Solicitud de Audiencia
Impacto de Internet en la Defensa y el Ejercicio de los Derechos Humanos
153 Periodo Ordinario de Sesiones
Washington D.C. Oct. 23-Nov. 7, 2014
ANEXO I

Índice:

1) Informe APC: Internet y Discriminación
2) Informe ADC: Libertad de Expresión e Internet
3) Informe F. Karisma: Educación y Cultura e Internet
4) Informe Derechos Digitales: Internet y Privacidad
5) FGV: Ley de Marco Civil de Brasil

Nota informativa de APC sobre internet y el derecho a no padecer discriminación

4 de agosto de 2014

Sección 1. Definición /fuente del derecho a la no discriminación:

1.a Marco internacional de los derechos humanos

Al amparo de la legislación internacional sobre derechos humanos, el derecho a no padecer discriminación garantiza la igualdad de todos los individuos ante la ley. En particular, se exige a los gobiernos que respeten y promuevan los derechos y libertades de las personas sin que medie discriminación o distinción basada en la raza, el color, el lenguaje, la religión, la opinión política o de otra índole, el origen nacional o social, la propiedad, el linaje o cualquier otra condición social. El derecho a no ser discriminado/a está consagrado en el artículo común 2 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por su sigla en inglés), el Pacto Internacional de Derechos Económicos, Sociales y Culturales (ICECSR, por su sigla en inglés) y la Declaración Internacional de Derechos Humanos (UDHR, por su sigla en inglés)

El Comité de Derechos Humanos de la ONU produjo un Comentario General, en el cual se define la discriminación como "cualquier diferenciación, exclusión, restricción o preferencia fundada en términos tales como la raza, el color, el sexo, el lenguaje, la religión, la opinión política o de otra índole, el origen nacional o social, la propiedad, el linaje o cualquier otra poosición social, y que tiene como propósito o como resultado la anulación o la disminución del reconocimiento, goce o ejercicio de todas las personas, en pie de igualdad, de todos los derechos y libertades" (Comentario General No.18, párr. 7).

Varios tratados internacionales profundizan diversos aspectos de la discriminación, entre otros la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial

(CERD, por su sigla en inglés), la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer (CEDAW, por su sigla en inglés), la Covención sobre los Deerechos del Niño (CRC, por su sigla en inglés) y la Covención sobre los derechos de las personas con discapacidad (CRPD, por su sigla en inglés).

1.b Sistema interamericano

El derecho a la no discriminación también está consagrado por el sistema interamericano en su carta fundacional, los instrumentos de derechos humanos y las convenciones dedicadas a la eliminación de la discriminación y el racismo.

La Carta de la Organización de los Estados Americanos declara que "todos los seres humanos, sin distinción de raza, sexo, nacionalidad, credo o condición social, tienen derecho al bienestar material y a su desarrollo espiritual, en condiciones de libertad, dignidad, igualdad de oportunidades y seguridad económica" (Carta de la OEA, Artículo 45, párr. a).

Tanto la Declaración Americana de los Derechos y Deberes del Hombre como la Convención Americana sobre Derechos Humanos incluyen disposiciones para asegurar el derecho a la no discriminación. La Convención Americana sobre Derechos Humanos va tan lejos como para decir que la derogación de las obligaciones de la Convención en situaciones de emergencia pública no puede involucrar discriminación sobre la base de la raza, el color, el sexo, el lenguaje, la religión o el origen social.

Más allá de esos instrumentos fundacionales, el sistema interamericano ha codificado la Convención Interamericana contra el Racismo y Toda Forma de Discriminación e Intolerancia, y subraya el deber de los estados de promover este derecho, entre otras maneras a través de "adoptar las políticas especiales y acciones afirmativas para garantizar el goce o ejercicio de los derechos y libertades fundamentales de personas o grupos que sean sujetos de racismo, discriminación racial o formas conexas de intolerancia con el objetivo de promover condiciones equitativas de igualdad de oportunidades, inclusión y progreso para estas personas o grupos".[1] El sistema interamericano también cuenta con convenciones dirigidas a tipos específicos de discriminación, como la discriminación racial y otras formas relacionadas de intolerancia, la violencia hacia las mujeres y la discriminación de las personas con discapacidades.

El sistema interamericano estableció varios mecanismos para controlar el cumplimiento de las normativas de derechos humanos. Junto a la Comisión Interamericana y la Corte de Derechos Humanos, cuenta además con relatorías sobre temas específicos estrechamente relacionados con el derecho a la no discriminación, como los derechos de los pueblos originarios, de las mujeres, los migrantes, la infancia, las personas afrodescendientes, los derechos de las personas lesbianas, gays, bisexuales, transexuales e intersexuales (LGBTI), y también contra la disrciminación racial y para la libertad de expresión y los/las defensores/as de los derechos humanos.

