigida a los países miembros de imponer alguna obligación a los PSI de supervisar, o monitorear a través de búsquedas activas los contenidos que se prestan por los servicios de transmisión, acceso, *catching* o *hosting*.
- V. La normativa americana, a través de la DMCA, únicamente está dirigida a infracciones de *copyright* mientras que la DCE aplica a cualquier tipo de infracción.³⁵ En EUA, otras leyes sectoriales diferentes a la DMCA incorporan la exención de responsabilidad de los PSI, como es la sección 230 de la *Communications Decency Act* que forma parte de la *Telecommunications Act* de 1996,³⁶ con la cláusula del

³⁴ Cfr. Piñeiro Ugarte, Lorena, *op. cit.*, nota 7, p. 181.

³⁵ Álvarez Amézquita, David *et al.*, *op. cit.*, nota 11, p. 60.

³⁶ *Telecommunications Act de 1996*, <http://www.fcc.gov/telecom.html>, 47 USC § 230. *Protection for Private Blocking and Screening of Offensive Material*, fecha de consulta, 12 de mayo de 2014.

buen samaritano (*Good Samaritan*).³⁷ Señala que inicialmente esta cláusula estaba prevista únicamente para la responsabilidad por la *third party speech* (difamaciones, afirmaciones falsas, etcétera, cometidas por usuarios de Internet), pero su alcance se ha ido expandiendo hasta cubrir la responsabilidad por todo tipo de infracciones civiles.

3. Canadá

En cuanto a la regulación en Canadá, su *Copyright Act* fue recientemente modificada por la Bill C-11 que recibió sanción real el 29 de junio de 2012, y la mayoría de sus disposiciones entraron en vigor el 7 de noviembre de 2012.³⁸ Estas modificaciones incluyeron el establecimiento, en su artículo 31.1 referente a los Servicios en la Red (*Network Services*), que los PSI y motores de búsqueda se encuentran eximidos de responsabilidad cuando actúan estrictamente como intermediarios en la comunicación, actividades de *hosting* y almacenamiento en caché. Esta exención de responsabilidad no se aplica si un PSI está diseñado principalmente para permitir actos de infracción de derechos de autor o si conoce de una decisión judicial que establece que el material que almacena infringe derechos de autor, y continúa con la actividad.

Sin embargo, lo realmente novedoso es que de acuerdo con los aún no vigentes artículos 41.25 y 41.26, referentes a las Medidas Tecnológicas de Protección e Información para la Gestión de Derechos (*Technological Protection Measures and Rights Management Information*) de la *Copyright Act* de Canadá modificada por la ya referida Bill C-11, se introduce un sistema de “notificación y aviso” (conocido como *notice and notice*), obligatorio para los PSI.

El sistema de notificación y aviso permite a propietarios del copyright enviar avisos de infracción a los PSI, que estarán legalmente obligados a remitir la notificación a sus suscriptores, que presuntamente estén violando

³⁷ Xalabarder, Raquel, “La responsabilidad de los prestadores de servicios en Internet (PSI) por infracciones de propiedad intelectual cometidas por sus usuarios”, IDP *Revista de Internet, Derecho y Política*, España, 2006, núm. 2, p. 13.

³⁸ Es importante señalar que el texto completo de la Bill C-11 (*Modernization Copyright Act*), que modifica la *Copyright Act* de Canadá se encuentra en el sitio web del Parlamento de Canadá, <http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5697419>. Es posible que en otros sitios gubernamentales de Canadá no se encuentre el texto de los artículos de la *Copyright Act* que aún no entran en vigor, como son los artículos 41.25 y 41.26, como podría ser el sitio web del gobierno canadiense, donde se centraliza la legislación de dicho país, <http://laws-lois.justice.gc.ca/eng/acts/C-42/index.html>. Fecha de consulta, 24 de febrero de 2014.

derechos. El PSI deberá mantener un registro de esta notificación y retener información de identificación del suscriptor durante seis meses (o 12 meses si se inician procesos judiciales). Si un PSI no reenvía las notificaciones podría ser responsable de daños civiles. Independientemente de lo anterior los titulares de derechos de autor tienen las herramientas para hacer valer sus derechos ante las autoridades correspondientes.

Cabe señalar que si bien la mayor parte de la ley entró en vigor en noviembre de 2012, estos artículos, referentes al sistema de “notificación y aviso”, quedaron pendientes de entrar en vigor, esperando los resultados de una consulta pública realizada por el gobierno canadiense a finales de 2013 y la posible reglamentación secundaria del proceso.

4. *Chile*

En mayo de 2010 fue modificada la ley núm. 17336, Ley de Propiedad Intelectual,³⁹ introduciendo el capítulo III llamado “Limitación de Responsabilidad de los Prestadores de Servicios de Internet”, que va desde el artículo 85L al 85U. Esta legislación establece las siguientes condiciones específicas:

- A. PSI de transmisión y acceso a Internet.
 - a) No haya modificado ni seleccionado el contenido de la transmisión, con excepción de aquellas modificaciones necesarias para facilitar la transmisión, como la división de paquetes.
 - b) No sea el iniciador de la transmisión.
 - c) No seleccione a los destinatarios.
- B. Almacenamiento temporal y automático (caché).
 - c) Respete las condiciones de acceso de usuarios y las reglas relativas a la actualización del material almacenado establecidas por el proveedor del sitio de origen.
 - d) No interfiera con la tecnología compatible y estandarizada utilizada en el sitio de origen para obtener información sobre el uso en línea del material almacenado.
 - e) No modifique el contenido.
 - f) Retire o inhabilite en forma expedita el acceso a material almacenado que haya sido retirado o al que se haya inhabilitado el

³⁹ Puede ser consultado en <http://www.leychile.cl/Navegar?idNorma=28933>. Fecha de consulta, 3 de abril de 2014.

acceso en su sitio de origen, cuando reciba una notificación por parte de un tribunal.

C. PSI de *hosting*, motores de búsqueda y directorios

- d) No tenga conocimiento efectivo del carácter ilícito de los datos, que en este sistema se traduce en que un tribunal ordene el retiro o bloqueo del contenido.
- e) No reciba un beneficio económico directamente atribuible a la actividad infractora, en los casos en que tenga el derecho y la capacidad para controlar dicha actividad;
- f) Designe públicamente un representante para recibir las notificaciones judiciales.⁴⁰
- g) Retire o inhabilite en forma expedita el acceso al material almacenado.

Cualquiera de las tres clases de PSI antes mencionadas, para disfrutar de la exención de responsabilidad, debe adicionalmente:

- Establecer públicamente los términos y condiciones para sus usuarios en caso de uso de contenido calificado judicialmente como infractor.
- No interferir en las medidas tecnológicas de protección y de gestión de derechos de obras protegidas.
- No haber generado, ni seleccionado el material o a sus destinatarios. Esta condición está exceptuada para motores de búsqueda.

El artículo 85 Q establece la posibilidad de que un juez dicte como medida precautoria (sin audiencia del proveedor del contenido) o dentro de su resolución definitiva el retiro o bloqueo de los contenidos infractores. En los casos de medidas prejudiciales se requerirá que el titular de los derechos de autor que solicita la medida rinda una garantía para salvaguardar los derechos del proveedor de contenido, en caso de que resultare improcedente su reclamación y el proveedor del contenido sea vulnerado en sus derechos.

En este caso el proveedor de contenido afectado podrá solicitar al tribunal chileno que deje sin efecto la medida de restricción de acceso o retiro

⁴⁰ A este respecto, el artículo 24 del reglamento de la Ley de Propiedad Intelectual chilena señala que la designación del representante de los PSI, deberá ser identificada en el sitio web del PSI, en forma destacada. El reglamento se puede consultar a través de <http://www.cultura.gob.cl/wp-content/uploads/2013/11/REGLAMENTO-PROPIEDADINTELECTUA L.pdf>. Fecha de consulta, 14 de abril de 2014.

de material, bastando para ello una solicitud y continuando el proceso legal respectivo.

El artículo 85 R, en su inciso b), considera la posibilidad de que un juez solicite al PSI el cierre de cuentas de usuarios, identificadas como infractoras reincidentes, algo muy similar a lo que sucede en Francia. Por su parte, el artículo 85 S autoriza al tribunal competente, a requerirle al PSI que entregue información que permita identificar al presunto infractor, a requerimiento de los titulares de derechos.

Ahora bien, en busca de inhibir posibles abusos de las medidas precautorias, el artículo 85 T. de la ya multicitada ley, establece la obligación de indemnizar por daños y perjuicios, adicional a la respectiva sanción penal, a quien a sabiendas proporcione información falsa relativa a supuestas infracciones a los derechos de autor, en estos casos.

Adicionalmente esta ley prevé, en su artículo 85 U, una notificación, de forma independiente, mediante la cual el PSI les comunica a sus usuarios que un titular de derechos de autor ha detectado que se han realizado utilidades no autorizadas de material protegido infringiendo la Ley de Propiedad Industrial a través de su computadora.

La notificación, en primer lugar, consiste en poner en conocimiento del usuario del PSI que se ha detectado que desde su equipo se llevan a cabo dichas actividades ilícitas y exhortar al usuario al inmediato cese de la actividad infractora, informándole que de continuar con la actividad presuntamente infractora, el usuario se arriesga a verse expuesto a las correspondientes acciones judiciales.

Adicional a lo anterior, la ley analizada específicamente señala la prohibición de los PSI a supervisar o monitorear los datos que transmitan, almacenen o referencien, prohibiendo la realización de búsquedas de hechos o circunstancias de actividades infractoras.

5. *Francia (modelo de respuesta gradual)*

Este país había implementado, desde el 1o. de julio de 2010, en la Ley Promotora de la Difusión y la Protección de la Creación en Internet, llamada extraoficialmente como la Ley HADOPI por las siglas de la autoridad responsable creada a través de la misma (Autorité pour la diffusion des œuvres et la protection des droits sur Internet o Alta autoridad para la difusión de obras y la protección de derechos en Internet, en español), un sistema de respuesta gradual, es decir, hacer del conocimiento de un usuario que está violando derechos de autor a través de su cuenta o computadora y tomar

medidas de forma gradual para evitarlo. En el modelo de respuesta gradual, los titulares de los derechos de autor alertan a los PSI sobre la existencia de direcciones IP utilizadas para subir contenidos protegidos a Internet sin la debida autorización.

Para detectar esta infracción no se monitorea la conducta individual de los usuarios, sino que se vigilan las redes *Peer to Peer* y los canales de distribución de archivos que vulneran los derechos de autor. Como paso siguiente, los PSI rastrean a cuál de sus suscriptores pertenece la dirección IP y contactan al usuario para informarle que su cuenta está siendo usada para violar derechos de autor y habrá de recibir una penalidad o sanción si no desiste de dicha actividad después de una serie de notificaciones.

En Francia se contemplaban tres avisos o notificaciones: como primer aviso, un correo electrónico; como segundo aviso, un correo certificado; y como último recurso el cierre de la conexión a Internet. Específicamente el usuario debía hacer caso omiso de dos avisos en el curso de seis meses y violar derechos de autor a través de su cuenta por tercera vez en un año, para que la Alta Autoridad por la Difusión de Obras y la Protección de Derechos en Internet (HADOPI),⁴¹ notificara a un tribunal penal, el cual a su vez solicitaba la suspensión de la cuenta.

Sin embargo, a través del decreto número 0157 del 9 de julio de 2013, el sistema de respuesta gradual fue derogado y dejado sin efectos. Cabe señalar que este país fue el primero en introducir leyes de respuesta gradual, pero únicamente estuvo vigente por aproximadamente tres años.

V. CONCLUSIONES

Es fundamental que México adopte un enfoque compatible con los sistemas internacionales. En virtud de que Internet es un sistema sin fronteras y dado que existen diferentes enfoques y tradiciones jurídicas distintas en cada país, no es necesario que el sistema sea idéntico, pero debe ser interoperable para permitir un desarrollo armonizado y con cooperación de autoridades de forma global. En este tenor, el tema abordado genera varios puntos de vista, pero, en el afán de servir al propósito de los debates que se lleven a cabo en México, serán delimitadas las siguientes recomendaciones particulares, las cuales fueron el objetivo del presente trabajo.

⁴¹ Es posible encontrar mayor información de la HADOPI en el sitio oficial <http://www.hadopi.fr/es>. Fecha de consulta, 24 de abril de 2014.

Inicialmente, se requiere una definición clara de lo que es un PSI, tipos o actividades que pueden desarrollar, ya sea servicios de acceso a Internet, *hosting*, memoria *caché*, motores de búsqueda, plataformas de intercambio, entre otros.

En cuanto a la responsabilidad del PSI, se considera que generalmente se está frente a una función de intermediación puramente pasiva y neutra, por lo que los PSI no deben ser declarados responsables de los contenidos intercambiados o almacenados en su infraestructura, en el caso de que éstos resulten ilícitos. Entendido por intermediación pasiva y neutral cuando no sea el originador del contenido, no lo modifique, no elija destinatarios, no tenga control del contenido y no lo almacene por más tiempo que el estrictamente necesario, así como no tenga conocimiento efectivo de que por su infraestructura, redes o servicios se están realizando actividades contrarias a la ley. No debe entenderse por control el simple hecho de que se utilicen sus medios para almacenar o transferir la información.

Es importante definir claramente cuando un PSI tiene conocimiento efectivo de que a través de sus redes o servicios se están realizando actividades ilícitas, para que pueda o no ser considerado responsable. El conocimiento efectivo parte de una notificación, independientemente de la obligación que adquiere el PSI a partir de ella (bajar el contenido y transmitirla al usuario presuntamente infractor).

Se recomienda que para el caso mexicano, por agilidad y protección de derechos de los usuarios, para que exista conocimiento efectivo por parte del PSI, la notificación debiera provenir de una autoridad administrativa con facultades dentro de su competencia. No se recomienda una autoridad judicial debido a lo tardado y burocrático que podría ser este proceso para los titulares de derechos de autor, así como para el PSI, que deberá contar con un número relevante de expertos en materia jurídica para dar atención y respuesta a requerimientos judiciales.

Para cumplir lo anterior deberá establecerse y definir a detalle un proceso ágil de análisis por parte de la autoridad administrativa (con el conocimiento especializado necesario) para evaluar las solicitudes de los titulares de derechos de autor y ordenar las provisionales o definitivas que deban realizar los PSI, así como el establecimiento de garantías y contragarantías para proteger a los interesados.

Ahora bien, una vez que se tenga el conocimiento efectivo, deben existir previsiones por un periodo de tiempo corto para que el PSI actúe y evite caer en un escenario de posible responsabilidad, como pueden ser los bloqueos o retiro del contenido o sitios. De la misma forma, para evitar cualquier tipo de abuso, es necesario que cualquier persona que solicite ante la

autoridad administrativa el bloqueo de contenido como medida preventiva, demostrándose posteriormente que no tenía derechos sobre el contenido en cuestión, deberá ser sancionado con una pena administrativa ejemplar e inclusive con el delito de falsedad de declaración ante autoridad administrativa establecida en el artículo 247 del Código Penal Federal.⁴²

Paralelamente, como refuerzo a este puerto seguro, podrían imponérsele obligaciones a los PSI que robustezcan la protección, y ayuden a inhibir y mitigar las vulneraciones a los derechos de autor, como puede ser el contener cláusulas de bloqueo de contenido en sus contratos con sus usuarios, la obligación de retransmitir a sus usuarios notificaciones privadas recibidas de los titulares del derecho de autor, nombramiento de un responsable interno para orientar a los titulares de derechos de autor y recibir notificaciones al respecto, almacenamiento de la información de identificación del equipo donde se está cometiendo presuntamente la actividad ilegal, y su entrega a las autoridades correspondientes.

Para no menoscabar la libertad de expresión, la privacidad de las personas, el derecho a la inviolabilidad de las comunicaciones privadas y no imponer cargas tecnológicamente inviables o altamente costosas a los PSI, se debe expresamente prohibir que los PSI fiscalicen, monitoreen, auditen o vigilen los contenidos que los usuarios almacenen, reproduzcan o comuniquen a través de sus servicios.

Es importante que el sistema sea equilibrado y funcional para los involucrados, que tenga un enfoque de disuadir infracciones y al mismo tiempo estimular a los autores a seguir generando obras y proteger el importante papel desempeñado por los PSI para permitir el intercambio de ideas e información, sin menoscabar las garantías de seguridad jurídica, debido proceso, libertad de expresión y privacidad de los usuarios de la red.

Como parte de los elementos para inhibir las prácticas ilegales en línea, todos los participantes deberán invertir en la concientización del público. Finalmente, el debate de este tipo de soluciones deberá integrar las voces e intereses de todas las partes relacionadas: autores, sociedades de gestión colectiva, PSI, plataformas, academia, sociedad civil, usuarios, industria de Internet, etcétera, e incluso deberán evaluarse otros participantes si los sistemas abarcan cualquier otro tipo de contenido contrario a la legislación,

⁴² Artículo 247. Se impondrán de cuatro a ocho años de prisión y de cien a trescientos días multa:

I. Al que, interrogado por alguna autoridad pública distinta de la judicial en ejercicio de sus funciones o con motivo de ellas, faltare a la verdad.

donde las reglas pudieran ser igualmente aplicables y no únicamente para material infractor de derechos de autor, lo cual es muy recomendable.

VI. BIBLIOGRAFÍA

- AGUILAR, Jorge, *La responsabilidad civil objetiva por daños al medio ambiente y su regulación en México*, Cámara de Diputados, Congreso de la Unión, México, 2010. Recuperado de <http://www.diputados.gob.mx/cedia/sia/redipal/redipal-02-10.pdf>.
- ÁLVAREZ AMÉZQUITA, David *et al.*, “Proveedores de Servicios de Internet y de contenidos, responsabilidad civil y derechos de autor”, *Revista Studiostitas*, Colombia, 2009, vol. 3, núm. 4.
- ÁNGEL, Ricardo de, *Tratado de responsabilidad civil*, Madrid, Civitas, 1993.
- COMISIÓN DE LAS COMUNIDADES EUROPEAS (CCE), *Libro verde: los derechos de autor y los derechos afines en la Sociedad de la Información*, Bélgica, 1995.
- CHWELOS, Paul, *Internet Service Providers Report*, Industry Canada, 2006. Recuperado de http://www.ic.gc.ca/eic/site/ippd-dppi.nsf/eng/h_ip01423.html.
- GRIJALVA, Agustín, *Internet y derechos de autor*, Ecuador, Facultad Latinoamericana de Ciencias Sociales (Flacso), recuperado de <http://www.flacso.org.ec/docs/sfintgrijalva.pdf>.
- JIJENA LEIVA, Renato *et al.*, *El derecho y la Sociedad de la Información: la importancia de Internet en el mundo actual*, México, Tecnológico de Monterrey, Porrúa, 2003.
- LITHWICK, Dara, *Legislative Summary of Bill C-32: An Act to amend the Copyright Act*, Parlamento de Canadá, 2010. Recuperado de <http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/40/3/c32-e.pdf>.
- LOREDO HILL, Adolfo, *Nuevo derecho autoral mexicano*, México, Fondo de Cultura Económica, 2000.
- MAZA, Íñigo de la, *Responsabilidad de los proveedores de servicios de Internet por infracción de los derechos de autor*, 2003. Recuperado de http://www.fundacionfueyo.udp.cl/articulos/inigo_de_la_maza/responsabilidad%20isp.pdf.
- ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The Seoul Declaration, the Future of Internet Economy*, Korea, 2008. Recuperado de <http://www.oecd.org/internet/consumer/40839436.pdf>.
- ORGANIZACIÓN MUNDIAL DEL COMERCIO (OMC), *¿Qué se entiende por “derechos de propiedad intelectual”?* Recuperado de http://www.wto.org/spanish/tratop_s/trips_s/intell_s.htm.

ORGANIZACIÓN MUNDIAL DE PROPIEDAD INTELECTUAL (OMPI), *Principios básicos del derecho de autor y los derechos conexos*. Recuperado de http://www.wipo.int/export/sites/www/freepublications/es/intproperty/909/wipo_pub_909.pdf.

———, *Intellectual Property on the Internet: A Survey of Issues*. Recuperado de http://www.wipo.int/copyright/en/ecommerce/ip_survey/.

PEGUERA POCH, Miquel, “Sólo sé que no sé nada (efectivamente): la apreciación del conocimiento efectivo y otros problemas en la aplicación judicial de la LSSI”, *Revista de Internet, Derecho y Política*, núm. 5, 2007. Recuperado de <http://www.uoc.edu/idp/5/dt/esp/peguera.pdf>.

———, *La exención de responsabilidad civil por contenidos ajenos en Internet*, 2002. Recuperado de <http://www.uoc.edu/in3/dt/20080/20080.pdf>.

PÉREZ-ALONSO, Rodrigo y PIEDRAS FERIA, Ernesto (coords.), *Una agenda digital: telecomunicaciones y tecnologías de la información en México*, México, Cámara de Diputados, LXI Legislatura, 2012.

PIÑEIRO UGARTE, Lorena, “Responsabilidad de los ISPs por violación a la propiedad intelectual: Estados Unidos, Europa y Chile”, *Revista Chilena de Derecho Informático*, Chile, 2011.

RAMÍREZ, Juan, *Responsabilidad civil objetiva*, México. Recuperado de http://www.conamed.gob.mx/comisiones_estatales/coesamed_nayarit/publicaciones/pdf/responsabilidad_civil.pdf.

RAMÍREZ Mónica, Andrea, “La responsabilidad de los PSI desde el punto de vista de los contenidos”, *Revista La Propiedad Inmaterial*, Colombia, núm. 13, 2009. Recuperado de [http://portal.uexternado.edu.co/pdf/5_revistaPropiedad Inmaterial/rpi%2013/MonicaRamirez.pdf](http://portal.uexternado.edu.co/pdf/5_revistaPropiedad%20Inmaterial/rpi%2013/MonicaRamirez.pdf).

RANGEL MEDINA, David, *Derecho de la propiedad industrial e intelectual*, México, UNAM, Instituto de Investigaciones Jurídicas, 1992.

RICKETSON, Sam., *WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment*, Ginebra, 2003. Recuperado de http://www.wipo.int/edocs/mdocs/copyright/en/ccr_9/ccr_9_7.pdf.

SANTÍN, Abel, *Peer 2 Peer Sistemas Operativos Distribuidos*. Recuperado de http://www.dit.upm.es/~jo_aquin/so/p2p/p2p.pdf Smedinghoff, Tomas J., *Online law: the SPA's legal guide to doing business on the Internet*, Software Publishers Association, EUA, 1996.

UBC, *Bill C-11: The Copyright Modernization Act*, Universidad de British Columbia. Recuperado de <http://copyright.ubc.ca/copyright-legislation/bill-c-11-the-copyright-modernization-act/>.

VIVIANA SARRA, Andrea, *Comercio electrónico y derecho*, Argentina, Astrea de Alfredo y Ricardo Depalma, 2000.

XALABARDER, Raquel, “Copyright y derecho de autor: ¿convergencia internacional en un mundo digital?” IDP *Revista de Internet, Derecho y Política*, España, núm. 1, 2005. Recuperado de <http://www.uoc.edu/idp/1/dt/esp/xalabarder02.pdf>.

“LA responsabilidad de los prestadores de servicios en Internet (ISP) por infracciones de propiedad intelectual cometidas por sus usuarios”, IDP *Revista de Internet, Derecho y Política*, España, núm. 2, 2006.

ZUCCHINO, Clara, *La responsabilidad de los PSIs por los contenidos generados y transmitidos por los usuarios*, Certamen IP 2008 Mentees Innovadoras para el desarrollo, 2a. ed., Argentina, 2008. Recuperado de https://www.u-cursos.cl/derecho/2011/2/D124T07237/35/material_docente/bajar?id_material=411759.

BITCOIN: PROBLEMAS REALES

Cristina GÓMEZ RODRÍGUEZ*

SUMARIO: I. *¿Qué es bitcoin?* II. *Problemas relacionados con el bitcoin.* III. *Reflexiones sobre la naturaleza jurídica del bitcoin.* IV. *Futuro de los criptoalgoritmos de intercambio.* V. *Conclusión.* VI. *Glosario.* VII. *Bibliografía.*

I. ¿QUÉ ES BITCOIN?

La palabra *bitcoin*, con minúsculas, se utiliza para referir a la unidad o algoritmo que genera una secuencia alfanumérica de treinta y tres caracteres que se crea e intercambia a través del software *Bitcoin*.¹

La palabra *Bitcoin*, por otra parte, con su primera letra mayúscula se usa para referir al *software* y red de minería *Bitcoin* que descifra la cadena de bloques que crean e intercambian la unidad *bitcoin* conocida también por su abreviatura *BTC*.²

La creación del *software Bitcoin* se atribuye a Satoshi Nakamoto, que apareció por primera vez el 31 de octubre de 2008 con un mensaje titulado “*Bitcoin P2P e-cash paper*” haciendo referencia a un documento sobre efectivo electrónico, en el que decía que estaba trabajando en un nuevo sistema electrónico de dinero sin intermediarios, remitiendo a la liga en la que se encontraba disponible la explicación sobre el funcionamiento del programa de cómputo.³ El *Bitcoin* entró en circulación en la red el 11 de febrero de

* Miembro de la primera generación de la maestría en derecho de las tecnologías de la información y comunicación de INFOTEC, organismo público adscrito a Conacyt.

¹ Bitcoin. “Algunas palabras en Bitcoin que usted puede escuchar”, www.bitcoin.org/es/vocabulario, última fecha de consulta el 9 de noviembre de 2014.

² *Idem*, última fecha de consulta el 9 de noviembre de 2014.

³ Pagliery, José, *Bitcoin and the Future of Money*, Triumph Books LLC, 2014, p. 5, <https://books.google.com.mx/books?id=r-ouBAAAQBAJ&printsec=frontcover&dq=bitcoin&hl=>

2009 cuando se publicó un enlace al programa del *software Bitcoin* que permite descifrar algoritmos que generan un *bitcoin*, en esa misma fecha se mina el primer lote de *bitcoins*. (indebidamente llamados moneda virtual).

El *Bitcoin* es una secuencia alfanumérica de treinta y tres caracteres obtenida a través de un *software minero*, que es un programa de cómputo con la función de descifrar un problema matemático, de cuya secuencia resulta la creación de un *bitcoin*.⁴ Se le llama *software minero* como una comparación a las excavaciones que tendrían que hacerse en una mina para poder encontrar oro, de forma análoga el ordenador utiliza su capacidad de procesamiento para descifrar un problema matemático, la computadora que cuente con mayor capacidad de procesamiento tendrá mayores probabilidades de descifrar el problema y como resultado generar un bitcoin.

El *Bitcoin* utiliza la tecnología *Peer to Peer*, cuya traducción significa punto-a-punto y se abrevia *P2P*,⁵ siendo una tecnología de código abierto para operar sin una autoridad central o banco, gestionando las transacciones y la emisión de *bitcoins* a través de la red.⁶ Nadie posee o controla el protocolo *Bitcoin* y todo el mundo puede participar.

Los que hacen seguro al *Bitcoin* son dos elementos. El primero, una cadena de bloque que se comparte y consulta con todas las máquinas mineras que lo validan. El segundo, el sistema de cifrado de clave pública.⁷ “Los sistemas criptográficos de clave pública utilizan un par de claves complementarias, mediante una de ellas se realiza el cifrado y la segunda se emplea para descifrar el mensaje. Una de las claves se mantiene secreta y la otra se hace pública. El hecho de que una de las claves se publique no compromete

es-419&sa=X&ei=zzjZVPLkLIq2yQTMuYCwDg&ved=0CDMQ6AEwAQ#v=onepage&q=bitcoin&f=false, última fecha de consulta el 9 de febrero de 2015.

⁴ Bitcoin. “Preguntas más frecuentes”, www.bitcoin.org/es/faq, última fecha de consulta el 9 de noviembre de 2014.

⁵ Wai-Sing Loo, Alfred, *Peer to Peer Computing: Building Supercomputers with Web Technologies*, Springer, 2007, p. 7, https://books.google.com.mx/books?id=6ftYxEokK7AC&pg=PA7&dq=peer+to+peer+definition&hl=es-419&sa=X&ei=XU_ZVM6xNIOVyATk6oLgCA&ved=0CBsQ6AEwAA#v=onepage&q=peer%20to%20peer%20definition&f=false, última fecha de consulta el 9 de febrero de 2015.

La red punto a punto (P2P) es una red de computadoras que permiten el intercambio directo de información entre los ordenadores conectados. Estas redes no requieren de clientes o servidores fijos, sino que forman una serie de nodos que funcionan como iguales, actuando simultáneamente como clientes y servidores respecto del resto de los nodos de la red.

Con acceso al código fuente de un programa de cómputo, desarrollado y distribuido libremente.

⁶ Bitcoin, <http://bitcoin.org/es/>, última fecha de consulta el 9 de noviembre de 2014.

⁷ Bitcoin Wiki, FAQ, “What is mining?”, <https://en.bitcoin.it/wiki/FAQ#Mining>, última fecha de consulta el 9 de noviembre de 2014.

la seguridad de la comunicación, ya que es imposible determinar la clave privada a partir de la clave pública”.⁸

La cadena de bloques se basa en el registro público y compartido de transacciones (entendidas como transferencias de valor entre las direcciones de *Bitcoin* que se incluyen en la cadena de bloques) en toda la red *Bitcoin*, las transacciones confirmadas se incluyen en la cadena de bloques sin excepción, de esa forma nuevas transacciones pueden ser verificadas asegurando que el cargo se hace a la cuenta que realiza el pago.

La integridad y el orden cronológico de la cadena de bloques se realizan mediante criptografía.⁹

El monedero *Bitcoin* mantiene una pieza secreta de datos denominada *llave privada* asignada a cada dirección *Bitcoin* que se utiliza para firmar cada operación como una prueba matemática que proviene de su propietario. Todas las transacciones son transmitidas por los usuarios y confirmadas por la red en un proceso llamado *minería*.

La *minería* consiste en descifrar un problema matemático para que se genere un *bitcoin*, requiere para su funcionamiento de la red *Bitcoin*, que es un acuerdo distribuido entre todos los equipos que participan en el proceso, para confirmar las transacciones e incluirlas en la cadena de bloques que será sometido a un paquete de cifrado y que será verificado por la red.

El *software* y la red *Bitcoin* impiden que otra persona pueda incluir nuevos bloques consecutivamente en la cadena; ninguna persona puede controlar lo que está incluido en ésta o reemplazar partes de la cadena de bloques para revertir sus propios gastos.¹⁰

⁸ España Boquera, María Carmen, *Servicios avanzados de telecomunicación*, España, Ediciones Díaz Santos, 2003, p. 61, <https://books.google.com.mx/books?id=yTSoYCiXYAAC&pg=PA61&dq=cifrado+de+clave+p%C3%BAblica&hl=es-419&sa=X&ei=y7PZVIvmJbPdsATfy4CQBw&ved=0CckQ6AEwAQ#v=onepage&q=cifrado%20de%20clave%20p%C3%BAblica&f=false>, última fecha de consulta el 9 de febrero de 2015.

⁹ Bitcoin, “Cómo funciona Bitcoin”, <http://bitcoin.org/es/como-funciona>, última fecha de consulta el 9 de noviembre de 2014.

Minería es la función que desarrolla el programa de cómputo Bitcoin, cuyo propósito es descifrar un problema matemático que genera un bitcoin; para que pueda llevarse a cabo la minería es necesario que los ordenadores que cuentan con el programa Bitcoin siempre estén conectados a la red para validar la información de la cadena de bloques del bitcoin que se genere, además de validar la cadena de bloques en otras transacciones.

¹⁰ *Idem*.

En el sistema *Bitcoin* (llamado también economía *bitcoin*) una vez minado el número total de unidades, no podrán generarse otras adicionales, los impulsores de este sistema destacan esta característica porque el dinero convencional es emitido por los bancos centrales que pueden emitir dinero fiduciario en el momento que lo determinen, generando un exceso de circulante que produce la inflación; comparan que, por el contrario, en el sistema *bitcoin* no habrá exceso

El *software Bitcoin* está diseñado para que cada bloque emita un determinado número de unidades *bitcoin* que se reduce a la mitad cada 210 000 bloques dificultado con el tiempo la *minería* de nuevos *bitcoins* que no podrán ser superiores a 21 millones, se estima que el último *bitcoin* estará disponible hacia el año 2140, con el bloque #6 929 999. Los simpatizantes han llamado a esto economía bitcoin, refieren que se trata de un modelo económico deflacionario porque no podrán generarse unidades adicionales.¹¹

El número total de unidades en ese momento permanecerá estático en 20 999 999.9769.¹² Para julio de 2014 existían 13 458 925 *BTC* en circulación, con un histórico creciente desde el año 2009.¹³

Debido a la ley de la oferta y la demanda,¹⁴ cuanto menos *bitcoins* estén disponibles, los que queden tendrán mayor demanda y por tanto tendrán un valor más alto.¹⁵

de unidades, por eso consideran que *bitcoin* es un modelo económico deflacionario. Sin embargo, para que se actualice la deflación tendría que generarse una disminución general de precios en un determinado lugar, hecho que *bitcoin* no ha generado, por lo tanto, el simple hecho de que exista un número limitado de *bitcoins* no garantiza un modelo económico deflacionario.

¹¹ Mochón, Francisco, *Principios de economía*, 4a. ed., México, McGraw Hill, 2010, pp. 333, 339 y 340.

La deflación ocurre cuando desciende el nivel general de precios, debido a una tasa de inflación negativa.

Cuando se utilizaba el oro, la abundancia o escasez de moneda en circulación, determinaba la subida o bajada de precios.

Con la progresiva sustitución del patrón metálico por la moneda fiduciaria, respaldada por un banco central nacional, el volumen de moneda en circulación se desligó de las reservas metálicas. La discrecionalidad de la gestión monetaria permitía ajustar la oferta monetaria a las oscilaciones de la producción agraria e industrial pero, a la vez, constituía una fuerte tentación para los estados ávidos de fondos que gastar.

Según los monetaristas, el crecimiento de la cantidad del dinero determina la tasa de inflación a largo plazo; los cambios en la cantidad de dinero influyen principalmente en los precios.

En el modelo inflacionario se genera más cantidad de dinero fiduciario, lo que produce un aumento de los precios y una reducción del poder adquisitivo.

¹² Bitcoin Wiki, FAQ, "How long will it take to generate all the coins?", https://en.bitcoin.it/wiki/FAQ#How_long_will_it_take_to_generate_all_the_coins.3F, última fecha de consulta el 9 de noviembre de 2014.

¹³ Blockchain Info, Gráficos, "Total de bitcoins en circulación", http://blockchain.info/es/charts/total-bitcoins?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=, última fecha de consulta el 9 de noviembre de 2014.

¹⁴ Mochón, Francisco, *op. cit.*, nota 11, pp. 40 y 45.

La ley de la demanda se refiere a la relación inversa existente entre el precio de un bien y la cantidad demandada, en el sentido de que al aumentar el precio disminuye la cantidad demandada, y lo contrario ocurre cuando se reduce el precio.

La ley de la oferta expresa la relación directa que existe entre el precio y la cantidad ofrecida: al aumentar el precio se aumenta la cantidad ofrecida.

¹⁵ Bitcoin Wiki, FAQ, "But if no more coins are generated, what happens when Bitcoins are lost? Won't that be a problem?", https://en.bitcoin.it/wiki/FAQ#If_no_more_coins_

Los *bitcoins* tienen valor porque son útiles y porque son escasos; en la medida en que sean aceptados en un mayor número de comercios, su valor se estabilizará.¹⁶ Es de destacar que los *bitcoins* tienen un valor de cambio y no cuentan con un valor inherente.

Existen sitios con listas de comercios que reciben como forma alternativa de pago el *bitcoin*, como es el caso del sitio <https://es.bitcoin.it/wiki/Comercio> en el que por país indica los establecimientos que lo reciben.¹⁷ O bien, el sitio web <https://en.bitcoin.it/wiki/Trade> que indica el uso del mismo por categoría de producto o servicio.¹⁸

El *bitcoin* ha cobrado fuerza por la preferencia que ha tenido como forma alternativa de pago en diversas transacciones; es así que, en abril de 2013, alcanzó un valor de mercado por la cantidad de 2 614 956 613.67025 USD. Sin embargo, en mayo del mismo año, tras la noticia de la incautación de cuentas asociadas con Mt.Gox (en ese momento principal casa de cambio de *bitcoins*), por no haberse registrado como transmisor de dinero ante el *FinCEN Financial Crimes Enforcement Network* (Departamento de lucha contra el lavado de dinero en EUA), el valor de capitalización de mercado descendió a 1 283 804 110.671 USD.¹⁹

En noviembre de 2013, el *New York Times* publicó que el vicegobernador del Banco Popular de China y director de la Administración Estatal de Divisas dijo que sería imposible que el Banco Central de China reconociera a *bitcoin* como instrumento financiero legítimo en un futuro próximo y que “la gente es libre de participar en el Mercado de Bitcoin y adoptar personalmente una perspectiva a largo plazo”.²⁰ Esta declaración desató el interés por parte

are_going_to_be_generated.2C_will_more_blocks_be_created.3F, última fecha de consulta el 9 de noviembre de 2014.

¹⁶ Bitcoin Wiki, FAQ, “Where does the value or Bitcoin stem from? What backs up Bitcoin?”, https://en.bitcoin.it/wiki/FAQ#Where_does_the_value_of_Bitcoin_stem_from.3F_What_backs_up_Bitcoin.3, fecha de última consulta el 9 de noviembre de 2014.

¹⁷ Bitcoin Wiki, “Comercio”, <https://es.bitcoin.it/wiki/Comercio>, fecha de última consulta el 9 de noviembre de 2014.

¹⁸ Bitcoin Wiki, “Trade”, <https://en.bitcoin.it/wiki/Trade>, fecha de última consulta el 9 de noviembre de 2014.

¹⁹ Blockchain Info, Gráficos, “Capitalización de mercado”, <http://blockchain.info/es/charts/market-cap>, fecha de última consulta el 9 de noviembre de 2014.

²⁰ *International New York Times*, “Bitcoin gets a caution nod from China’s Central Bank”, <http://sinosphere.blogs.nytimes.com/2013/11/22/bitcoin-gets-a-cautious-nod-from-china-central-bank/>, última fecha de consulta el 9 de noviembre de 2014.

“Administration of Foreign Exchange, said that it would be impossible for China’s Central Bank to recognize the Bitcoin as a legitimate financial instrument in the near future. But, Mr.Yi added, people are free to participate in the Bitcoin market and he would personally adopt a long-term perspective on the currency”.

de la población de este país de adquirir *bitcoins*, lo que detonó el precio que al día 26 de noviembre de 2013 fue de 942 dólares por *bitcoin*; ello provocó una capitalización de mercado con un valor de 10 815 909 623 dólares. Como referencia, es necesario mencionar que el valor de un *bitcoin* al 15 de agosto de 2013 fue de 109.5 dólares (82.04 euros).²¹ A principios de diciembre de 2013 el Banco Central chino prohibió a las instituciones financieras cualquier transacción que involucrara *bitcoins*, ese mismo mes se anunciaron medidas restrictivas suplementarias. Debido a esto la plataforma *Bitcoin* China debía suspender los depósitos en yuanes que los usuarios podían hacer en sus carteas electrónicas; tales decisiones han repercutido en la caída de los precios.²²

En marzo de 2014 el Banco Popular de China exigió a los bancos y casas de cambio cerrar antes del 15 de abril de 2014, todas las cuentas abiertas por los operadores de los sitios webs que comercian con *bitcoins*, los titulares de las cuentas podrían retirar el dinero pero no se podían hacer nuevos depósitos, por lo que los interesados en continuar con la actividad tendrían que mover sus servidores fuera del país; en ese momento China era uno de los mercados de mayor demanda de *bitcoins*, por lo que tal declaración provocó la caída en el precio de la unidad que en esa fecha se cotizó por debajo de los 500 dólares.²³

Los acontecimientos legales marcan la recuperación o caída del precio del *bitcoin*, tal es el caso del anuncio para considerar las operaciones de *bitcoins* para el pago de impuestos, o el arresto del presidente de la casa de cambio *BitInstant*, así como la cancelación del sitio y otras plataformas en la que se utilizaban *bitcoins*. En general, acontecimientos relacionados con la confianza o seguridad marcan la volatilidad y el precio del *bitcoin*, a manera de referencia tenemos que al 15 de agosto de 2013 un *bitcoin* podía adquirirse por 109.5 dólares,²⁴ mientras que al 27 de noviembre de 2013 por 1 044 dólares²⁵ y al 9 de noviembre de 2014 por 363.55 dólares.²⁶

²¹ En qué invertir, “Bitcoin en tiempo real”, <http://www.enqueinvertir.com/bitcoin-en-tiempo-real.php>, fecha de última consulta el 15 de agosto de 2013.