Sección 2: Relevancia del derecho a la no discriminación para internet

2.a ¿Cuáles son las oportunidades y los desafíos que la tecnología plantea al derecho a la

[1] http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-68_racismo.asp, preámbulo y Artículo 5.

no discriminación?

El desarrollo rápido, sin precedentes, de las nuevas tecnologías de la comunicación y la información, particularmente de internet y las redes sociales, tuvo un impacto profundo y a la vez complejo sobre la discriminación, tanto en línea como fuera de las redes.[2] Por un lado, la tecnología puede ser un potente facilitador para los grupos marginados, al proporcionarles tanto un medio de expresión como los recursos para ejercer toda una gama de derechos humanos. Se reconoce que la naturaleza distribuida y abierta de internet fomenta las manifestaciones de una pluralidad de voces y perspectivas que pueden enfrentar y desafiar las posturas discriminatorias, a la vez que empoderar a las personas y grupos a los que apunta la discriminación.

Por otro lado, la tecnología puede a su turno dar lugar a una diseminación más amplia de contenidos discriminatorios, y puede producir nuevas formas, manifestaciones y dimensiones de la discriminación. Además, como señala el Relator especial de la ONU sobre formas contemporáneas del racismo en un informe reciente, la mayoría de las veces las voces de las personas a las que suele apuntar la discriminación continúan ausentes, debido a que éstas carecen de acceso a internet y las redes sociales, por lo que las ideas racistas siguen sin ser cuestionadas.[3] Tanto las desigualdades de acceso a internet y a las redes sociales, como la propiedad de los medios y la gobernanza de internet amplifican la intolerancia.

2.b ¿De qué manera impacta la tecnología en el derecho a la no discriminación en las Américas?

La discriminación en línea se manifiesta de muchas maneras en las Américas. Aquí se presenta una lista no exhaustiva de ejemplos:

- En Colombia, las mujeres activistas y defensoras de los derechos humanos, e integrantes de redes o movimientos han sido **víctimas de piratería, piratería telefónica y programas espía, o les han robado su computadora**. Estos ataques se efectúan tanto para intimidar y amenazar a las mujeres como para obtener información confidencial, como bases de datos con información sobre las victimas del conflicto colombiano, o demandas y procesos judiciales, por ejemplo.[4]
- En México, el dominio 1dmx.org, un sitio web que funcionaba como portal para recibir, clasificar y publicar videos, fotos y testimonios de violaciones a los derechos humanos por parte de las fuerzas de seguridad, fue **suspendido por una supuesta violación de los términos de uso**. Las ONG de la región consideraron a esa acción como un acto de **censura política en internet**.[5]
- En Argentina, algunas investigaciones conluyeron que **los tratantes de personas emplean las redes sociales, el correo electrónico, el chat y los teléfonos celulares** para construir una relación de confianza en línea y convencer a las víctimas de que abandonen sus

[2] Al tratar la discriminación en línea, esta nota informativa se concentra en la discriminación hacia individuos y la información e ideas que buscan y comparten en línea. No se hace referencia al importante tema relacionado de la neutralidad de la red, el principio según el cual todo tráfico debe ser tratado de manera equitativa, no discriminatoria, independientemente de su origen.

[3] http://www.ohchr.org/Documents/Issues/Racism/A-HRC-26-49.pdf

[4] http://giswatch.org/en/country-report/womens-rights-gender/colombia

[5] http://www.digitalrightslac.net/en/censura-politica-en-internet-una-realidad-en-mexico-con-un-poco-de-ayuda-de-estados-unidos-y-godaddy-com/

hogares, sus familias y hasta su país, para poder explotarlas. Es un método usado con frecuencia con adolescentes, que encuentran en estas relaciones la posibilidad de huir de sus problemas familiares.[6]

• Un estudio reciente en Estados Unidos encontró que casi la mitad (42 %) de jóvenes LGBT dijo haber **padecido acoso u hostigamiento en internet**, tres veces más que los/las jóvenes no-LGBT. De cada cuatro jóvenes LGBT, una/uno dijo haber sido **hostigado/a o acosado/a en línea, durante el último año, debido a su orientación sexual o identidad de género**. Un quinto sufrió un acoso similar via mensaje de texto.[7]

2.c En qué se parece y en qué se diferencia la discriminación en internet y fuera de línea a la luz de los principios generales de derechos humanos

Si bien la tecnología puede introducir nuevas formas y manifestaciones de la discriminación, y a menudo aumentar su escala, es importante señalar que la discriminación en línea integra un continuo con la que se vivencia fuera de internet. Sin embargo, debido a que la discriminación en línea no suele ser reconocida como una violación a los derechos humanos, y porque las leyes van a menudo a la zaga de las innovaciones tecnológicas, es frecuente que falte protección y reparación para las víctimas de discriminación en línea.