²² *El Economista*, “Se desploma la cotización del bitcoin por culpa de China”, <http://eleconomista.com.mx/mercados-estadisticas/2013/12/18/china-impacta-bitcoin>, fecha de última consulta el 9 de noviembre de 2014.

²³ *El País*, Tecnología, “El Banco Central chino ordena cerrar todas las cuentas con bitcoins”, http://tecnologia.elpais.com/tecnologia/2014/03/28/actualidad/1396002045_716448.html, fecha de última consulta el 9 de noviembre de 2014.

²⁴ Precio del bitcoin, <http://preciodelbitcoin.com/>, fecha de última consulta el 15 de agosto de 2013.

²⁵ CNN Money, “Bitcoin prices top \$1000”, <http://money.cnn.com/2013/11/27/investing/bitcoin-1000/>, fecha de última consulta el 9 de noviembre de 2014.

²⁶ CoinMill, “El convertidor de divisas”, http://es.coinmill.com/BTC_USD.html, última fecha de consulta el 9 de noviembre de 2014.

A diferencia de la moneda convencional, el *bitcoin* no cuenta con un respaldo en oro, por lo tanto, si se pierde la confianza en este medio alternativo de pago, su valor cae sin importar que sea escaso.

Por la naturaleza descentralizada y de código abierto, el *Bitcoin* es la primera red de pago gestionada por los usuarios. Se menciona que incluso los desarrolladores no tienen poder para forzar un cambio en el protocolo sin el apoyo de suficientes usuarios, desarrolladores o mineros que estén de acuerdo.²⁷ Se refiere que esta característica genera pagos seguros y coloca al *bitcoin* como una alternativa de pago en el comercio electrónico. Este protocolo fue diseñado para evitar la falsificación o la simulación y otros ataques.

Los *bitcoins* se guardan en un monedero electrónico desde el cual se hacen las disposiciones para los pagos o bien utilizando un servicio de *e-wallet*, cuya traducción sería carterita o monedero electrónico ofrecido por terceros.

Otra forma de adquirirlos es comprándolos a través de las casas de bolsa de *bitcoins*, entre las que se destacaba la japonesa *MtGox* que en febrero de 2014 se declaró en quiebra debido a la pérdida de más de 850 000 *bitcoins*.²⁸ Sin embargo, el 10 de marzo de 2014 se anunció el cierre de dicha plataforma, debido a una acción de piratería que significó la pérdida de 744 mil *bitcoins*, equivalente a 350 millones de dólares,²⁹ dicha casa de bolsa abandonó la idea de reestructurarse bajo la ley de protección a la bancarrota y pidió a un tribunal su liquidación.³⁰

Existen otras casas de bolsa de *bitcoins* en las que inclusive se ofrece el cambio de *bitcoins* por divisas de diferentes países, en la página de Internet <http://bitcoincharts.com/> se encuentra un convertidor que calcula el valor de compra y venta de cada una de las monedas de acuerdo con el valor de mercado que tenga el *bitcoin* al momento de la transacción.

La página www.bitcon.org ofrece servicios de pago para personas o empresas, refiriendo consejos sobre la forma en que puede protegerse el mone-

²⁷ Bitcoin, <http://bitcoin.org/es/bitcoin-para-entusiastas>, última fecha de consulta el 16 de agosto de 2013.

²⁸ *The Washington Post*, “Mt Gox collapse spurs calls to regulate Bitcoin”, http://www.washingtonpost.com/business/technology/mt-gox-collapse-spurs-calls-to-regulate-bitcoin/2014/02/28/df44f5c6-a0b7-11e3-a050-dc3322a94fa7_story.html, última fecha de consulta el 7 de enero de 2015.

²⁹ *El Universal*, “Desaparece de web plataforma de operaciones de Bitcoin”, <http://www.eluniversal.com.mx/finanzas-cartera/2014/bitcoin-plataforma-desaparece-990349.html>, fecha de última consulta el 9 de noviembre de 2014.

³⁰ CNN Tecnología, “China instala su primer cajero *bitcoin* pese a la presión de su gobierno”, <http://mexico.cnn.com/tecnologia/2014/04/16/china-instala-su-primer-cajero-de-bitcoin-pese-a-la-presion-de-su-gobierno>, última fecha de consulta el 9 de noviembre de 2014.

dero, informándoles que *bitcoin* no es anónimo ya que cualquiera puede ver el balance y las transacciones de cualquier dirección *Bitcoin*, sin embargo, la identidad del propietario no puede ser asociada con su dirección *Bitcoin*, hasta que la información personal sea revelada en un intercambio. Por otra parte, en el sitio web <https://blockchain.info/es/charts> se puede encontrar información graficada sobre el comportamiento de *bitcoin* desde distintas perspectivas.³¹

II. PROBLEMAS RELACIONADOS CON EL BITCOIN

1. *Desestabilización del sistema financiero centralizado*

Por ahora el valor de los *bitcoins* en circulación es poco en comparación con la suma acumulada del dinero que circula alrededor del mundo, emitido y reconocido por los gobiernos, sin embargo, cabe la reflexión sobre qué pasaría si el *bitcoin* se prefiriera en lugar de las monedas del gobierno.

Algunas notas en sitios web indican que en la crisis económica de Chipre se llegó a preferir al *bitcoin* como forma de asegurar el valor del dinero ante una posible confiscación o devaluación de la moneda de aquel país.³²

Además, hay que considerar que alrededor del *bitcoin* se ha desarrollado toda una industria, como son cajeros automáticos, máquinas mineras de mayor capacidad, casas de cambio, aplicaciones para teléfonos inteligentes, así como una red de comercios que aceptan como forma de pago dicha unidad.

2. *Competencia con el Sistema Bancario*

Por otra parte, los servicios generados alrededor de *bitcoin* tienen una similitud con los servicios que prestan los bancos. Por ejemplo:

- a) Servicios de cartera, equivalente a los servicios de depósito de valores.

³¹ Blockchain Info, Gráficos, <https://blockchain.info/es/charts>, última fecha de consulta el 9 de noviembre de 2014.

³² Rankia, Comunidad financiera, “La crisis de Chipre incrementa la fuga de dinero hacia bitcoin, los bancos centrales empiezan a preocuparse”, www.rankia.com/foros/bancos-cajas/temas/1723351-tesis-chipre-incrementa-fuga-dinero-hacia-bitcoin-bancos-centrales-empiezan-preocuparse, última fecha de consulta el 9 de noviembre de 2014.

- b) La transferencia electrónica de valores.
- c) El cambio de divisas.
- d) Cuentas empresariales mancomunadas.³³
- e) Aplicaciones telefónicas para conocer el valor del *bitcoin*, así como para realizar transferencias y pagos.³⁴
- f) Cajeros.

La diferencia es que el sistema bancario establecido en cada uno de los países se encuentra regulado por las leyes respectivas, y para poder ofrecer servicios bancarios se necesita cumplir con diferentes ordenamientos de seguridad, control, pago de impuestos, y otras obligaciones. Además de ser supervisadas por organismos gubernamentales que cuidan su funcionamiento dentro del marco de la ley.

Existe el riesgo que un número mayor de personas puedan interesarse en *bitcoin* y si éste sufriera un desplome o se utilizara para defraudar podría generar un problema social en donde los afectados pedirían al gobierno que se aplicaran las leyes para recuperar su dinero.

3. Operaciones ilícitas

A. Lavado de dinero

En mayo de 2013 las noticias de que *bitcoin* se había visto expuesta al lavado de dinero y otras actividades criminales, sometió a la mayor operadora de *bitcoins* a una investigación por parte del gobierno de Estados Unidos, por considerarla una institución que realiza servicios monetarios sin licencia y no cumplía con los lineamientos de la *Bank Secret Act (BSA)*, legislación sobre el secreto bancario, que establece la obligación de llevar un control o registro que permita identificar a las personas que realizan transacciones; la consecuencia fue que se intervinieron dos de sus cuentas.³⁵ En enero de 2014 se anunció el arresto del presidente de la casa de bolsa *BitInstant*, acusado de lavar dinero para los clientes de la plataforma *Silk Road (Ruta de la*

³³ Bitcoin, “Bitcoin for Businesses”, www.bitcoin.org/en/bitcoin-for-businesses, última fecha de consulta el 9 de noviembre de 2014.

³⁴ Blockchain Info, Monedero, “Mi monedero”, <https://blockchain.info/es/wallet>, fecha de última consulta el 9 de noviembre de 2014.

³⁵ Facua, Banca, “EEUU interviene dos cuentas a la mayor operadora de moneda virtual *Bitcoin*, la japonesa Mt. Gox”, <https://www.facua.org/es/noticia.php?Id=7617>, última fecha de consulta el 9 de noviembre de 2014.

seda) en la que se vendían drogas; de acuerdo con el anuncio la plataforma de *BitInstant* fue retirada.³⁶

En Estados Unidos el *FinCEN Financial Crimes Enforcement Network*, Departamento de lucha contra los delitos financieros, en marzo de 2013, determinó que las empresas dedicadas al intercambio de dinero debían inscribirse a este organismo y obtener una licencia obligatoria para llevar a cabo sus actividades.³⁷

B. Fraude

El interés en el incremento del valor del *bitcoin*, se ha utilizado para cometer fraudes engañando a personas para que inviertan en éstos a cambio de un rendimiento futuro, como ocurrió con la compañía *Bitcoin Save and Trust* que fue acusada junto con su fundador *Shavers*, por un grupo de personas que había entregado sus *bitcoins* a cambio de un rendimiento del 1% diario,³⁸ finalmente se descubrió que fueron víctimas de un fraude en el esquema *ponzi*.³⁹

C. Evasión fiscal

Como el *bitcoin* no está regulado en las leyes hacendarias, se ha dejado fuera de las declaraciones fiscales, lo que propicia la posibilidad de evasión fiscal; sin embargo, en Alemania se busca regular las actividades en *bitcoins* para que las ganancias sobre la venta sean consideradas para efecto del pago de impuestos.⁴⁰ En Estados Unidos se estableció considerar a *bitcoin* como una propiedad para efecto del pago de impuestos.⁴¹

³⁶ CNN Español, “Arrestan a dos operadores de bitcoin por lavado de dinero”, <http://cnnespanol.cnn.com/2014/01/27/arrestan-a-dos-operadores-de-bitcoin-por-lavado-de-dinero/>, última fecha de consulta el 9 de noviembre de 2014.

³⁷ FinCEN, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies”, http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html, última fecha de consulta el 9 de noviembre de 2014.

³⁸ Forbes, “Federal Judge Rules Bitcoin is Real Money”, www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/, última fecha de consulta el 9 de noviembre de 2014.

³⁹ U.S. Securities and Exchange Commission “Ponzi Schemes”, <http://www.sec.gov/answers/ponzi.htm>, última fecha de consulta el 7 de enero de 2015.

⁴⁰ Techcrunch, “Germany Recognizes Bitcoin as “Private Money”, sales tax coming soon”, www.techcrunch.com/2013/08/19/germany-recognizes-bitcoin-as-private-money-sales-tax-coming-soon/?utm_medium=referral&utm_source=pulseneews, última fecha de consulta el 9 de noviembre de 2014.

⁴¹ USA Today, “IRS: Answer to tax questions about Bitcoin”, <http://www.usatoday.com/story/money/business/2014/03/25/irs-answers-on-bitcoin-tax-guidance/6874925/>,

D. *Narcotráfico y otras actividades ilícitas*

En octubre de 2013, una noticia de la *BBC* indica que el sitio web *Silk Road*, utilizado para la venta de drogas fue tomado por el FBI y los bitcoins confiscados.⁴² Por otra parte, la cadena de noticias *CNN* indica que en la *deep web*,⁴³ utilizando el cifrado *Tor*,⁴⁴ en el año 2011 se creó un sitio identificado como *Silk Road* que permitía a los usuarios el comercio de bienes y servicios ilegales, utilizando *bitcoin* como pago, dicho sitio fue cerrado por el FBI y el presunto creador arrestado.⁴⁵

IV. REFLEXIONES SOBRE LA NATURALEZA JURÍDICA DE BITCOIN

1. *¿El bitcoin puede ser moneda?*

De acuerdo con la información obtenida en diferentes fuentes periodísticas y páginas web, podemos observar que al *bitcoin* se le viene atribuyendo el término de moneda (aspecto de mercadotecnia), debido a que uno de sus usos permite cambiarlo por bienes o servicios en una actividad equiparable al dinero, ya que inclusive permite dividirse en unidades más pequeñas.⁴⁶

última fecha de consulta el 9 de noviembre de 2014. Véase también IRS, “Virtual currency Guidance: Virtual currency is treated as Property for U.S. Federal Tax Purposes; General Rules for property Transactions Apply”, <http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance>, última fecha de consulta el 9 de noviembre de 2014.

⁴² BBC News Technology, “Bitcoin value drops after FBI shuts Silk Road drugs site”, www.bbc.co.uk/news/technology-24381847, última fecha de consulta el 9 de noviembre de 2014.

⁴³ Casademo, Jordi (coord.), *Redes de comunicaciones: de la telefonía móvil a Internet*, Universitat Politècnica de Catalunya, 2010, p. 151, <https://books.google.com.mx/books?id=2D9FO9nX-XsC&pg=PA151&dq=internet+profunda&hl=es-419&sa=X&ei=ljnZVK3MFI0yQTqZIC4BA&ved=0CCEQ6AEwAQ#v=onepage&q=internet%20profunda&f=false>, última fecha de consulta el 9 de febrero de 2015.

⁴⁴ Areitio, J. Javier, *Seguridad de la Información. Redes informáticas y sistemas de información*, Paraninfo, 2008, p. 298, https://books.google.com.mx/books?id=_z2GcBD3deYC&dq=red++tor&hl=es&source=gbs_navlinks_s, última fecha de consulta el 7 de enero de 2015.

⁴⁵ CNN World, “How FBI caught Ross Ulbricht, alleged creator or criminal marketplace Silk Road”, <http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html>, última fecha de consulta el 9 de noviembre de 2014.

⁴⁶ Bitcoin Wiki, “Units”, <https://en.bitcoin.it/wiki/Units>, última fecha de consulta el 9 de noviembre de 2014.

Sin embargo, el *bitcoin* no es moneda o dinero propiamente dicho porque no lo emite ningún gobierno; los autorizados para emitir billetes y acuñar moneda son los bancos centrales de los diferentes países; dicha actividad es área estratégica del gobierno y, por lo tanto, ningún particular está autorizado para ejercer tal función.⁴⁷

Cualquier actividad particular tendiente a generar cosas que puedan ser intercambiadas por otros bienes o servicios será una actividad de trueque, sin embargo, el caso de *bitcoin* tiene algunas particularidades.

En primer término, *bitcoin* no es una moneda sino un algoritmo que únicamente puede ser intercambiado o transferido dentro del protocolo del *software Bitcoin*, por lo tanto no es aceptado de forma general, ni puede intercambiarse físicamente sino a través de medios electrónicos.

Por otra parte, si bien es cierto que en la actualidad los bancos utilizan medios electrónicos para realizar transferencias y operaciones de pago de divisa convencional, también es cierto que ese hecho no modifica la naturaleza jurídica de las monedas convencionales, ya que se depositan para que pueda hacerse su representación electrónica; ese dinero está sujeto al control del gobierno que las emitió, contando con una reserva para respaldar su valor, o bien, la moneda puede contar con un valor intrínseco si sus materiales son metales preciosos; en cualquiera de los casos el Estado concede a la moneda la calidad de “dinero” con un valor específico.

Por otro lado, para que un bien sea considerado como dinero debe cubrir tres principales funciones a) como medio de intercambio, se utiliza para pagar por bienes y servicios; b) como unidad contable, para medir y comparar el valor de otros bienes; c) como almacén de valor, conserva el valor comercial para futuro intercambio.⁴⁸ Además, el dinero es reconocido por los gobiernos de otros países que a su vez emiten sus propias monedas y que intercambian entre ellos a través de los entes financieros autorizados.

Por el contrario, en el caso de *bitcoin* no existe un país o Estado que pueda controlar su valor ni su emisión; en realidad el *bitcoin* no es un bien tangible sino intangible que a diferencia de las monedas convencionales, no cuenta con una reserva que lo respalde; tampoco cuenta con metales preciosos que le generen un valor intrínseco; el valor del *bitcoin* lo genera la ley de la oferta y la demanda, en la medida que se acepta como unidad de intercambio; por esa razón la función de unidad contable para fijar precios y

⁴⁷ Artículo 28, séptimo párrafo de la Constitución Política de los Estados Unidos Mexicanos.

⁴⁸ Mishkin, Frederic S., *Moneda, banca y mercados financieros*, 10a. ed., México, Pearson, 2014, pp. 53, 54 y 55.

documentar deudas no es del todo estable, ya que si bien es cierto se pudiera hablar de uno o diez *bitcoins* como referencia de precio o deuda, también es cierto que el valor del *bitcoin* no es nominal sino volátil dependiendo de las circunstancias que influyan en su demanda, por lo que es inestable.

La función como almacén de valor que permita transferir la capacidad para comprar bienes y servicios a lo largo del tiempo pudiera actualizarse mientras el *bitcoin* sea aceptado como medio de pago, con la limitante que el mercado en el que es aceptado es muy pequeño en comparación con la economía mundial, además que debido a su volatilidad puede cotizarse en el futuro a un precio inferior al que se adquirió, por lo tanto, la inversión se depreciaría. La única función que pudiera coincidir con la función del dinero es la de intercambio ya que el *bitcoin* es aceptado a cambio de bienes y servicios.

Una publicación de *Forbes* indicó que un juez federal de Estados Unidos declaró que el *bitcoin* es dinero; esta declaración se hizo en razón de la demanda que un grupo de personas realizaron en contra de Trendon T. Shavers, fundador de *Bitcoin Save and Trust*, ya que en noviembre de 2011 Shavers anunció que estaba en el negocio de vender *bitcoins* a un grupo de personas locales y ofreció a los inversores 1% de interés diario.⁴⁹

La *SEC Security Enforcement Commission*, regulador bursátil en EUA, acusa de fraude a *Bitcoin Save and Trust* por las operaciones que realizó a través de un sistema *ponzi* en el que se prometía a los inversionistas de *bitcoins* un 7% de rentabilidad semanal por las operaciones que *Bitcoin Save and Trust* realizaba con los *bitcoins*, entre las que se incluía la venta de estas divisas a personas que querían comprar grandes cantidades. El acusado utilizaba los rendimientos para pagar a los que se iban incorporando, mientras se transferían a sus cuentas más de 150 000 *bitcoins* que utilizó, entre otras cosas, para pagar el alquiler, comida, bebida y apuestas. Finalmente, la pirámide se vino abajo y se anunció el cierre de la plataforma.⁵⁰ En este caso el argumento de la defensa fue que *SEC* y los tribunales no tenían jurisdicción porque *bitcoin* no es dinero.

La *SEC* alegó que el termino *security* (valores) comprende cualquier nota, valores, acciones propias, seguridad futura, un canje basado en bonos o valores y contrato de inversión es cualquier contrato, transacción o esquema

⁴⁹ Forbes, "Federal Judge Rules Bitcoin is Real Money", www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/, última fecha de consulta el 9 de noviembre de 2014.

⁵⁰ El Bitcoin.org, "Bitcoin es dinero, dice un juez de Texas", <http://elbitcoin.org/bitcoin-es-dinero-dice-juez-texas/>, última fecha de consulta el 9 de noviembre de 2014.

de participación de una inversión de dinero en una empresa común y con la expectativa de los beneficios que se puedan alcanzar en el futuro.

Debido a la controversia sobre la competencia de la *SEC*, el caso llegó al juez estadounidense L. Mazzant para determinar si las inversiones realizadas en el caso *Bitcoin Save and Trust* corresponden a los valores (*security*) definidos por las leyes de valores; el juez se pronunció y dijo que el término *security* se define como cualquier nota, valores, acciones propias de una garantía futura, canjes basados en valores. Además, precisó que un contrato de inversión es cualquier contrato, transacción, o esquema de participación de una inversión en dinero en una empresa con la expectativa de los beneficios que deriven del esfuerzo del promotor o de un tercero. Señaló que *bitcoin* puede ser utilizado como dinero, puede ser utilizado para comprar bienes o servicios, o para pagar gastos personales como Shavers demostró. La única limitación es la de los lugares que lo aceptan como moneda. Además, también se puede cambiar por moneda convencional, como el dólar estadounidense, el euro, el yen y el yuan, por lo que es una moneda o forma de dinero y los inversores que quisieron invertir en *Bitcoin Save and Trust* realizaron siempre una inversión en dinero.⁵¹

El juez determinó que las inversiones en *Bitcoin Save and Trust* cumplen con la definición del contrato de inversión y, por lo tanto, de valor financiero, por lo que considera que la Corte tiene jurisdicción sobre ese caso.⁵² Cabe mencionar que ésta es la primera resolución en la que un juez trata el tema de *bitcoin*.

Del análisis de la resolución del juez Mazzant se advierte que el estudio fue para determinar si los contratos realizados entre Shavers y los afectados correspondían o no a contratos de inversión, en ningún momento era determinar la naturaleza jurídica del *bitcoin* como moneda; más bien se enfoca en el *uso* que se da a éste, señalando que se utiliza para comprar bienes o servicios y como una unidad documentada en un contrato de inversión.

Por esta razón, considero que cuando el juez refirió que *bitcoin* se usa como moneda y que es una forma de moneda o dinero, la palabra “*forma*” se realizó en un plano de equiparación en cuanto a funcionalidad y no en cuanto a su naturaleza jurídica.

En ese sentido, el *Internal Revenue Service*, Servicio de Impuestos Internos de Estados Unidos, en marzo de 2014, emitió una guía de respuestas a las

⁵¹ Case 4:13-CV-416, Memorandum opinion regarding the court’s subject matter jurisdiction, “Securities and exchange commission v. Trendon T. Shavers and Bitcoin Saving and Trust”, <http://www.courthousenews.com/2013/08/06/Bitcoin.pdf>, última fecha de consulta el 9 de noviembre de 2014.

⁵² *Idem*.

preguntas de impuestos sobre *bitcoin*, aclarando que para efectos de impuestos federales, *bitcoin* es considerado como una propiedad y no como una moneda.⁵³

Por otra parte, una noticia indica que Alemania ha reconocido a *bitcoin* como moneda privada,⁵⁴ sin embargo esta nota se refiere a una comparecencia que el ministro de economía realizó ante el parlamento en donde señaló a *bitcoin* como unidad de cambio y no existe decreto del parlamento que reconozca a *bitcoin* como dinero en cuanto a su naturaleza jurídica independiente, sino que está vinculado a los particulares que la aceptan como pago, aun así se ventila la posibilidad de que las ganancias de la venta realizada en *bitcoins* sean objeto de pago de impuestos.⁵⁵

La denominación dinero electrónico o moneda virtual que se ha atribuido a *bitcoin* se debe, por una parte, a una cuestión de mercadotecnia y, por otra, a que no existe una disposición que reserve el término a las entidades autorizadas para emitir dinero electrónico; es importante que a la representación electrónica del dinero también se le otorguen las garantías y el respaldo que tienen las monedas convencionales respaldadas por los gobiernos, es decir, una unidad de dinero electrónico debería estar respaldada por una unidad de moneda convencional respaldada por las reservas del gobierno.

En este sentido España reguló la emisión del dinero electrónico, emitiendo la Ley 21/2011 de dinero electrónico⁵⁶ y el Real Decreto 778/2012 del 4 de mayo de 2012, en el que se precisa el régimen jurídico aplicable a la emisión del dinero electrónico, señalando que únicamente pueden emitir dinero electrónico las entidades debidamente autorizadas y reconocidas en la ley, las que deberán contar con un capital social, se indica que el dinero electrónico contará con un valor nominal que en el momento de ser solicitado deberá reembolsarse el valor monetario del dinero que se disponga. Las entidades de dinero electrónico están sujetas a supervisión y pueden ofrecer servicios de pago. La denominación de entidad de dinero electrónico y

⁵³ Internal Revenue Service, "Notice 2014-21", Notice regarding taxes that apply to transaction using virtual currencies, <http://www.irs.gov/pub/irs-drop/n-14-21.pdf>, última fecha de consulta el 9 de noviembre de 2014.

⁵⁴ *El Economista*, "El gobierno alemán reconoce oficialmente la moneda virtual bitcoin", www.economista.mobi/mercados-cotizaciones/noticias/5078793/08/13/El-Gobierno-aleman-reconoce-oficialmente-la-moneda-virtual-bitcoin.html, última fecha de consulta el 9 de noviembre de 2014.

⁵⁵ Techcrunch. *op. cit.*, nota 40.

⁵⁶ *Boletín Oficial del Estado*, "Ley 21/2011, de 26 de julio, de dinero electrónico", Madrid, 27 de julio de 2011, Sec. I. p. 84235, <https://www.boe.es/boe/dias/2011/07/27/pdfs/BOE-A-2011-12909.pdf>, última fecha de consulta el 9 de noviembre de 2014.

su abreviatura EDE, están reservadas a las entidades autorizadas, estableciendo la prohibición de utilizar dicha denominación sin autorización. Se exceptúan de la ley las redes limitadas de proveedores o servicios (vales de servicio de guardería, vales de servicios sociales, etcétera).⁵⁷

En este mismo sentido el 16 de enero de 2013, Perú emitió la Ley 29985 que regula la emisión del dinero electrónico, así como la supervisión de las empresas que lo emiten. Se define al dinero electrónico como un valor monetario representado por un crédito exigible a su emisor con la característica que es almacenado en un soporte electrónico, aceptado como medio de pago por una entidad distinta al emisor, es emitido por un valor igual a los fondos recibidos, es convertible a dinero en efectivo, no constituye depósito y no genera intereses.⁵⁸

Por lo tanto, el *bitcoin* no es dinero electrónico sino un *criptoalgoritmo* que tiene un mensaje de datos que genera un documento electrónico y a la vez una anotación en cuenta contenida en el monedero.

2. ¿*Bitcoin*, título de crédito electrónico?

Sabemos que con los avances de la informática y la actualización de la legislación, actualmente contamos con títulos de crédito electrónicos, cuyo antecedente fueron los títulos de crédito que otorgaban al tenedor del documento (papel) la posibilidad de exigir del suscriptor el cumplimiento de la obligación en el documento consignado. En ese supuesto se encuentran los pagarés, las letras de cambio y las acciones. Estos documentos son generadores de riqueza desde el momento en que el obligado los firma y se compromete a cumplir con el pago, además estos documentos pueden ponerse en circulación y negociarse a cambio de otros productos o servicios.

Tomando en consideración lo anterior, ¿al ser el *bitcoin* un documento electrónico sería o no equiparable a un título de crédito? Nuevamente la posibilidad de intercambiarse por productos o servicios contra la entrega del documento electrónico pudiera llevarnos a responder que sí es un título de crédito electrónico; sin embargo, cuando consideramos que el título de

⁵⁷ Boletín Oficial del Estado, “Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico”, Madrid, publicado el 5 de mayo de 2012, Sec. I, p. 33992, <https://www.boe.es/boe/dias/2012/05/05/pdfs/BOE-A-2012-5993.pdf>, última fecha de consulta el 9 de noviembre de 2014.

⁵⁸ Banco Central de la Reserva de Perú, “Ley No. 29985: Ley del Dinero Electrónico”, <http://www.bcrp.gob.pe/transparencia/normas-legales/ley-del-dinero-electronico.html>, última fecha de consulta el 9 de noviembre de 2014.

crédito necesariamente debe ser suscrito o emitido por una persona física o moral a quien hacerle exigible la obligación,⁵⁹ ese hecho ya no coincide con la característica del *bitcoin* que no se le puede exigir a ninguna persona, ya sea física o moral, de modo que quien recibe un *bitcoin* asume el riesgo que éste no le fuera aceptado en otro intercambio y no tendría contra quien exigir la obligación.

Por otra parte, un título de crédito siempre tiene una cantidad cierta que se obliga a cubrir quien lo suscribe, sin embargo el *bitcoin* no cuenta con una cantidad cierta ni determinada, ya que el valor del *bitcoin* será variable.

Si bien es cierto que estamos familiarizados con los títulos de crédito desmaterializados, también es cierto que el *bitcoin* no cumple con las cuatro características que deben tener los títulos de crédito que son: *incorporación* de la obligación en el propio documento; *legitimación* significa que quien posea el título está autorizado para ejercer el derecho documentado en el mismo y que tiene el endoso a su favor, posesión y presentación del título a quien deberá pagarlo; *literalidad* se refiere a lo que resulte del texto consignado; y, finalmente, la *autonomía* se refiere a que el portador ejerce un derecho propio distinto e independiente de las relaciones jurídicas existentes entre los anteriores poseedores;⁶⁰ en ese sentido, el *bitcoin* carece de legitimación porque su tenedor no sabrá a quién exigir la obligación, carecen de incorporación y literalidad porque no tienen una obligación expresamente consignada, y la autonomía es cuestionable porque su valor depende de la validación de la cadena de bloques de la operación precedente. Por lo anterior, el *bitcoin* no es un título de crédito.

3. Entonces, ¿qué es el *bitcoin*?

Volviendo a la esencia del *bitcoin*, tenemos que es un bloque encriptado, generado por un algoritmo; el bloque contiene información en un mensaje de datos que puede entenderse como un documento electrónico, entonces tiene la característica de ser una cosa que no podemos ver y que sólo puede interpretarse a través del *software* que lo creó, por lo tanto, es un *bien intangible* que tendrá valor y se considerará como activo mientras sea aceptado.

El *bitcoin* es un *criptoalgoritmo* de intercambio con tres funciones: 1) trueque de bienes o servicios; 2) de cambio monetario, y 3) de especulación, con

⁵⁹ Durán Díaz, Oscar Jorge, *Los títulos de crédito electrónicos, su desmaterialización*, México, Porrúa, 2009, p. 27.

⁶⁰ *Ibidem*, p. 33.

el que se espera obtener una ganancia de capital para después cambiarse en una operación de trueque o de cambio monetario.

A lo largo de la historia el comercio ha evolucionado de diferentes formas; los modelos de negocio se han vuelto cada vez más sofisticados, pero sin importar siempre recibían a cambio del producto o servicio, una contraprestación tangible, ya fuera en el sistema de trueque o en el sistema del dinero existía algo que físicamente se intercambiaba; sin embargo, en el caso del *bitcoin* las personas venden cosas o servicios a cambio de un *bien intangible* que no pueden ver ni tocar y que no tiene un respaldo económico.

El hecho que estos *bienes intangibles* sean utilizados como forma de pago pone en entredicho a las legislaciones actuales que no han previsto una figura igual, por consecuencia en muchos países, entre éstos México, no hay reglas para quienes los generan, ni para quienes los intercambian ni mucho menos para quienes lo reciben como formas de pago.

IV. FUTURO DE LOS CRIPTOALGORITMOS DE INTERCAMBIO

Es importante destacar que el *bitcoin* no es el único algoritmo que está compitiendo por posicionarse como *bien intangible de intercambio*; existen alrededor de cien *criptoalgoritmos* conocidos como *altcoins* que compiten entre sí.⁶¹

El que ha logrado mayor posicionamiento hasta el momento es el *bitcoin*, en segundo lugar el *litecoin* que logró mejorar los tiempos de validación de las operaciones reduciéndolos de diez a dos minutos; y en tercer lugar se encuentra el *PPcoin* que en su proceso de minería logró mejorar el ahorro de energía.⁶²

El *software* de *Bitcoin* es de código abierto, este hecho permite utilizarlo para hacerle cambios o mejoras, sin embargo, eso no significa que se modifique el código con el que funciona el *bitcoin*, ya que parte de su éxito se basa en la desconfianza de los usuarios que no permitirían variantes al sistema; por el contrario, las modificaciones son las que están dando lugar a las *altcoins* (alternativas de algoritmos de intercambio).

Los factores que pueden influir sobre el futuro de los *criptoalgoritmos* (*bitcoin*) tanto en su valor como permanencia son, por una parte, las acciones

⁶¹ Criptomonedas, “Bitcoin y las nuevas monedas virtuales que están cambiando al mundo”, www.criptomonedas.org/altcoins-monedas-alternativas/#more-160, última fecha de consulta el 9 de noviembre de 2014.

⁶² MIT Technology Review, “Bitcoin no es la única criptomoneda que existe”, www.technologyreview.es/read_article.aspx?id=42902, última fecha de consulta el 9 de noviembre de 2014.

que los particulares tengan ante éstos y, por otra, las medidas que adopten los gobiernos.

Las acciones de los particulares están directamente relacionadas a su aceptación, de esa forma, en la medida que más comercios acepten el pago de productos y servicios con *bitcoins* o *altcoins*, mayor será la demanda y, como consecuencia, su valor. Por el contrario, a menor demanda y aceptación, menor valor, esta hipótesis no llevaría a su desaparición, pero sí afectaría su capacidad de cambio.

Con respecto a las *acciones de los gobiernos* una reacción sería la *prohibición*, sin embargo, el hecho de prohibir las *criptoalgoritmos* de intercambio en un país o en todo el mundo no es un factor determinante para que éstos desaparezcan, puesto que mientras existan grupos de personas dispuestos a aceptarlos e intercambiarlos por productos o servicios éstos continuarán.

En ese sentido, el Banco Central de Tailandia dictaminó que el *bitcoin* no es ninguna moneda y prohibió su uso en cualquier tipo de operación legal dentro del país asiático. La decisión implica que cualquier operación con *bitcoins* pasa a ser ilegal, incluida la compra y venta de bienes y servicios. Al mismo tiempo se prohíben los envíos de *bitcoins* fuera de Tailandia y la recepción desde el extranjero.⁶³

Otra acción del gobierno sería la de competir con los *criptoalgoritmos* de intercambio. Cabe preguntarse si en el futuro los gobiernos verán la posibilidad de que su moneda compita con los *altcoins*, de forma que generen una moneda respaldada y desmaterializada, utilizando protocolos equiparables a los que utilizan los *criptoalgoritmos* de intercambio para su validación y transferencia. Además, en ese escenario de competencia, el banco central podría autorizar y supervisar a las emisoras de dinero electrónico, reservando el término de dinero electrónico para las representaciones electrónicas del dinero emitido por el gobierno con las reglas de garantía y respaldo de la moneda convencional. Esto parece poco probable, sin embargo, el tiempo definirá la postura de los gobiernos frente a tales planteamientos.

Otra acción del gobierno puede ser la regulación: el interés de regular el *bitcoin* y en general los *criptoalgoritmos* de intercambio puede verse enfocado en prevenir la evasión fiscal, evitar acciones de lavado de dinero y crear certeza jurídica en las inversiones que realicen los particulares bajo ese esquema.

Es muy difícil controlar y, por tanto, regular los procesos de minería de los *criptoalgoritmos* puesto que su código de creación está distribuido en todo

⁶³ CNBC, “Bitcoin, prohibido en Tailandia”, <http://www.cnbc.com/id/100923551>, última fecha de consulta el 9 de noviembre de 2014.

el mundo sin poder identificar a una persona o institución determinada, sin embargo, la regulación puede hacerse en las operaciones de intercambio.

En ese orden de ideas, la regulación podría hacerse de la siguiente forma: 1) estableciendo reglas para los comercios y establecimientos que reciben como pago *bitcoins* o *altcoins*, para que declaren sus operaciones; 2) regular las casas de cambio que aceptan el intercambio de *bitcoins* por divisas convencionales, de modo que exista un registro de estas instituciones que deberán operar con reglas específicas y la obligación de declarar sus operaciones; 3) regulando las instituciones que prestan servicios de *e-wallet*, o depósito de criptoalgoritmos de intercambio; 4) regulando los servicios de inversión y especulación basados en *bitcoins* o *altcoins*; 5) regular los servicios de pago que fungen como intermediarios entre compradores y vendedores; 6) reformar las leyes hacendarias, de valores, de prevención de lavado de dinero, y 7) cualquier otro análogo que pueda ayudar a prevenir operaciones ilícitas y alinear las operaciones hacia la transparencia.

En Alemania se está hablando de este tema porque el *bitcoin* genera un comercio electrónico paralelo y los comerciantes generan ganancias que no declaran para efectos fiscales; ese simple hecho le interesa al gobierno. Por otra parte, en Bélgica el ministro de Finanzas, Koen Greens,⁶⁴ señaló que en aquel país el uso del *bitcoin* está limitado a un puñado de comercios y considera que el sistema financiero es fuerte como para detectar el intercambio de grandes cantidades; por lo tanto, el recelo sobre el lavado de dinero puede ser fácilmente abordado.⁶⁵

Los servicios desarrollados alrededor de dicha unidad no habían sido regulados hasta que en marzo de 2013 el FinCEN de EUA indicó que las entidades estadounidenses que generan “moneda virtual” como *bitcoin* (*mineros*) y venden las unidades por dinero real se convierten en empresas de servicios monetarios MSB,⁶⁶ por lo tanto, están obligadas a cumplir con los requisitos legales de transmisor de dinero. Ahora deberán identificar a las personas con las que realizan los intercambios.⁶⁷

⁶⁴ El bitcoin.org, “El ministro de Finanzas de Bélgica, sin nada que objetar a bitcoin”, www.elbitcoin.org/ministro-finanzas-belgica-bitcoin/, última fecha de consulta el 9 de noviembre de 2014.

⁶⁵ Fore Minute, “After Germany, Belgium is interested in Bitcoin, No startup bitcoin economy yet in the country”, www.forexminute.com/tag/minister-of-finance-koen-geens, última fecha de consulta el 9 de noviembre de 2014.

⁶⁶ FinCEN, Money Services Business, http://www.fincen.gov/financial_institutions/msb/definitions/msb.html, última fecha de consulta el 9 de febrero de 2015.

⁶⁷ FinCEN, Regulation to Persons Administering, Exchanging, or Using Virtual Currencies, March 18, 2013. http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html, fecha de última consulta el 9 de noviembre de 2014.

En México, el 17 de diciembre de 2013 el periódico *El Financiero* publicó que en el Distrito Federal se contaría con el primer cajero *bitcoin* disponible a partir de febrero de 2014, las personas que cuenten con *bitcoins* adquiridos del sitio *Coinbase* podrán ligar sus cuentas con su monedero *Pademobile*; así lo anunció el director general de *Pademobile*, una plataforma de pago que utiliza los números celulares de México como un monedero para recibir depósitos de dinero y realizar pagos en diversos establecimientos y sitios web.⁶⁸ Por su parte, CNN, en marzo de 2014 informó que en Tijuana Baja California, ya se instalaron los primeros cajeros *bitcoin*.⁶⁹

El 10 de marzo de 2014, el Banco de México, *Banxico*, se pronunció a través de un comunicado de prensa titulado “*Advertencia sobre el uso de activos como sucedáneos de los medios de pago en moneda de curso legal*”, en el cual expresó que debido al interés de los medios de comunicación y ciertos sectores del público en los activos virtuales, tales como *bitcoin*, *litecoin* y otros, el Banco de México considera importante difundir información al respecto y alertar de los riesgos que conlleva el uso de dichos activos virtuales. El Banco de México destaca que no son moneda de curso legal, no se les reconoce como medio de cambio oficial, ni como depósito de valor u otra forma de inversión. Advierte al público sobre los riesgos de adquirir estos activos y marca las diferencias en relación con la moneda de curso legal entre los que se destacan los siguientes: en México no son monedas de curso legal, debido a que *Banxico* no lo emite ni respalda, tampoco los regula ni supervisa. No tiene poder liberatorio de obligaciones de pago debido a que las personas y comercios no están obligados a aceptarlo. Muestra una gran volatilidad debido al carácter altamente especulativo, con alto riesgo de depreciación y de pérdida monetaria. No hay regulación ni garantía que asegure a los consumidores o comercios que puedan recuperar su dinero cuando invierten en ese tipo de activos, debido a que, en caso de pérdida, difícilmente procedería un recurso legal ya que no existe una organización que asuma las obligaciones por dichos activos. Las instituciones reguladas del sistema financiero mexicano no están autorizadas para usar, ni para efectuar operaciones con ellos. Indica que en otras jurisdicciones se ha señalado su uso en operaciones ilícitas incluyendo aquellas relacionadas con fraude y con el lavado de dinero. El comunicado aclara que quien acepte este tipo de activos

⁶⁸ Taringa, “México tendrá su primer cajero de bitcoins”, <http://www.taringa.net/posts/noticias/17419400/Mexico-tendra-su-primero-cajero-de-Bitcoins.html>, última fecha de consulta el 9 de noviembre de 2014.