Hay también desafíos específicos del entorno digital para la protección del derecho a la no-discriminación. Por ejemplo, al haber grandes cantidades de información personal disponible en línea, se vuelve mucho más fácil apuntar a una persona a partir de su orientación sexual, religión o ideología política. Además, la discriminación en línea tiene lugar por lo general en plataformas y redes de propiedad y regulación privadas. Esto coloca en manos de los actores corporativos una responsabilidad increíble, que incluye el poder de censura. Como resultado, a menudo hay serias deficiencias en lo que atañe a la transparencia y el debido proceso, incluyendo las apelaciones. Más allá de esto, las compañías suelen ser inconsistentes al hacer cumplir las normas comunitarias.

Sección 3: Marcos legales / regulatorios en la región

La Relatora especial de la OEA sobre libertad de expresión Dra. Catalina Botero se refirió al tema de la no discriminación en línea en su informe anual más reciente. La Relatora especial recomienda que se tomen medidas para "promover de manera progresiva el acceso universal, no sólo a la infraestructura sino también a la tecnología necesaria para su uso, y a la mayor cantidad posible de información disponible en internet; eliminar los obstáculos arbitrarios al acceso a la infraestructura, la tecnología y la información en línea, y adoptar medidas de diferenciación positiva que permitan que las personas y comunidades marginadas y discriminadas puedan disfrutar este derecho de manera efectiva."

Al considerar este tema desde la perspectiva de la libertad de expresión, la Relatora especial señaló: "En lo que respecta a internet, la obligación de no discriminar significa que, además de los deberes de dar acceso y asegurar el pluralismo antes mencionados, es necesario emprender acciones por todos los medios adecuados para garantizar que todas las personas -sobre todo

[6]http://giswatch.org/en/country-report/womens-rights-gender/argentina
[7]http://www.glsen.org/press/study-finds-lgbt-youth-face-greater-harassment-online

quienes pertenecen a grupos vulnerables o que manifiestan críticas a asuntos de interés público- puedan diseminar contenido e información en condiciones de igualdad. En este sentido, es necesario garantizar que en internet no haya un trato discriminatorio de determinados contenidos en detrimento de otros distribuidos por cierto sector de la sociedad."

Las recomendaciones de la Relator especial son convincentes, en parte porque en la región existe una importante brecha en los marcos legales y regulatorios. Este es realmenteun desafío global, ya que la legislación va a la zaga de los avances tecnológicos, a menudo la tecnología no es bien entendida, y se suele presionar para que haya respuestas políticas a las violaciones de derechos humanos relacionadas con la tecnología. Incluso el Marco Civil de Brasil, que es citado en todo el mundo como la vanguardia legislativa sobre internet y los derechos humanos, no incluye una protección explícita a la discriminación en línea.[8]

En lo que respecta a los marcos legales y regulatorios de la región, todavía existen importantes desafíos a la protección contra la discriminación en línea, porque incluso en los casos en que existe protección contra la discriminación, ocurre a menudo que las violaciones en línea no son consideradas tales, y la protección legal o bien no existe o no se aplica. Estos estudios de caso de México permiten ilustrar estas brechas.

Louisa[9]
Louisa es psicóloga, y es una activista por los derechos de las mujeres y las personas LGTTBI. Luisa fue sometida a amenazas, discriminación y vigilancia de su teléfono celular, su correo electrónico y sus redes sociales debido a su activismo en defensa de los derechos de las lesbianas. La fiscalía se negó a ocuparse del caso con el argumento de que las amenazas y acosos a traveés de esos medios no son delitos. Luisa se puso en contacto con CONAPRED, el Consejo nacional para la prevención de la discriminación, que sólo intervino en la primera de sus denuncias (sobre la amenza de quemar su casa porque ella es lesbiana) y logró que la fiscalía emprendiera acciones, aunque nunca se autorizó la presentación de una denuncia formal.

En los casos de agresiones posteriores Luisa se dirigió directamente a los medios de comunicación y luego pasó a la protesta pública ante la falta de respuesta de CONAPRED y la fiscalía, lo cual sumó a su caso una situación de violencia institucional. La respuesta de los intermediarios fue tibia: la compañía telefónica no proporcionó una solución y la solución propuesta por el blog no fue relamente eficaz.