⁶⁹ CNN México, “ABC para entender un cajero bitcoin”, <http://mexico.cnn.com/tecnologia/2014/03/24/abc-para-entender-un-cajero-de-bitcoin>, última fecha de consulta el 9 de noviembre de 2014.

en intercambio de un bien o servicio, o lo adquiera, asume los riesgos antes mencionados. Al concluir indica que el Banco de México, en coordinación con otras autoridades seguirá la evolución e implicaciones y que, de juzgarlo necesario, emitirá la regulación pertinente.⁷⁰

Si bien es cierto, el comunicado que emitió el Banco de México advirtió sobre los riesgos del *bitcoin*, y que quien lo adquiere lo hace bajo su propio riesgo, también es cierto que no prevé supuestos específicos, por lo que el uso de los criptoalgoritmos de intercambio, aun cuando todavía no está expresamente regulado, puede verse sometido a diferentes áreas del derecho, por una parte al área mercantil porque *bitcoin* se utiliza como una mercancía que se compra o vende; o porque se utiliza como forma alternativa de pago.

También puede tener repercusiones en el área civil al ser objeto de controversias en esta materia, como podría ser que en un divorcio se demande la disolución de la sociedad conyugal que incluye una cantidad de *bitcoins*, o el caso de una sucesión cuyos inventarios incluyan *bitcoins* como parte de la masa hereditaria, otro supuesto serían los *contratos de permuta*⁷¹ en los que se establezca como contraprestación la entrega de *bitcoins* como si se tratara de cualquier otro bien. En ese sentido, los bienes son muebles por su naturaleza o por disposición de la ley, el Código Civil Federal establece que son muebles por su naturaleza aquellos que pueden trasladarse de un lugar a otro, ya se muevan por sí mismos o por fuerza exterior; por otra parte, por determinación de la ley son muebles las obligaciones y los derechos o acciones que tienen por objeto cosas muebles o cantidades exigibles en virtud de acción personal, también establece como muebles los derechos de autor y, en general, todos los demás no considerados por la ley como inmuebles.⁷² Si bien es cierto los conceptos antes mencionados se vienen aplicando a bienes tangibles, también es cierto que por disposición de ley la clasificación de bienes muebles también se otorgó a intangibles como derechos y obligaciones, así como a los derechos de autor. Sin embargo, habrá que preguntarse si *bitcoin* cubre los supuestos previstos por la ley para considerarse bien mueble sin necesidad de que lo diga expresamente, o si requiere del reconocimiento legal expreso dadas sus particularidades que aun cuando puede moverse de

⁷⁰ Banco Nacional de México, Comunicado de Prensa, “Advertencia sobre el uso de activos virtuales como sucedáneos de los medios de pago en moneda de curso legal”, <http://www.banxico.org.mx/informacion-para-la-prensa/comunicados/miscelaneos/boletines/%7B5D9E200E-2316-A4B8-92A9-3A5F74938B87%7D.pdf>, última fecha de consulta el 9 de noviembre de 2014.

⁷¹ Código Civil Federal, Publicado en el *Diario Oficial de la Federación* el 24 de diciembre de 2013, p. 214.

⁷² *Ibidem*, pp. 82 y 83.

un lugar a otro por medios externos, esa movilización no es tangible, sino desmaterializada, visible únicamente por medios electrónicos; además no es una acción ni una obligación que pueda hacerse exigible a determinada persona, por lo que aun cuando a simple vista pareciera viable la equiparación a bien mueble habrá que prever la posibilidad que la ley incluya en esa clasificación los activos intangibles o bienes desmaterializados en un sentido más amplio, ya que conforme avanzan las Tecnologías de la Información, se generarán nuevas formas de bienes intangibles.

Otra área del derecho en la que puede repercutir el tema del *bitcoin* y las *altcoins* en general, es el área penal ya que *bitcoin* se ha convertido en objeto o instrumento de delito. Como objeto de delito, porque se han registrado robos de *bitcoins* vulnerando la seguridad de los medios de almacenamiento.⁷³ También se ha usado como instrumento de delito en actividades de narcotráfico, o bien, como medio comisivo en operaciones de lavado de dinero, evasión fiscal y fraude. Recordemos que en materia penal no aplica la analogía por lo que si las circunstancias de modo tiempo y lugar del ilícito no encuadran en la descripción antijurídica, no podrán sancionarse las conductas, aun cuando en el transcurso de la investigación pueda rastrearse la trayectoria de los bitcoins en el historial del monedero electrónico.

La posibilidad de regulación en países desarrollados como Estados Unidos, Alemania y Bélgica, o las restricciones de Tailandia y China podrían generar una migración de *mineros* hacia países considerados paraísos informáticos carentes de legislación sobre los criptoalgoritmos de intercambio; si bien es cierto que “en apariencia” no han representado una preocupación para los países de Latinoamérica, es importante empezar a realizar los planeamientos necesarios para evitar que se convierta en un problema.

V. CONCLUSIÓN

La unidad *bitcoin* no es moneda, tampoco título de crédito electrónico, es un bien intangible que se ha incorporado como alternativa de pago en las operaciones de comercio electrónico.

Aunque la unidad bitcoin pudiera equipararse a un bien mueble dada su movilidad y transferencia, es cuestionable que actualmente pudiera considerarse como bien mueble ya que el Código Civil Federal establece que los bienes son muebles por su naturaleza o por disposición de la ley. Son mue-

⁷³ *The Wall Street Journal*, “Mt. Gox head believes no more bitcoins will be found”, <http://online.wsj.com/articles/mt-gox-head-believes-no-more-bitcoin-will-be-found-1403850830>, última fecha de consulta el 9 de noviembre de 2014.

bles por su naturaleza aquellos que pueden trasladarse de un lugar a otro (concepto aplicable a cosas tangibles) y por disposición de la ley los derechos o acciones personales que tiene por objeto cosas muebles. Por lo tanto, si en el futuro se considerara reconocer a la información en general como un bien mueble sería necesario que la ley lo declare de esa forma y se incorpore a los bienes intangibles.

El *bitcoin* tiene tres funciones: 1) trueque de bienes o servicios; 2) de cambio monetario, y 3) de especulación.

Además del *bitcoin* existen otros criptoalgoritmos de intercambio llamados *altcoins*, entre los que se destacan *litecoin* y *PPcoin*; debido a su reciente aparición no habían sido regulados quedando fuera de supervisión y varias noticias informan que se han utilizado en la comisión de los ilícitos de fraude, narcotráfico, evasión fiscal y lavado de dinero.

El *bitcoin* también ha llamado la atención de las autoridades alrededor del mundo, como en el caso de Tailandia en donde se prohíbe su compra o venta; en China se permitió a los particulares adquirirlos y se impusieron restricciones de uso para las entidades financieras; en Alemania se está considerando para efectos del pago de impuestos; en Estados Unidos se establecieron reglas para las casas de cambio de *bitcoins* que ahora deben cubrir las obligaciones de instituciones de operaciones monetarias, identificando a las personas con las que realizan sus transacciones. El juez L. Mazzant dictó la primera sentencia relacionada con *bitcoin*, resolviendo que el *bitcoin* se considera una forma de moneda y por tanto reconoce la competencia de la *Security Exchange Commission* para intervenir en el caso de inversiones en *bitcoins*. La *Internal Revenue Service* informó que, para efectos de los impuestos federales en Estados Unidos, *bitcoin* deberá ser considerado como propiedad y no como moneda.

En México, a diferencia de España y Perú, no existe una ley de dinero electrónico ni se encuentra protegido el término *dinero electrónico*.

El Banco de México emitió un comunicado de prensa indicando que *bitcoin* no es moneda de curso legal, ni tiene carácter liberatorio de obligaciones de pago, las instituciones reguladas del sistema financiero no están autorizadas ni para usar ni para efectuar operaciones con ellos; quien adquiere *bitcoin* lo hace bajo su propio riesgo debido a su volatilidad y carencia de respaldo.

Aun con la advertencia del Banco de México, continúan las operaciones de intercambio de *bitcoins* a través de la aplicación *pademobile* y de los cajeros automáticos instalados en el Distrito Federal y Tijuana.

Por otra parte, la falta de regulación de los criptoalgoritmos de intercambio no impedirá su uso; inclusive la prohibición tampoco sería una li-

mitante ya que, debido a su característica intangible y su fácil transferencia por medios electrónicos, es difícil anticipar la realización de operaciones en *bitcoins*. Sin embargo, es posible conocer las operaciones realizadas en cierto monedero ya que los estados de cuenta son públicos, lo que pudiera facilitar las reglas para la supervisión y considerar las ganancias para efectos fiscales, así como para tener un registro de los comercios que aceptan esta unidad como forma de pago, establecer las reglas de compra de *bitcoins* para evitar el lavado de dinero y prevenir otras actividades ilícitas.

La posibilidad de que el *bitcoin* tenga mayor aceptación y aumenten las operaciones comerciales con esta unidad incrementa la posibilidad de litigios ante los tribunales, aun cuando el Banco de México advirtió que quien lo adquiere lo hace bajo su propio riesgo, estas unidades de *bitcoin* pueden verse sometidas a transacciones entre particulares, de manera que será un nuevo reto para los jueces aplicar una legislación que por el momento no contempla la existencia de los criptoalgoritmos de intercambio.

En México, jurídicamente, el *bitcoin* no está sujeto a una regulación, ya que ninguna ley prevé el supuesto de criptoalgoritmos de intercambio, ni la posibilidad de atribuirle un valor al mismo, por lo tanto, las operaciones que se realicen por parte de comercios establecidos o constituidos en México por el momento han quedado fuera de la fiscalización tributaria.

VI. GLOSARIO

Algoritmo. En informática el término algoritmo se utiliza para describir un método de resolución de un problema, que es adecuado para su implementación como programa de computadora.

Altcoin. En inglés *alt* se refiere a alternativa, unida a la palabra *coin*, se refiere a moneda alternativa, término que se ha utilizado para indicar a las variantes de los programas informáticos que crean algoritmos de intercambio. Entre las variantes más populares se encuentran PPcoin y Litecoinin.

Bit. En términos de sistemas un *bit* es la unidad más pequeña de información en una computadora.

Bitcoin. Con la primera letra en minúscula, es la palabra que se utiliza para referir al resultado del algoritmo que genera una secuencia alfanumérica de treinta y tres caracteres que constituye la unidad bitcoin.

Bitcoin. Con la primera letra mayúscula se utiliza para referir al programa de cómputo y red de minería Bitcoin que descifra la cadena de bloques que crean la unidad bitcoin.

BTC. Abreviatura con la que se identifica a la unidad bitcoin.

Cifrado de clave pública. Los sistemas criptográficos de clave pública utilizan un par de claves complementarias, mediante una de ellas se realiza el cifrado y la segunda se emplea para descifrar el mensaje. Una de las claves se mantiene secreta y la otra se hace pública. El hecho de que una de las claves se publique no compromete la seguridad de la comunicación, ya que es imposible determinar la clave privada a partir de la clave pública.

Coin. Su traducción al español es Moneda.

Criptografía. Técnicas de cifrado o codificación destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Criptograma de intercambio. Algoritmos encriptados que contienen información que puede ser leída en el programa que lo creó, utilizados para intercambiarse por productos o servicios.

Criptomonedas. Término empleado para referir a los algoritmos encriptados que se aceptan como medios de intercambio de bienes y servicios. Indebidamente se emplea la palabra moneda porque los algoritmos no cuentan con dicha característica.

Código abierto. Se utiliza para referir a los programas de cómputo sobre los que se hace el código fuente, permitiéndose el desarrollo y distribución libremente.

Deep web / Internet profunda. Es como se conoce al contenido que no forma parte de Internet superficial, esto se debe a que los buscadores no son capaces de indexar todas las páginas contenidas en Internet por alguna de las siguientes razones: a) porque las páginas o sitios web están protegidos con contraseña; b) porque existen documentos en formatos no indexables. Se estima que la *deep web* es 500 veces mayor que la Internet superficial.

Economía Bitcoin. Así se denomina al conjunto de operaciones realizadas dentro de la red y protocolo Bitcoin, incluye la minería y las múltiples transferencias que se realizan de dichas unidades.

EDE. Abreviatura para referir a las entidades de dinero electrónico.

Encriptación. Proceso de transformación de un texto plano a una forma que no pueda ser leída por alguien que no tenga los mecanismos utilizados para llevar a cabo la encriptación. El texto transformado recibe el nombre de texto cifrado. Existe una gran cantidad de algoritmos para llevar a cabo este proceso.

FinCEN. Financial Crimes Enforcement Network. Departamento encargado de la lucha contra el lavado de dinero en Estados Unidos.

MSB Money Services Business. En los negocios de servicios monetarios se incluye a cualquier persona que realice de forma regular o no las siguientes actividades: distribuya o intercambie moneda, emita cheques de viajero y

giros postales o aquellos que tengan valor almacenado, transmisor de dinero y cambio de cheques.

Minería. Es la función que desarrolla el programa de cómputo Bitcoin, cuyo propósito es descifrar el problema matemático que genera un bitcoin; para que pueda llevarse a cabo la minería es necesario que las máquinas mineras (ordenadores que cuentan con el programa Bitcoin) siempre estén conectadas a la red para validar la información de la cadena de bloques del bitcoin que se genere, además de validar la cadena de bloques de otras transacciones.

Monedero Bitcoin. Cuenta en la que se almacenan las unidades bitcoin, desde la cual se pueden hacer pagos y transferencias.

Llave Pública y Llave privada. Son un par de llaves digitales asociadas a una persona o entidad, generadas por métodos criptográficos. La llave pública es usada para cifrar la información. Mientras que la llave privada se usa para descifrar la información.

Peer to Peer / P2P. La red punto a punto es una red de computadoras que permiten el intercambio directo de información entre los ordenadores conectados. Estas redes no requieren de clientes o servidores fijos, sino que forman una serie de nodos que funcionan como iguales, actuando simultáneamente como clientes y servidores respecto del resto de los nodos de la red.

Ponzi. El esquema *ponzi* es una operación fraudulenta en el que las ganancias que se entregan a los primeros inversionistas son obtenidas del dinero generado por ellos mismos, o del dinero de nuevos inversores que caen en el engaño con la esperanza de obtener una tasa de retorno extremadamente alta.

Protocolo. Lenguaje que permite comunicar computadoras (nodos) entre sí.

Red Bitcoin. Al conjunto de ordenadores en los que está instalado el programa de cómputo Bitcoin, que se conectan e intercambian información entre sí con la tecnología P2P.

SEC. Security Enforcement Commission, regulador bursátil en Estados Unidos, encargado de proteger a los inversores, mantener mercados justos, ordenados y eficientes, así como facilitar la formación de capital.

Software. Programa de cómputo diseñado para permitir a la computadora realizar determinadas tareas y funciones.

Software Bitcoin. Programa de cómputo de código abierto mediante el cual se realiza la minería de bitcoins, así como la validación de operaciones y transferencias de dicha unidad.

Software Minero. Programa de cómputo con la función de descifrar un problema matemático, de cuya secuencia resulta la creación de un *bitcoin*.

Tor. Es la abreviatura del proyecto llamado *The Onion Router* / ruteador cebolla. Se trata de un *software* que permite a los mensajes viajar desde su origen al destino, a través de la red de ruteadores especiales cuyo objetivo es que el tráfico de mensajes intercambiados entre los usuarios de dicha red no revele su identidad (dirección IP), conservando la secrecía de la información, emplea la criptografía en capas, metafóricamente, como las capas de una cebolla.

VII. BIBLIOGRAFÍA

- AREITO, J. Javier, *Seguridad de la información. Redes informáticas y sistemas de información*, Paraninfo, 2008, https://books.google.com.mx/books?id=_z2GcBD3deYC&dq=red++tor&hl=es&source=gbs_navlinks_s, última fecha de consulta el 7 de enero de 2015.
- BANCO CENTRAL DE LA RESERVA DE PERÚ, “Ley núm. 29985: Ley del Dinero Electrónico”, consultada en el sitio <http://www.bcrp.gob.pe/transparencia/normas-legales/ley-del-dinero-electronico.html>, última fecha de consulta el 9 de noviembre de 2014.
- BANCO NACIONAL DE MÉXICO, Comunicado de Prensa, “Advertencia sobre el uso de activos virtuales como sucedáneos de los medios de pago en moneda de curso legal”, nota del 10 de marzo de 2014, obtenido de la página <http://www.banxico.org.mx/informacion-para-la-prensa/comunicados/miscelaneos/boletines/%7B5D9E200E-2316-A4B8-92A9-3A5F74938B87%7D.pdf>, última fecha de consulta el 9 de noviembre de 2014.
- BBC NEWS TECHNOLOGY, “Bitcoin value drops after FBI shuts Silk Road drugs site”, nota del 3 de octubre de 2013, consultable en el sitio www.bbc.co.uk/news/technology-24381847, última fecha de consulta el 9 de noviembre de 2014.
- BITCOIN, “Preguntas más frecuentes”, www.bitcoin.org/es/faq, última fecha de consulta el 9 de noviembre de 2014.
- BITCOIN WIKI, “Comercio”, <https://es.bitcoin.it/wiki/Comercio>, última fecha de consulta el 9 de noviembre de 2014.
- BITCOIN WIKI, “Trade”, <https://en.bitcoin.it/wiki/Trade>, fecha de última consulta el 9 de noviembre de 2014.
- BITCOIN WIKI, “Units”, <https://en.bitcoin.it/wiki/Units>, última fecha de consulta el 9 de noviembre de 2014.

BITCOIN WIKI, FAQ, “How long will it take to generate all the coins?”, https://en.bitcoin.it/wiki/FAQ#How_long_will_it_take_to_generate_all_the_coins.3F, última fecha de consulta el 9 de noviembre de 2014.

BITCOIN WIKI, FAQ, “But if no more coins are generated, what happens when Bitcoins are lost? Won't that be a problem?”, https://en.bitcoin.it/wiki/FAQ#If_no_more_coins_are_going_to_be_generated.2C_will_more_blocks_be_created.3F, última fecha de consulta el 9 de noviembre de 2014.

BITCOIN WIKI, FAQ, “What is mining?”, <https://en.bitcoin.it/wiki/FAQ#Mining>, última fecha de consulta el 9 de noviembre de 2014.

BITCOIN WIKI, FAQ, “Where does the value of Bitcoin stem from? What backs up Bitcoin?”, https://en.bitcoin.it/wiki/FAQ#Where_does_the_value_of_Bitcoin_stem_from.3F_What_backs_up_Bitcoin.3, fecha de última consulta el 9 de noviembre de 2014.

BITCOIN, “Bitcoin for Businesses”, www.bitcoin.org/en/bitcoin-for-businesses, última fecha de consulta el 9 de noviembre de 2014.

BITCOIN, <http://bitcoin.org/es/>, última fecha de consulta el 9 de noviembre de 2014.

BITCOIN, Comunidad web patrocinada por Bitcoin Foundation, consultada en <http://bitcoin.org/es/>, fecha de última visita el 9 de noviembre de 2014.

BLOCKCHAIN INFO, herramientas para estudiar y analizar las transacciones de bitcoins, consultado en <http://blockchain.info/es>, fecha de última visita el 9 de noviembre de 2014.

BOLETÍN OFICIAL DEL ESTADO, “Ley 21/2011, de 26 de julio, de dinero electrónico”, Madrid, publicado el 27 de julio de 2011, consultada en <https://www.boe.es/boe/dias/2011/07/27/pdfs/BOE-A-2011-12909.pdf>.

BOLETÍN OFICIAL DEL ESTADO, “Real Decreto 778/2012, del 4 de mayo, de régimen jurídico de las entidades de dinero electrónico”, Madrid, publicado el 5 de mayo de 2012, consultada en <https://www.boe.es/boe/dias/2012/05/05/pdfs/BOE-A-2012-5993.pdf>.

CASADEMO, Jordi (coord.), “Redes de comunicaciones: de la telefonía móvil a Internet”, Universitat Politècnica de Catalunya, S.L., 2010, <https://books.google.com.mx/books?id=2D9FO9nX-XsC&pg=PA151&dq=internet+profunda&hl=es-419&sa=X&ei=ljnZVK3MFLi0yQTqzIC4BA&ved=0CCEQ6AEwAQ#v=onepage&q=internet%20profunda&f=false>, última fecha de consulta el 9 de febrero de 2015.

CNBC, “Bitcoin, prohibido en Tailandia”, nota del 30 de julio de 2013, consultada en <http://www.cnn.com/id/100923551>.

CNN ESPAÑOL, “Arrestan a dos operadores de Bitcoin por lavado de dinero”, nota del 27 de enero de 2014, consultado en <http://cnnespanol.cnn.com/2014/01/27/arrestan-a-dos-operadores-de-bitcoin-por-lavado-de-dinero/>, última fecha de consulta 9 de noviembre de 2014.

CNN MÉXICO, “ABC para entender un cajero bitcoin”, nota del 24 de marzo de 2014, obtenida de <http://mexico.cnn.com/tecnologia/2014/03/24/abc-para-entender-un-cajero-de-bitcoin>, última fecha de consulta 9 de noviembre de 2014.

CNN MONEY, “Bitcoin prices top \$1000”, nota del 27 de noviembre de 2013, obtenida en <http://money.cnn.com/2013/11/27/investing/bitcoin-1000/>, fecha de última consulta el 9 de noviembre de 2014.

CNN TECNOLOGÍA, “China instala su primer cajero bitcoin pese a la presión de su gobierno”, nota del 16 de abril de 2014, nota consultada en <http://mexico.cnn.com/tecnologia/2014/04/16/china-instala-su-primer-cajero-de-bitcoin-pese-a-la-presion-de-su-gobierno>, última fecha de consulta el 9 de noviembre de 2014.

CNN WORLD, “How FBI caught Ross Ulbricht, alleged creator or criminal marketplace Silk Road”, <http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html>, última fecha de consulta el 9 de noviembre de 2014.

CÓDIGO CIVIL FEDERAL, publicado en el *Diario Oficial de la Federación* el 24 de diciembre de 2013.

COINMILL, “El convertidor de divisas”, http://es.coinmill.com/BTC_USD.html, última fecha de consulta el 9 de noviembre de 2014.

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

CRIPATOMONEDAS, “Bitcoin y las nuevas monedas virtuales que están cambiando al mundo”, nota del 27 de agosto de 2013, www.criptomonedas.org/altcoins-monedas-alternativas/#more-160, última fecha de consulta el 9 de noviembre de 2014.

DURÁN DÍAZ, Oscar Jorge, *Los títulos de crédito electrónicos, su desmaterialización*, México, Porrúa.

EL BITCOIN.ORG, “Bitcoin es dinero, dice un juez de Texas”, nota del 9 de agosto de 2013, obtenida de <http://elbitcoin.org/bitcoin-es-dinero-dice-juez-texas/>, última fecha de consulta el 9 de noviembre de 2014.

EL BITCOIN.ORG, “El ministro de Finanzas de Bélgica, sin nada que objetar a bitcoin”, nota del 12 de septiembre de 2013, obtenida de www.elbitcoin.org.

org/ministro-finanzas-belgica-bitcoin/, última fecha de consulta el 9 de noviembre de 2014.

El Economista, “El gobierno alemán reconoce oficialmente la moneda virtual bitcoin”, nota del 19 de agosto de 2013, obtenida de www.economista.mobi/mercados-cotizaciones/noticias/5078793/08/13/El-Gobierno-aleman-reconoce-oficialmente-la-moneda-virtual-bitcoin.html, última fecha de consulta el 9 de noviembre de 2014.

El Economista, “Se desploma la cotización del bitcoin por culpa de China”, <http://eleconomista.com.mx/mercados-estadisticas/2013/12/18/china-impacta-bitcoin>, fecha de última consulta el 9 de noviembre de 2014.

El País, Tecnología, “El Banco Central chino ordena cerrar todas las cuentas con bitcoins”, nota del 28 de marzo de 2014, obtenida de http://tecnologia.elpais.com/tecnologia/2014/03/28/actualidad/1396002045_716448.html, fecha de última consulta 9 de noviembre de 2014.

El Universal, “Desaparece de web plataforma de operaciones de Bitcoin”, nota del martes 25 de febrero de 2014, obtenida de <http://www.eluniversal.com.mx/finanzas-cartera/2014/bitcoin-plataforma-desaparece-990349.html>, fecha de última consulta el 9 de noviembre de 2014.

En qué invertir, “Bitcoin en tiempo real”, <http://www.enqueinvertir.com/bitcoin-en-tiempo-real.php>, fecha de última consulta el 15 de agosto de 2013.

ESPAÑA BOQUERA, María Carmen, Servicios avanzados de telecomunicación, España, Ediciones Díaz Santos, 2003, <https://books.google.com.mx/books?id=yTSoYCiXYAAC&pg=PA61&dq=cifrado+de+clave+p%C3%ABlica&hl=es-419&sa=X&ei=y7PZVIvmJbPdsATfy4CQBw&ved=0CCKQ6AEwAQ#v=onepage&q=cifrado%20de%20clave%20p%C3%ABlica&f=false>, última fecha de consulta el 9 de febrero de 2015.

FACUA, Banca, “EEUU Interviene dos cuentas a la mayor operadora de moneda virtual Bitcoin, la japonesa Mt. Gox”, nota del 18 de mayo de 2013, obtenida de <https://www.facua.org/es/noticia.php?Id=7617>, última fecha de consulta el 9 de noviembre de 2014.

FINCEN, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies”, emitido el 18 de marzo de 2013, consultado en http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html, última fecha de consulta el 9 de noviembre de 2014.

FORBES, “Federal Judge Rules Bitcoin is Real Money”, nota del 7 de agosto de 2013, consultada en www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/, última fecha de consulta el 9 de noviembre de 2014.

FORE MINUTE, “After Germany, Belgium is interested in Bitcoin, No startup bitcoin economy yet in the country”, nota obtenida de www.forexminute.com/tag/minister-of-finance-koen-geens, última fecha de consulta el 9 de noviembre de 2014.

INTERNAL REVENUE SERVICE, “Virtual currency Guidance: Virtual currency es treated as Property for U.S. Federal Tax Purposes; General Rules for property Transactions Apply”, nota del 25 de marzo de 2014, obtenida de <http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance>.

“NOTICE 2014-21”. Notice regarding taxes that apply to transaction using virtual currencies, consultada en <http://www.irs.gov/pub/irs-drop/n-14-21.pdf>, última fecha de consulta 9 de noviembre de 2014.

International New York Times, “Bitcoin gets a cautious nod from China’s Central Bank”, nota del 22 de noviembre de 2013, obtenida de la página <http://sinosphere.blogs.nytimes.com/2013/11/22/bitcoin-gets-a-cautious-nod-from-chinas-central-bank/>, última fecha de consulta el 9 de noviembre de 2014.

MISHKIN, Frederic S., *Moneda, banca y mercados financieros*, 10a. ed., México, Pearson, 2014.

MIT Technology Review, “Bitcoin no es la única criptomoneda que existe”, nota del 16 de abril de 2013, obtenida de la página www.technologyreview.es/read_article.aspx?id=42902, última fecha de consulta el 9 de noviembre de 2014.

MOCHON, Francisco, *Principios de economía*, 4a. ed., México, McGraw Hill, 2010.

PAGLIERY, José, “Bitcoin and the future of money”, Triumph Books LLC, 2014, <https://books.google.com.mx/books?id=r-ouBAAAQBAJ&printsec=frontcover&dq=bitcoin&hl=es-419&sa=X&ei=zzjZVPLkLIq2yQTMuYCwDg&ved=0CDMQ6AEwAQ#v=onepage&q=bitcoin&f=false>, fecha de última consulta el 9 de febrero de 2015.

Precio del Bitcoin, <http://preciodelbitcoin.com/>, fecha de última consulta el 15 de agosto de 2013.

RANKIA, Comunidad financiera, “La crisis de Chipre incrementa la fuga de dinero hacia bitcoin, los bancos centrales empiezan a preocuparse”, nota del 19 de marzo de 2013, consultable en el sitio www.rankia.com/foros/bancos-cajas/temas/1723351-tesis-chipre-incrementa-fuga-dinero-hacia-bitcoin-bancos-centrales-empiezan-preocuparse, última fecha de consulta el 9 de noviembre de 2014.

TARINGA, “México tendrá su primer cajero de bitcoins”, <http://www.taringa.net/posts/noticias/17419400/Mexico-tendra-su-primer-cajero-de-Bitcoins.html>, última fecha de consulta el 9 de noviembre de 2014.

TECHCRUNCH, “Germany Recognizes Bitcoin as “Private Money”, sales tax coming soon”, nota del 19 de agosto de 2013, consultada en www.techcrunch.com/2013/08/19/germany-recognizes-bitcoin-as-private-money-sales-tax-coming-soon/?utm_medium=referral&utm_source=pulsenews, última fecha de consulta el 9 de noviembre de 2014.

The Wall Street Journal, “Mt. Gox head believes no more bitcoins will be found”, <http://online.wsj.com/articles/mt-gox-head-believes-no-more-bitcoin-will-be-found-1403850830>, última fecha de consulta el 9 de noviembre de 2014.

The Washington Post, “Mt. Gox collapse spurs calls to regulate Bitcoin”, http://www.washingtonpost.com/business/technology/mt-gox-collapse-spurs-calls-to-regulate-bitcoin/2014/02/28/df44f5c6-a0b7-11e3-a050-dc3322a94fa7_story.html, última fecha de consulta el 7 de enero de 2015.

U.S. Securities and Exchange Commission, “Ponzi Schemes”, <http://www.sec.gov/answers/ponzi.htm>, última fecha de consulta el 7 de enero de 2015.

USA Today, “IRS: Answer to tax questions about Bitcoin”, nota del 25 de marzo de 2014, <http://www.usatoday.com/story/money/business/2014/03/25/irs-answers-on-bitcoin-tax-guidance/6874925/>, última fecha de consulta el 9 de noviembre de 2014.

WAI-SING LOO, Alfred, *Peer to Peer Computing: Building Supercomputers with Web Technologies*, Springer, 2007, https://books.google.com.mx/books?id=6ftYxEokK7AC&pg=PA7&dq=peer+to+peer+definition&hl=es-419&sa=X&ei=XU_ZVM6xNIOVyATk6oLgCA&ved=0CBsQ6AEwAA#v=onepage&q=peer%20to%20peer%20definition&f=false, última fecha de consulta el 9 de febrero de 2015.

LA TRANSPOSICIÓN DEL CONVENIO DE BUDAPEST SOBRE LA CIBERDELINCUENCIA EN LA LEGISLACIÓN FRANCESA EN LA PRÁCTICA

Cynthia SOLÍS*
Vincent LEMOINE**

SUMARIO: I. *Introducción.* II. *La Convención sobre cibercriminalidad.* III. *El problema de la aplicación práctica de la Convención de Budapest en Francia.* IV. *El problema de la modificación de los datos.* V. *El problema del lugar de almacenamiento de los datos.* VI. *Bibliografía.*

I. INTRODUCCIÓN

El uso de las nuevas tecnologías de información y la comunicación en los asuntos judiciales, han llevado a los jueces y en especial a los investigadores a cuestionar las modalidades de aplicación del Código de Procedimientos Penales. Sin lugar a dudas, existe un gran incremento en los actos ilícitos resultantes del uso de estos vastos sistemas de comunicación, que ahora simbolizan el estandarte de una sociedad inmersa en la red.

De hecho, las nuevas tecnologías pueden permitir o facilitar la comisión de un delito, como el uso de un teléfono para informar a los delincuentes en un acto específico o permitir la comisión del delito directamente usando una computadora para realizar una intrusión en un sistema remoto.

En los últimos años, estos sistemas han cambiado profundamente la naturaleza de las relaciones sociales y las relaciones entre los individuos, en particular en cuanto a sus orientaciones. Este tipo de herramientas no

* Investigadora adscrita al Centro de Estudios e Investigación en derecho inmaterial de las universidades Panthéon Sorbonne y Paris Sud; y maestra en derecho de la innovación técnica.

** Perito en forense informática, profesor investigador de la Universidad Paris Sud y doctor en derecho.

sólo se utilizan para fines privados (correo electrónico, *chat*, búsquedas en la web), sino también para el uso profesional, y en general en todos los actos de la vida (medios de pago, transferencias electrónicas, transporte). De hecho, ¿Existen herramientas utilizadas hoy en día, que no incluyan algún tipo de tecnología? ¿Quién no ha hecho uso del comercio electrónico para hacer una compra?

Con el desarrollo del acceso a través de la banda ancha a partir de 2001, las nuevas tecnologías se han convertido en una parte esencial de la economía (compras, gestión, publicidad, etcétera). Ellos están en constante crecimiento, y el número de personas que los utilizan no ha dejado de crecer.

En quince años, hemos pasado de simple “*pager*” para recibir un mensaje de texto, a Internet a través del teléfono móvil para recibir la radio de banda ancha, la televisión, y el progreso no se detiene allí. Una encuesta realizada por el sitio web de Silicon¹ en septiembre de 2010, puso de relieve que Francia tenía 21.4 millones de suscriptores de Internet y 62.6 millones de teléfonos móviles.

En paralelo, los actos delictivos relacionados con las nuevas tecnologías o cometidos por ellos, también están en aumento. No es raro ver cada semana en las noticias un caso de pedofilia, intrusión, fraude o abuso a través de sitios web.

Desde 1978, el legislador tuvo la intención de prevenir esta situación a través de la Ley de Protección de Datos,² mejor conocida como la Ley de Informática y Libertades, con respecto a la creación de bases de datos. Esta legislación es más conocida bajo el acrónimo de la comisión encargada de supervisar este tipo de delitos, es decir, la “CNIL”,³ Comisión Nacional de Informática y Libertades, la cual es fruto del proyecto que nació muerto llamado Safari.

En 1988, la Ley Godfrain⁴ creó nuevos tipos penales, orientados a criminalizar ciertas conductas relacionadas con el procesamiento automatizado de datos. Las nuevas tecnologías, en general, se pueden utilizar directamente para atacar, permitir o facilitar la comisión de los mismos.

¹ *Les abonnements Internet se tassent en France*, por Christophe Lagane en <http://www.silicon.fr/les-abonnements-internet-se-tassent-en-france-43682.html>, consultado el 20 de octubre de 2014.

² <http://www.cil.cnrs.fr/CIL/spip.php?rubrique281>, consultado el 20 de octubre de 2014.

³ *Atteinte aux systèmes d'informations*, por Alain Bensoussan, en www.alain-bensoussan.com, consultado el 20 de octubre de 2014.

⁴ *Panorama de la cybercriminalité en 2010*, en el sitio de CLUSIF, <http://www.clusif.asso.fr>, consultado el 20 de octubre de 2014.

La definición más apropiada para describir la nueva tecnología es “cualquier medio para comunicar, procesar, almacenar datos, así como la gestión de los sistemas informáticos o incluso mecánicos”. El alcance de estas nuevas tecnologías es relativamente grande.

El legislador francés, a través del artículo L.32 de la Ley de Telecomunicaciones Electrónicas, define con mucha precisión la terminología, tomando en cuenta diversos aspectos técnicos y jurídicos, citados a continuación:

1. *Comunicaciones electrónicas*. Se entiende por comunicaciones electrónicas a las emisiones, transmisiones o recepciones de signos, señales, escritos, imágenes o sonidos, enviados por vía electromagnética.
2. *Red de comunicaciones electrónicas*. Se entiende por red de comunicación electrónica, toda instalación o conjunto de instalaciones para el transporte o la difusión y, en su caso, otros medios de garantizar la entrega de las comunicaciones electrónicas, incluidos los de conmutación y enrutamiento. Se consideran como redes de comunicación electrónica: las redes satelitales, redes terrestres, así como los sistemas que utilizan dichas redes, siempre y cuando se utilicen para el suministro de redes de comunicaciones electrónicas y asegurar la difusión o las utilizadas para la distribución de servicios la comunicación audiovisual.

Pero, ¿qué es en sí un dato informático?

A nivel de la Unión Europea. En términos del artículo primero de la Convención Europea en materia de la lucha contra la cibercriminalidad del 21 de noviembre de 2001, mejor conocida como la Convención de Budapest,⁵ esta expresión “Datos informáticos”, se define como: “Toda representación de hechos, de información o de conceptos en formato idóneo para ser tratada a través de medios informáticos, incluido el propio sistema de tratamiento”.

Una de sus principales características es la de ser intangible, es decir, palpables como cualquier otro documento en papel. Únicamente el soporte material que contiene los datos, por ejemplo, un disco duro, un CD-Rom, una memoria flash o incluso una terminal móvil, pueden ser percibidas físicamente; es por ello que la propia explicación de motivos de la Convención

⁵ http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF, consultado el 19 de octubre de 2014.

proporciona una serie de definiciones importantes, utilizadas a lo largo de su redacción.

Los datos informáticos pueden constituir un recurso para un sistema o una red informática. Por sistema informático es importante comprender todo dispositivo que, por sí mismo o en su conjunto, aseguran a través de la ejecución de un programa, un tratamiento automatizado de datos. Es entonces el conjunto de elementos que participan en la administración, almacenamiento, tratamiento, transporte y difusión de la información en el seno de una organización, en conjunto con el propio medio informático como una computadora, un servidor o cualquier sistema de explotación donde se encuentre presente.

A nivel Francia. El legislador reagrupa las diferentes definiciones jurídicas en un código único, el citado anteriormente de la Ley de Comunicaciones Electrónicas, en su artículo L.32, en el que se dispone lo siguiente:

1. *Comunicaciones electrónicas.* Se entiende por comunicaciones electrónicas a las emisiones, transmisiones o recepciones de signos, señales, imágenes o sonidos por vía electromagnética.

2. *Redes de comunicaciones electrónicas.* Se entiende por red de comunicaciones electrónicas, toda instalación o conjunto de instalaciones de transporte o difusión, y en su caso, otros medios que aseguren el encaminado de comunicaciones electrónicas, en particular aquellos de conmutación y enrutamiento.

Se consideran como redes de comunicaciones electrónicas: las redes satelitales, redes terrestres, sistemas que utilicen la red eléctrica para garantizar el encaminado de las comunicaciones electrónicas y aquellas que aseguren la difusión o distribución de servicios de comunicación audiovisual.

3. *Red abierta al público.* Se entiende por red abierta al público toda red de comunicaciones electrónicas establecidas o utilizadas para proveer al público de servicios de comunicación electrónicas o servicios de comunicación al público por vía electrónica.

Hoy en día es muy difícil que alguien no cuente con un teléfono celular o acceso a Internet, sobre todo en países desarrollados como los europeos, en México, incluso miles de personas cuentan con este tipo de dispositivos tales como: computadoras portátiles, tabletas, GPS (*Global Positioning System*) y teléfonos inteligentes, ya sean propios o de sus lugares de trabajo; todos ellos conectados a Internet.

La industria poco a poco ha automatizado procesos sustituyendo el trabajo humano por el de las máquinas; en la obra intitulada *Las TIC en los desarrollos habitacionales de México*, editada por INFOTEC, se demuestra la

importancia que tienen las nuevas tecnologías en la vida diaria de nuestros connacionales.

Desgraciadamente, si el legislador francés hubiese previsto en aquella época reprimir ciertas acciones a través de las citadas leyes, no hubiera necesitado modificar el Código de Procedimientos Penales para crear nuevas disposiciones para facilitar la ejecución de las investigaciones judiciales. Desde hace diez años, al fin ha puesto en marcha la creación de numerosas reformas en la materia.

En paralelo, en un ámbito puramente civil la firma electrónica en Francia no fue reconocida como válida hasta el año 2000 por la Ley núm. 2000-230 del 13 de marzo de 2000 la cual incluyó la adaptación del derecho de la prueba a través de tecnologías de la información relativa a la firma electrónica y su decreto 2001-272⁶ del 30 de marzo de 2001. Esta ley se dio con motivo de la transposición de la directiva comunitaria del 13 de diciembre de 1999,⁷ estableciendo un esquema comunitario para las firmas electrónicas.

En materia de procedimiento penal especial en materia de nuevas tecnologías, fija las reglas aplicables a los diferentes actores de la justicia: magistrados, policías, gendarmes, incluyendo aquellos actos y procedimientos que permitiesen realizar requisiciones de informáticas, intervención de equipos y sistemas de cómputo e interceptar correspondencia electrónica.

II. LA CONVENCION SOBRE CIBERCRIMINALIDAD

En realidad no fue hasta 2001, que las primeras disposiciones a nivel de la Unión Europea vieron la luz a través de la Convención del 23 de noviembre de 2001 de Budapest. De hecho era imperativo que el derecho penal pudiera seguir el ritmo de las evoluciones tecnológicas, las cuales, además de ofrecer beneficios inigualables, también abren un universo de posibilidades para los delincuentes.

En la exposición de motivos de dicha Convención, el Consejo Europeo hace énfasis en ello.

La recomendación núm. R(89) 9 del Consejo de Europa,⁸ ciertamente ha permitido acercarse a las concepciones nacionales que tocan al uso

⁶ <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796>, consultado el 10 de octubre de 2014.

⁷ http://www.dnielectronico.es/marco_legal/directiva_1999_93_CE.html, consultado el 20 de octubre de 2014.

⁸ Véase el índice cronológico y referencias en <http://www.mjusticia.gob.es/cs/Satellite/1292344070605?blobheader=application%2Fpdf&blobheadername1=Co>

abusivo de las computadoras. Únicamente un instrumento jurídico internacional puede tener la eficacia necesaria contra estos nuevos fenómenos, un instrumento que permitiese la cooperación internacional y, además de ello, tratar cuestiones de derecho sustantivo y adjetivo. Uno de los grandes avances es incluir la posibilidad y legitimidad jurídica de combatir el crimen a través de los mismos medios informáticos, es decir, que el remedio y la enfermedad se encuentren al mismo nivel de competencia.

Sin pretender colocar a la convención en un pedestal ni tomarla como la panacea en el tema, es cierto que es la piedra angular de los avances en materia de cibercriminalidad, no solamente para la Unión Europea sino para los demás Estados firmantes, dentro de los cuales, según las predicciones, se encontrará nuestro país.

La Convención ha ido perfeccionando sus preceptos, por ejemplo, con el protocolo adicional relativo a la incriminación de actos de racismo y xenofobia a través de sistemas informáticos del 28 de enero de 2003 en Estrasburgo, así como la de Lanzarote del 25 de octubre de 2007 en materia de explotación y abuso sexual infantil.

Ahora bien, aterrizando en la realidad actual, no basta con las buenas intenciones, ya que muchos de los Estados firmantes han tardado demasiado en ratificar, además de que existe una gran paradoja, ya que la Convención de Schengen⁹ de 1990, puesta en marcha en 1995, instauró la apertura de las fronteras entre los Estados firmantes, así como la libre circulación de personas y bienes.

El Tratado de Lisboa, del 13 de diciembre de 2007, vino a completar las reglas jurídicas de la zona Schengen, reforzando la noción de “espacio de libertad, seguridad y justicia”, por lo cual, ya se encontraba sobreentendida la obligación de cooperación policial y judicial entre los Estados para garantizar estas premisas.

Luego entonces, no es fácil explicar cómo es que países como España y Bélgica siguen negándose a cooperar en la materia sin ratificar la Convención de Budapest, lo cual complica en la práctica la persecución de delitos informáticos desde Francia, haciendo obligatoria la exigencia de una requisición internacional para acceder a cooperar.

ntent-Disposition&blobheadername2=EstudioDoctrinal&blobheadervalue1=attachment%3B+filename%3D1991_1599.pdf&blobheadervalue2=1288777592356, consultado el 20 de octubre de 2014.

⁹ http://europa.eu/legislation_summaries/glossary/schengen_agreement_es.htm, consultado el 20 de octubre de 2014.

Lo anterior implica un proceso bastante complejo y pesado que desde luego se convierte en una incoherencia con la manifestación de buenas intenciones de cooperación en la materia.

El principal mensaje de la décimo segunda edición del Congreso de las Naciones Unidas de 2010 para la prevención del crimen y la justicia penal, fue justamente la puesta en marcha de instrumentos jurídicos eficaces, en particular la Convención de Budapest, como representación del mejor medio para ayudar a los países para ayudar a luchar contra la cibercriminalidad en todo el mundo.

Canadá, por ejemplo, recibió con singular interés el mensaje redundando en la creación de sus dos proyectos de Ley, el C.51¹⁰ y el C.52,¹¹ en materia de investigaciones informáticas y prevención del ciberdelito.

Por lo tanto, una de las principales inquietudes de los servicios policíacos a nivel Unión Europea, que se ven obligados a reflexionar acerca de las dificultades en cuanto a las investigaciones, la uniformidad de las legislaciones, y principalmente por parte del Colegio Europeo de Policía (CEPOL). Este organismo se ha dedicado a organizar regularmente seminarios a lo largo de todos los países de la Unión Europea destinado a la capacitación de policías y gendarmes, el último de ellos llevado a cabo en Atenas en 2010.

Entrando a detalle, la Convención de Budapest permite definir conceptos unificados a fin de que los Estados puedan utilizar la misma terminología al momento de adaptar su legislación local, así como tomar las medidas pertinentes para su puesta en marcha, misión que no es nada sencilla al interior de cada país.

Los temas que se abordan son extensos e incluyen desde los lógicamente aplicables como intrusiones ilícitas a sistemas, falsificaciones y fraudes informáticos, hasta aquellos relativos a la protección de la propiedad intelectual, pornografía infantil y abuso sexual de menores.

Otra de las innovaciones que presenta es la de permitir las nociones de tentativa y complicidad en las infracciones evocadas en sus artículos 2o. al 8o., así como la responsabilidad de las empresas, recordando que puede ser penal, civil o administrativa, según el caso.

Ahora bien, para algunos países como Francia, este tipo de disposiciones no representan ninguna novedad ya que se encontraban incluidas desde 1978 y 1988 respectivamente; sin embargo, es imposible negar que a nivel

¹⁰ <http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/40/3/c51-f.pdf>, consultado el 20 de octubre de 2014.

¹¹ <http://www.ledevoir.com/politique/canada/332857/projet-de-loi-c-52-l-intimite-numericque-des-canadiens-pourrait-etre-menacee>, consultado el 15 de octubre de 2014.

de procedimientos penales, sí representa un gran avance, sobre todo en la parte que toca a la obtención de evidencias informáticas.

Por ejemplo, el artículo 16 de la Convención de Budapest¹² impone a las partes, la adopción de medidas legislativas que permitan a sus autoridades competentes el ordenar la conservación rápida de evidencias informáticas específicas, tales como datos de tráfico o almacenamiento en un sistema informático y, sobre todo, cuando son volátiles, es decir, susceptibles de pérdida o modificación.

Concretamente en los hechos, los servicios de investigación se vuelven lentos y se contraponen con lo establecido si tomamos en cuenta que existe la obligación de recurrir mediante una demanda por escrito a la Sección Central de Cooperación Operativa de la Policía, mediante la cual se pueda garantizar que los datos queden “congelados” durante 90 días y cuando así se requiera otros 90 días más; tiempo en el que el magistrado revisará si procede la emisión de una carta rogatoria internacional al país que aloje la información.

III. EL PROBLEMA DE LA APLICACIÓN PRÁCTICA DE LA CONVENCIÓN DE BUDAPEST EN FRANCIA

La mayor parte de intercambios realizados cotidianamente por los internautas, en términos de correos electrónicos, mensajería instantánea, redes sociales y almacenamiento de información en la nube, pasan por servidores o prestadores de servicios radicados en Estados Unidos, por ejemplo: Hotmail, Yahoo, Gmail, Twitter, Facebook, etcétera. Aun cuando este país es firmante de la convención desde 2006, la realidad es que tanto investigadores como magistrados parecen desconocer a detalle las disposiciones relativas al acceso de dichos datos.

El artículo 57-1 del Código Francés de Procedimientos Penales, inspirado en el artículo 19 de la Convención de Budapest, permite realizar intervenciones a distancia, si bien es cierto que los redactores de la Convención comprendían los diferentes servicios judiciales como la policía y la gendarmería francesas, el artículo 57-1, únicamente permite estas intervenciones en el territorio francés.

Sin embargo, en términos del artículo 31 de la Convención, sobrevive la posibilidad de requerir directamente al Estado miembro su cooperación a través de una demanda de cooperación judicial formulada por las autori-

¹² *Ibidem*, p. 4.

dades francesas. Por lo que compete a Estados Unidos, lo más frecuente en materia de investigaciones de este tipo es adherirse al decreto 2001-1122,¹³ el cual establece la cooperación entre Estados Unidos y Francia, y conviene mucho más a los intereses de la investigación.

Si bien es cierto que el proceso es largo y pesado, es más sencillo que seguir el procedimiento establecido en la Convención, lo cual retrasaría mucho más la investigación sin contar el hecho de la desaparición de las pruebas.

IV. EL PROBLEMA DE LA MODIFICACIÓN DE LOS DATOS

El primer problema al que se enfrentan los investigadores especialistas, como el coautor de la obra, Vincent Lemoine, implica utilizar la computadora de la persona investigada y con ello modificar los eventuales datos alojados en ella, ya sea agregando o modificando los datos existentes al momento de actualizarlos.

Este problema radica en la propia arquitectura de los sistemas y del propio tiempo. Es un hecho que al momento de que un investigador o el mismo usuario de una computadora interactúa con ella, desde luego que será modificada la información, lo anterior como resultado de la propia actualización de los sistemas, de los antivirus, descarga de correos electrónicos, etcétera.

El conjunto de los procesos anteriormente descritos se cargan en la memoria viva de la computadora, mejor conocida como memoria RAM (*Random Access Memory*), así como en los archivos temporales que se guardan en los diferentes espacios del disco duro. Particularmente la información que se encuentra en archivos de paginación del sistema operativo (*pagefile.sys*) o el archivo de hibernación (*hiberfile.sys*).

Estos archivos, cuyo tamaño es bastante significativo, también almacenan todos los archivos abiertos y las operaciones realizadas a través del sistema operativo, por lo tanto, todas las modificaciones serán efectuadas cuando el sistema esté en funcionamiento y serán multiplicadas si el investigador las utiliza para expatriar los datos.

Por ejemplo, desde que una computadora se conecta a Internet, la información es transmitida permanentemente a través de paquetes basados en el protocolo TCP/IP, lo que permite una conexión a distancia entre dos

¹³ <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000393833>, consultado el 10 de octubre de 2014.

sistemas que se encuentran o pueden encontrarse completamente lejanos uno de otro.

Del otro lado, nos enfrentamos al hecho de que la operación tiene que ser realizada desde el sistema inicial, es decir, el domicilio de la persona donde tuvo lugar la investigación, lo que necesita un mínimo de conocimientos técnicos por parte del grupo de investigadores y, en la práctica, muy pocos oficiales cuentan con dichos conocimientos; tratándose de investigaciones realizadas en empresas el asunto puede volverse aún más complejo; por ejemplo, un Centro de Datos que normalmente se encuentran en el extranjero.

Antes de proceder a la investigación es indispensable identificar el lugar preciso donde reside la información a analizar, realizando un inventario completo de la configuración del *hardware* y del *software*, pero sobre todo el nivel de seguridad, el cual seguramente deberá de ser bastante alto; y si a eso le agregamos el hecho de que muchas empresas cuentan con funcionalidades de “puerta trasera” mediante las que pueden respaldar y restaurar su información, es necesario saber si están implementadas para que el investigador las desactive e impida la alteración de la evidencia, lo cual la mayoría de los investigadores desconoce y pasa por alto. El artículo 57-1 del Código Francés de Procedimientos Penales prescribe a los agentes de la policía judicial a realizar una investigación directamente a partir de un sistema en funcionamiento, luego entonces, se contrapone directamente con el principio fundamental de la criminalística que impide alterar los indicios.

De hecho, el principio dictado por Edmon Locard,¹⁴ se aplica perfectamente desde el momento que una computadora se encuentra funcionando sobre una red informática y es por ello, que esta disposición, si bien es legal, es raramente utilizada por los investigadores.

Estos últimos prefieren realizar sus peritajes *a posteriori*, por técnico especialista en la tecnología de la que se trate, lo cual no se encuentra previsto en las disposiciones del Código de Procedimientos Penales.

Hay que recordar que el espíritu del proceso no se limita a la investigación policial, pero es un hecho que marca la diferencia en cuanto al seguimiento del mismo. Ya sea que se trate de la fase de instrucción preparatoria o del juicio o en ambos casos, un peritaje puede ser exigido ya sea por el juez o por el ministerio público, o incluso por las partes, para aclarar algún punto preciso.

¹⁴ Referencia al principio de Intercambio de Locard, <http://inza.wordpress.com/2006/03/05/edmond-locard/>, consultado el 20 de octubre de 2014.

En este caso, cuando el perito sea llamado a presentar su informe, se enfrentará al problema de evidenciar todas aquellas manipulaciones efectuadas en el sistema a analizar, por lo tanto, se constatará que la evidencia ha sido alterada y debe precisarlo correctamente al momento de presentar verbalmente las conclusiones de su informe.

En efecto, uno de los principios esenciales en materia criminalística, tal como se evoca en la obra de Harlan Carvey, llamada *Herramientas de análisis forense en Windows*, es indispensable describir cada acción y mencionar fecha y hora de las mismas, así como las personas que han sido autorizadas para tal efecto en el expediente, lo que conocemos en México, como la cadena de custodia. En el caso de descargas de información remota, únicamente se habla de los datos visibles y no aquellos ocultos o borrados, la recuperación de éstos puede llevarse a cabo, pero el costo es exponencial.

Para poder realizar este tipo de análisis, se requiere de programas especializados llamados “e-discovery”. Algunas compañías, como *Guidance Software*, trabajan arduamente en ingresar al mercado sobre todo de los investigadores y posicionar este tipo de herramientas.

El principio de la alteración de un indicio fue retomado en el capítulo IV relativo a las barreras u obstáculos en cuanto a la presentación de pruebas en justicia, en el artículo 434-4¹⁵ del Código Penal francés, el cual dispone:

Se castigará con tres años de prisión y 45 000 euros de multa, cualquier acto que obstaculice o manipule la manifestación de la verdad, como lo es:

1o. Modificar el lugar de los hechos de un crimen o delito, a través de la alteración, la falsificación, el borrado de rastros o indicios, ya sea aportando, moviendo o suprimiendo objetos,

2o. Destruir, sustraer, ocultar o alterar un documento público o privado o un objeto susceptible de facilitar el descubrimiento de un crimen o un delito, la búsqueda de pruebas o la condena de los culpables.

En caso de que los hechos previstos en el presente artículo sean cometidos por una persona que ya sea por sus funciones, es llamada a coadyuvar a manifestar la verdad de los hechos, la pena aumentará a cinco años de prisión y 75 000 euros de multa.¹⁶

¹⁵ <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418608&cidTexte=LEGITEXT000006070719>, consultado el 26 de octubre de 2014.

¹⁶ *Idem*.

Estamos en presencia de un agravante en razón de la cualidad del sujeto, en este caso, el investigador, un técnico o un perito en la materia, ya que todas estas personas son llamadas a coadyuvar en la impartición de justicia a través de la manifestación de la verdad. Es conveniente recordar que los datos informáticos son extremadamente volátiles y que todo acceso a distancia tendrá el impacto que ya se ha mencionado.

La única solución legalmente admisible podría ser el proceder en dos tiempos, es decir: en un primer tiempo realizar una copia bit a bit del disco duro de la computadora y después colocar el disco duro original sellado. Una copia bit a bit es una copia idéntica de un disco. De hecho, contrariamente a ciertas pruebas biológicas de que no es posible la clonación, un soporte digital puede ser clonado en numerosas ocasiones sin límite.

En una segunda etapa es necesario colocar la copia bit a bit del disco duro clon, en la computadora y en ese momento comenzar las investigaciones, de esta manera, la prueba no será alterada y por lo tanto y las pruebas obtenidas a distancia serán copiadas en el clon y no en el original.

Si esta operación, que es jurídica y técnicamente admisible, puesto que la copia de datos informáticos se encuentra prevista por el artículo 56 del Código de Procedimientos Penales, la realidad es que no puede llevarse a cabo de forma tan sencilla dada la creciente capacidad de los nuevos discos duros, ya que esto implica un tiempo de copia bastante importante a través de sistemas para los cuales se debe contar aproximadamente un minuto por cada gigabyte.

Por otra parte, esta copia debe realizarse en presencia de la persona que será investigada, esto impacta desde luego el proceso ya que este periodo puede ser superior a las 24 horas en caso de grandes volúmenes de datos o de demasiados soportes a copiar. La copia no puede interrumpirse y esto reduce los tiempos de retención legal del objeto a analizar.

De hecho, el estándar actual en la capacidad del disco duro en un equipo es de aproximadamente 320 gigabytes lo cual significa que en el mejor de los casos necesitaremos al menos tres horas. Podrían obtenerse mejores tiempos de copia, sin embargo, tendría que llevarse a cabo a través de una copia física cuyos costos son mucho más altos.

La solución mejor adaptada a los investigadores para no perder tiempos procesales importantes es una técnica comúnmente utilizada en el caso de las investigaciones llevadas a cabo en las empresas, las cuales permiten realizar simultáneamente los peritajes tanto en los documentos como en los sistemas informáticos.

Otra opción, en ausencia de un tercero auxiliando la investigación, sería realizar una búsqueda utilizando un CD en vivo que protege el disco

duro de la computadora contra cualquier cambio. Por lo general, es una distribución, a menudo GNU / Linux en CD-ROM que se carga en la memoria RAM y permite analizar los datos de la computadora de una persona sospechosa, sin hacer cambios, y también recuperar datos remotos para ser copiados en un medio extraíble.

V. EL PROBLEMA DEL LUGAR DE ALMACENAMIENTO DE LOS DATOS

El segundo problema deviene directamente de la naturaleza misma del funcionamiento de las redes y de la noción de territorialidad de los datos. De hecho, numerosos prestadores de servicios de Internet como Google, MSN o Yahoo, proponen aplicaciones de mensajería en la nube o lo que se conoce comúnmente como *Cloud Computing* por su nombre en inglés.

Las direcciones creadas por un internauta poseen una extensión con un nombre de dominio .fr; lo cual presume que al ser un servicio que se ofrece en el territorio francés, es la legislación francesa la que debería aplicarse, desgraciadamente no es así. En efecto, es el derecho del Estado donde los datos residen, el que se aplica, aun cuando sea un servicio en lengua francesa, con un nombre de dominio de la región y destinado principalmente a usuarios de la misma.¹⁷

Esta circunstancia complica enormemente el trabajo del investigador, desde que simplemente consulta una bandeja de entrada de correo electrónico, ya que nunca sabe en qué país realmente está alojada la información. La sola indicación de la dirección IP del país donde se encuentra almacenada la información, es ya una advertencia a la vista, antes de bajar o abrir un correo en los servicios que así lo permiten, como Yahoo o Hotmail. Por el contrario, para Gmail, no existe ningún indicador de la implantación del servidor de descarga.

De hecho, para los Webmails Yahoo y Hotmail, una vez que el investigador desee acceder a la información contenida en la mensajería de un tercero en su presencia, en el marco de una medida precautoria, él obtendrá información relativa a la dirección IP del servidor, pero únicamente del archivo adjunto.

Esta información no está disponible en simple lectura del correo, por lo tanto, es necesario recurrir a una investigación del tipo “rastreo de ruta”

¹⁷ Para conocer las reglas aplicables a los derechos sobre un nombre de dominio .fr, http://www.afnic.fr/medias/documents/Presentation_AFNIC_atelier_18_octobre_2011.pdf, consultado el 15 de octubre de 2014.

para intentar localizar el sitio de implantación geográfica del servidor en cuestión y verificar los eventuales criterios de competencia en cuanto a la territorialidad y, sobre todo, la aplicación de la Convención de Budapest.

Por lo tanto, podríamos pensar que esta cuestión regulada en la propia convención, en su artículo 32, relativo al acceso transfronterizo de datos almacenados, ya sea con consentimiento o cuando son accesibles al público, dispone:

Que una parte, puede sin la autorización de la otra:

- a) Acceder a los datos accesibles al público (fuente pública), sin importar la localización geográfica de los datos; o
- b) Acceder o recibir a través de un sistema informático, situado en su territorio, datos informáticos almacenados o situados en algún otro Estado, si la parte obtiene el consentimiento legal y voluntario de la persona legalmente autorizada a divulgar estos datos por ese medio.

Sin embargo, en el primer caso se puede dar el valor de una declaración por parte del experto; en el segundo caso, ya que el hecho de que el acceso a los datos de un correo electrónico no provienen de una fuente abierta, sino de un entorno privado, por lo tanto requiere, como se estipula en el artículo 32 de la Convención, “el consentimiento legal y voluntario de la persona”.

En el caso de una investigación preliminar, es necesario recabar el consentimiento expreso y por escrito en la forma prevista por la ley. La única manera de acceder a los datos sin este consentimiento es obtener una autorización expedida por el juez. Sin embargo, esta disposición sólo es aplicable a los delitos punibles con más de cinco años de prisión.¹⁸

La redacción de este acuerdo tiene su base desde hace más de cien años en el artículo 127 del Decreto Orgánico del 20 de mayo 1903 por el que se establecen normas relativas a la organización y el servicio de la policía. Aunque este decreto fue derogado por la Ley núm. 2009-971,¹⁹ del 3 de agosto de 2009, su formulación es una práctica o un uso y costumbre, ya que no aparece textualmente en ninguno de los artículos del Código de Procedimientos Penales. Está formulado de la siguiente manera: “Sabiendo que me puedo oponer a la perquisición, consiento expresamente que se lleve

¹⁸ *Ibidem*, p. 4.

¹⁹ Referencia retomada de forma no textual en la Ley 2009-971, <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020954146&dateTexte=&categorieLien=id>, consultado el 20 de octubre de 2014.

a cabo, así como la incautación que considere de utilidad para la investigación”.

Anteriormente, este consentimiento únicamente aplicaba a bienes inmobiliarios, ya que su campo de aplicación se precisaba en el mismo artículo de la siguiente manera: “Ninguna investigación, visita o decomiso, podrá hacerse sin el consentimiento libre, expreso y en conocimiento de causa, de la persona en cuestión”.

Esto se ha adaptado en función de las circunstancias para ser admisible en una gran cantidad de situaciones. Se trata simplemente de poner en evidencia que la persona implicada puede oponerse a dichas operaciones, únicamente precisando la causa de la investigación. Podrá ser reformulada siempre y cuando no se viole su esencia.

A este efecto, según las reglas procesales, generalmente debe precisarse el domicilio, en el cuerpo de un proceso verbal. Cada descubrimiento de evidencia debe ser objeto de una mención precisa acerca de sus características y del lugar donde fue encontrado; esto implica que en el caso de un peritaje informático debe mencionarse, entre otras cosas, la dirección de correo electrónico de la que se trate, el espacio o lugar donde se encuentra alojado, precisar la dirección IP ligada a los elementos descargables para verificar la ley aplicable.

Los datos no tangibles no pueden ser percibidos físicamente, pero al ser extraídos del servidor, gracias a la interface del correo electrónico en el que se encuentran en vista de ser copiados en un soporte extraíble, el cual será objeto de una copia de seguridad cifrada, podremos convertir al soporte en un bien tangible.

La manifestación del consentimiento expreso, la identidad de la persona propietaria de la dirección de correo, la dirección incriminada, así como el del servidor, deberán adjuntarse.

Ahora bien, la segunda dificultad es la limitación de los poderes coercitivos del oficial de policía, quien, en el caso de una indagación realizada en un domicilio, se encuentra facultado para llevarla a cabo sin necesidad de consentimiento expreso; no es así en el de la búsqueda de evidencia a distancia, la cual opera desde un Estado firmante de la convención Budapest, es obligatorio obtener el consentimiento expreso de la persona titular del sistema informático, únicamente los datos que residan en Francia se encuentran exonerados.

La particularidad de este proceso es que el investigador realiza la perquisición y luego solicita la autorización para acceder a los datos, luego

entonces, esta disposición se encuentra en clara contradicción del derecho francés²⁰ en sí mismo.

En todo caso, la redacción de un proceso verbal de investigación debe ser lo más precisa posible, sobre todo en materia de datos informáticos, para constatar que el conjunto de obligaciones legales impuestas por el artículo 57-1 del Código de Procedimientos Penales han sido respetadas y, desde luego, los acuerdos internacionales.

VI. BIBLIOGRAFÍA

- ARPAGIAN, Nicolas, *La cybersécurité*, París, PUF, 2010.
- BENSOUSSAN, Alain, *Atteinte aux systèmes d'informations*, recuperado de www.alain-bensoissan.com, 20 de octubre de 2014.
- FILIOL, E. y RICHARD, F., *Cybercriminalité*, París, Dunod, 2006.
- GIROT, Jean-Luc, *Le harcèlement numérique*, París, Dalloz, 2005.
- LAGANE, Christophe, *Les abonnements Internet se tassent en France*, recuperado de www.silicon.fr, 20 de octubre de 2014.
- LIRA, Óscar, *Cibercriminalidad, fundamentos de investigación en México*, México, Inacipe, 2010.
- Panorama de la cibercriminalité XE "cybercriminalité"*, en 2010, recuperado de CLUSIF, <http://www.clusif.asso.fr>, 20 de octubre de 2014.

²⁰ En el marco de los fundamentos y principios del derecho francés, entre ellos, el de presunción de inocencia en un proceso penal, <http://www.justice.gouv.fr/organisation-de-la-justice-10031/les-fondements-et-principes-10032/le-droit-a-un-proces-equitable-10027.html>, consultado el 20 de octubre de 2014.

DE LOS AUTORES

MOISÉS CARVAJAL

Es licenciado en pedagogía por la Universidad Veracruzana y estudiante de la maestría en educación virtual de la misma casa de estudios.

MIGUEL CASILLAS

Es doctor en sociología por la Escuela de Altos Estudios en Ciencias Sociales de París; maestro en ciencias con especialidad en educación en el Departamento de Investigaciones Educativas (CINVESTAV/IPV) y licenciado en sociología por la UNAM. Actualmente es investigador de tiempo completo en la Universidad Veracruzana y miembro del Sistema Nacional de Investigadores (SNI) I.

VANESSA DÍAZ

Es candidata a doctor por la Universidad de Tasmania (Australia), es maestra en derecho por la Universidad Anáhuac del Sur, y licenciada en derecho en la Universidad del Pedregal. Realizó un diplomado en derecho comparado de la Información por la Universidad de Oxford (Inglaterra). Es académica del Instituto de Investigaciones Jurídicas de la UNAM desde el año 2000 a la fecha. Se especializa en temas de flujo de información biométrica, nuevas tecnologías y derecho de la información.

GONZALO FARRERA BRAVO

Catedrático e investigador del Instituto de Investigaciones Jurídicas de la UNAM y de la UAM Iztapalapa. En la Escuela Libre de Derecho es catedrático de la Clínica de Teoría Política e investigador honorario. Profesor del posgrado en derecho y del posgrado en pedagogía de la UNAM. Profesor de la especialidad en Administración de justicia del Consejo de la Judicatura, Poder Judicial del Estado de Michoacán, UMSNH.

MYRNA ELIA GARCÍA BARRERA

Doctora en derecho egresada de la Facultad de Derecho y Criminología de la UANL. Investigadora en el Centro de Investigación de Tecnología

Jurídica y Criminológica de la Facultad de Derecho y Criminología de la UANL. Catedrática de la propia Facultad de Derecho y Criminología de la UANL y de la Universidad de Monterrey. Directora de Equidad de Género y Protección a Grupos Vulnerables del Poder Judicial del Estado de Nuevo León (SNI) I.

ALEJANDRO DE LA GARZA REYES

Es licenciado en derecho por la Facultad de Derecho de la Barra Nacional de Abogados, maestro en defensa y promoción de los derechos humanos por la Universidad Autónoma de la Ciudad de México. Ha sido profesor visitante en el Instituto Max Planck de Derecho Internacional y Derecho Comparado en Heidelberg, Alemania. Actualmente es profesor en la Universidad del Valle de México y titular del Despacho jurídico De la Garza y Abogados.

JONATHAN G. GARZÓN GALVÁN

Es licenciado en derecho con mención honorífica por la Barra Nacional de Abogados, licenciado en ciencia política y administración pública con mención honorífica por la UNAM. Maestro en derecho de la empresa con mención honorífica emitido por la Universidad Panamericana y maestro en comercio electrónico por el Instituto Tecnológico de Estudios Superiores de Monterrey. Actualmente, es gerente de Proyectos y Productos de Tecnología en Cecoban S.A. de C.V., y profesor de posgrado en el ITAM, La Salle, Universidad Panamericana y el ITESM. Fungió como miembro del Consejo Directivo y vicepresidente jurídico de la Asociación Mexicana de Internet (AMIPCI) durante los periodos 2011 y 2012.

CRISTINA GÓMEZ RODRÍGUEZ

Licenciada en derecho por la Universidad Autónoma de Querétaro, especialista en derecho del trabajo y maestra en administración pública estatal y municipal por la misma universidad. Actual candidata a maestra en derecho de las tecnologías de la información y comunicación del posgrado de excelencia de Conacyt en el Fondo de Documentación e Información para la Industria, INFOTEC.

FLORIAN HUBER

Maestro en derecho internacional de los derechos humanos por la Universidad de Essex, Inglaterra. Actualmente es profesor visitante e investigador de la Escuela de Política y Relaciones Internacionales del Instituto de De-

rechos Humanos y Derecho Internacional Humanitario, respectivamente, de la Escuela de Derecho de la Universidad Sergio de Arboleda, Colombia. Entre 2011 y 2013 fue visitante profesional, abogado consultor y abogado asesor en el área legal de la Secretaría de la Corte Interamericana de Derechos Humanos.

FEDERICO CÉSAR LEFRANC WEEGAN

Doctor Cum Laude en derecho por la Universidad Autónoma de Barcelona. Obtuvo el título de máster en derecho penal, constitución y derechos, y el diploma de “Estudios avanzados en derecho penal” por la Universidad Autónoma de Barcelona. Es licenciado en derecho por la Universidad Autónoma Metropolitana (UAM). Es profesor investigador de tiempo completo adscrito a INFOTEC.

DANIELA MARTÍNEZ SALINAS

Estudiante de la licenciatura en ciencia política de la UAM Iztapalapa. Asistente de investigador del Laboratorio de Política Pública y Derechos Humanos de la UAM Iztapalapa.

VINCENT LEMOINE

Doctor en ciencias criminales por la Escuela Doctoral de la Universidad París Sud. Maestro en seguridad de los sistemas de información por la Universidad Tecnológica de Troyes. Maestro en derecho de nuevas tecnologías de la sociedad de la información por la Universidad París Ouest. Perito en criminalística del Tribunal de Apelación de Versalles. Especialista en seguridad de sistemas de información y cibercriminalidad. Ingeniero en seguridad en sistemas de información forense en materia de ciberdefensa y encargado de la gestión, tratamiento y calificación de incidentes de seguridad.

CARLOS ORTIZ LÓPEZ

Abogado de la Universidad Católica de Colombia, especialista en derecho de autor, propiedad industrial y nuevas tecnologías de la Universidad Externado de Colombia. Actual docente e investigador en propiedad intelectual con la Facultad de Derecho de la Universidad Cooperativa de Colombia.

FREDY ALEXANDER PRADA V.

Abogado egresado de la Universidad Nacional de Colombia, investigador y escritor en temas de derecho, en la actualidad se desempeña como consultor independiente.

ALBERTO RAMÍREZ-MARTINELL

Es doctor en tecnología educativa por la Universidad de Lancaster, Inglaterra; maestro en ciencias de la computación y los medios de comunicación por la Universidad de Ciencias Aplicadas de Furtwangen, Alemania; ingeniero en Computación por la Universidad Nacional Autónoma de México y licenciado en humanidades por la Universidad del Claustro de Sor Juana. Actualmente se desempeña como investigador de tiempo completo en la Universidad Veracruzana y miembro del Sistema Nacional de Investigadores (SNI) I.

CYNTHIA SOLÍS

Maestra en derecho de la innovación técnica por las universidades Paris I Panthéon Sorbonne y Paris Sud. Doctoranda en el área de cibercriminalidad en la Universidad Paris Sud. Ha cursado estudios de gobernanza de Internet en la South School of Internet Governance (Brasil) y en Diplo Foundation (Ginebra), experta certificada en materia de protección de datos personales por NYCE. Conferenciante y socia presidente de la firma Lex Informática Abogados.

EVELYN TÉLLEZ CARVAJAL

Licenciada en relaciones internacionales y en derecho por la Universidad Nacional Autónoma de México, maestra en derecho por la División de estudios de Posgrado de Derecho de la misma casa de estudios. Formó parte del Grupo de Investigación Otto Hahn del Instituto Max Planck de Derecho Internacional y Derecho Comparado en Heidelberg, Alemania. Actualmente es profesora investigadora de tiempo completo adscrita a INFOTEC.

KARLA VALENCIA

Maestra en desarrollo regional por el Colegio de Veracruz, técnico académico en el Instituto de Investigaciones en Educación de la Universidad Veracruzana.

CAROLINA VELANDIA H.

Abogada egresada de la Universidad Nacional de Colombia, magister en negociaciones económicas internacionales de la Universidad Andina Simón Bolívar, especialista en derecho minero y petrolero de la Universidad Externado de Colombia, en la actualidad se desempeña como abogada en el sector petrolero.

Revista de DERECHO PRIVADO



Universidad Nacional Autónoma de México
Instituto de Investigaciones Jurídicas

SÍGUENOS EN



<http://biblio.juridicas.unam.mx/revista/DerechoPrivado/>

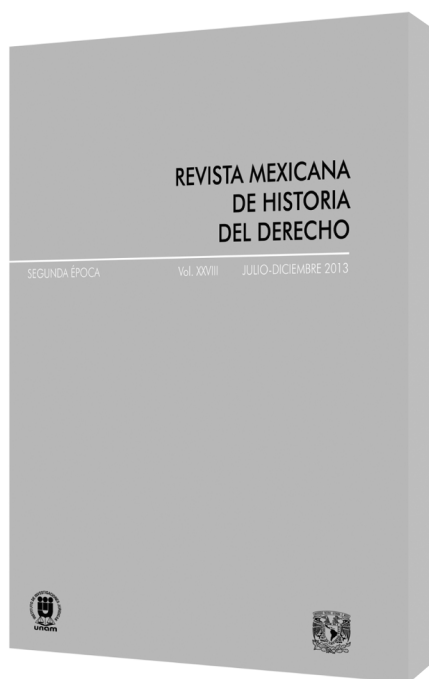


www.juridicas.unam.mx / www.biblio.juridicas.unam.mx

Instituto de Investigaciones Jurídicas

Coordinación de Distribución, Promoción y Fomento Editorial
Circuito Maestro Mario de la Cueva s/n, Ciudad de la Investigación
en Humanidades, Ciudad Universitaria, 04510 México,
D. F., teléfonos: 5622-7474 ext. 1704 Fax 5665-2193
Correo: distiij@unam.mx

● ● ● REVISTA MEXICANA DE HISTORIA DEL DERECHO



Universidad Nacional Autónoma de México
Instituto de Investigaciones Jurídicas

SÍGUENOS EN



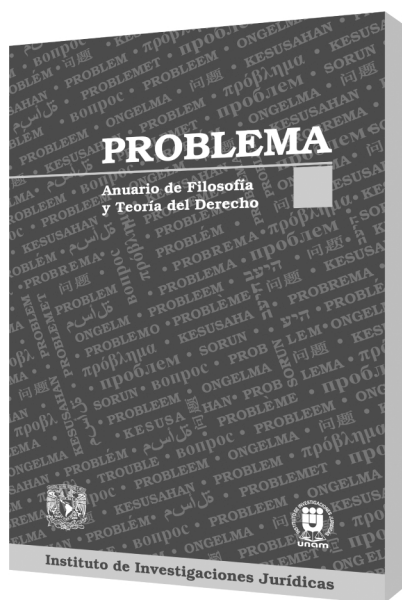
<http://biblio.juridicas.unam.mx/revista/HistoriaDerecho/>



www.juridicas.unam.mx/www.biblio.juridicas.unam.mx
Instituto de Investigaciones Jurídicas
Coordinación de Distribución, Promoción y Fomento Editorial
Circuito Maestro Mario de la Cueva s/n, Ciudad de la Investigación
en Humanidades, Ciudad Universitaria, 04510 México,
D. F., teléfonos: 5622-7474 ext. 1704 Fax 56 65 21 93
Correo: distij@unam.mx.

••• PROBLEMA

Anuario de Filosofía y Teoría del Derecho



Universidad Nacional Autónoma de México
Instituto de Investigaciones Jurídicas

SÍGUENOS EN

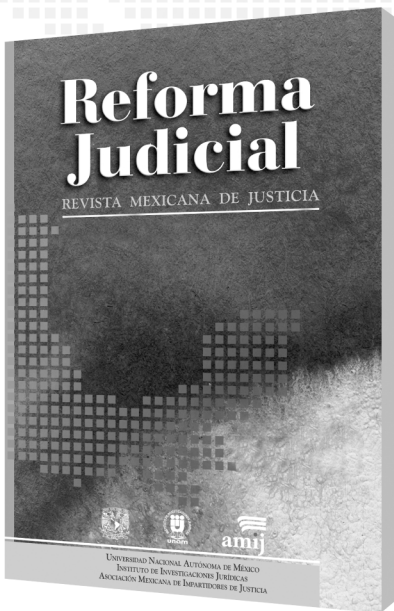


<http://biblio.juridicas.unam.mx/revista/FilosofiaDerecho/>



www.juridicas.unam.mx / www.biblio.juridicas.unam.mx
Instituto de Investigaciones Jurídicas
Coordinación de Distribución, Promoción y Fomento Editorial
Circuito Maestro Mario de la Cueva s/n, Ciudad de la Investigación
en Humanidades, Ciudad Universitaria, 04510 México,
D. F., teléfonos: 5622-7474 ext. 1704 Fax 5665-2193
Correo: distiij@unam.mx

Reforma Judicial



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE INVESTIGACIONES JURÍDICAS
ASOCIACIÓN MEXICANA DE IMPARTIDORES DE JUSTICIA

SÍGUENOS EN



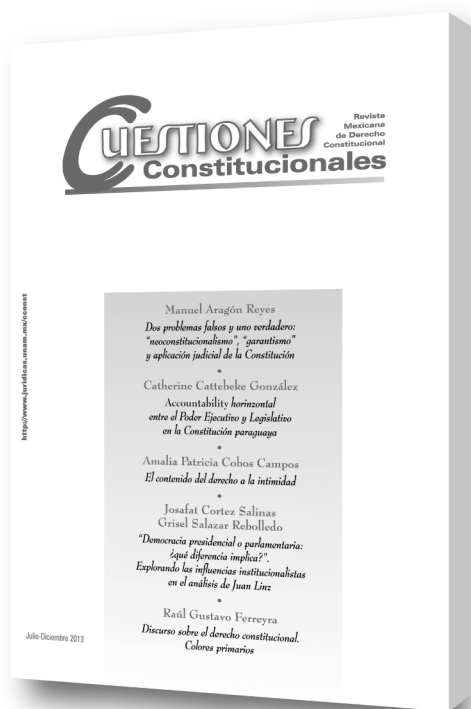
<http://biblio.juridicas.unam.mx/revista/ReformaJudicial/>



www.juridicas.unam.mx/www.biblio.juridicas.unam.mx
Instituto de Investigaciones Jurídicas
Coordinación de Distribución, Promoción y Fomento Editorial
Circuito Maestro Mario de la Cueva s/n, Ciudad de la Investigación
en Humanidades, Ciudad Universitaria, 04510 México,
D. F., teléfonos: 5622-7474 ext. 1704 Fax 5665-2193
Correo: distiij@unam.mx

CUESTIONES Constitucionales

Revista
Mexicana
de Derecho
Constitucional



Universidad Nacional Autónoma de México
Instituto de Investigaciones Jurídicas

SIGUENOS EN



<http://biblio.juridicas.unam.mx/revista/CuestionesConstitucionales/>



www.juridicas.unam.mx/www.biblio.juridicas.unam.mx
Instituto de Investigaciones Jurídicas
Coordinación de Distribución, Promoción y Fomento Editorial
Circuito Maestro Mario de la Cueva s/n, Ciudad de la Investigación
en Humanidades, Ciudad Universitaria, 04510 México,
D. F., teléfonos: 5622-7474 ext. 1704 Fax 5665-2193
Correo: distij@unam.mx

Derecho y TIC. Vertientes actuales, editado por el Instituto de Investigaciones Jurídicas de la UNAM, se terminó de imprimir el 6 de enero de 2016 en los talleres de Impresión Comunicación Gráfica, S. A. de C. V., Manuel Ávila Camacho 689, col. Sta. Ma. Atzahuacán, delegación Iztapalapa, 09500 México, D. F. Se utilizó tipo *Baskerville* en 9, 10 y 11 puntos. En esta edición se empleó papel cultural 70 x 95 de 50 kilos para los interiores y cartulina couché de 250 gramos para los forros; consta de 500 ejemplares (impresión *offset*).