Lo destacable de este caso es que Louisa trató de usar las instituciones a cargo de la protección contra la discriminación, pero éstas no hicieron nada por ella:

- Documentó y guardó copias de las amenazas, al menos de los mensajes de correo electrónico.
- Informó a las autoridades acerca del incidente -a la policía, a entidades que se ocupan de

[8]Si bien el Marco Civil no incluye resguardos explícitos contra la discriminación en línea, el artículo 4 establece entre sus metas la promoción del derecho al acceso a internet de toda persona. Asimismo, contiene disposiciones sobre neutralidad de la red, que está relacionada con la discriminación, como se señaló más arriba, aunque va más allá del alcance de este informe.

[9]http://giswatch.org/en/country-report/womens-rights-gender/mexico

los derechos humanos y también a los proveedores de servicios en los que se publicaron las amenazas, reclamando que los proveedores actuaran según está previsto en los términos del servicio.

- Cuando no obtuvo respuesta de una autoridad, se dirigió a otra autoridad. Insistió en hacer que el sistema funcionara, pese a sus flaquezas.
- Cuando no obtuvo respuesta de ninguna autoridad, en el segundo caso, acudió a los medios de comunicación
- Además, siguió uno de los principios básicos de la libertad de expresión: no combatir las palabras ofensivas mediante la censura sino con más palabras; y al menos en un caso logró que personas religiosas conservadoras modificaran su concepción del lesbianismo.

Finalmente, trató de aprender todo lo posible sobre seguridad en línea, y compartió lo aprendido.

Sección 4: Jurisprudencia reciente sobre el derecho particular, casos actualmente en litigio

A nivel global, el problema de la discriminación racial y las nuevas tecnologías es considerado un tema emergente crítico. El Relator especial de la ONU sobre formas contemporáneas de racismo centró su informe annual en temas relactivos al uso de las nuevas tecnologías de la infromación, internet incluida, para la diseminación de ideas racistas y mensajes de odio, y para incitar el odio y la violencia por motivos raciales. El informe examina el contexto, las tendencias principales y las manifestaciones de racismo en internet y las redes sociales, y proporciona un panorama de los marcos legales y políticos así como de las medidas tomadas a nivel internacional, regional y nacional, al igual que de algunas de las normativas regulatorias adoptadas por los proveedores de internet y redes sociales. El Relator especial presenta ejemplos de las medidas tomadas para respondes al uso de internet y las redes sociales para propagar racismo, odio, xenofobia y otras formas de intolerancia relacionadas, a la vez que destaca la contribución positiva de internet y las redes sociales en tanto herramientas eficaces para combatir el racismo, la discriminación, la xenofobia y la intolerancia.

En las conclusiones y recomendaciones de su informe, el Relator especial señala la importancia de los esfuerzos legales y políticos para combatir la incitación al odio en internet, pero advierte que las medidas legislativas deben tener en cuenta la obligación de los estados de proteger otros derechos fundamentales, como la libertad de expresión y opinión, tal como lo proclaman tanto la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial como el Pacto Internacional sobre Derechos Civiles y Políticos, y nunca deben usarse como pretexto para la censura. El Relator especial afirrma que "[c]ombatir el uso de internet y las redes sociales para propagar contenido racista, etnofóbico y xenofóbico, que incita a la violencia, requiere una perspectiva que incluya a múltiples partes interesadas" (A/HRC/26/49, párr. 66), destacando así el papel determinante del sector privado.

Al ocuparse de las acciones concretas para enfrentar el racismo en línea, el Relator especial señala la importancia del acceso asequible a internet y la promoción del contenido local, en particular de los grupos que más a menudo son objeto de discriminación racial, para así reducir la asimetría informativa y las concepciones erróneas que nutren a los sentimientos racistas y xenófobos (A/HRC/26/49, párr. 68-69).

El Relator especial recuerda a los estados la importancia de reconocer el papel fundamental que desempeña la educación en el combate al racismo, la discriminación racial, la xenofobia y la intolerancia, y alienta el desarrollo de programas educativos y de promoción de la alfabetización en medios de comunicación, en particular para los y las jóvenes.

Reconociendo la importancia de que haya movimientos fuertes que contrarresten el racismo y la intolerancia en línea, el Relator especial sugiere: "La infraestructura en propiedad comunitaria, la capacitación en manejo de redes y de contenido, y el uso de software alternativo, como el software libre y de fuente abierta, pueden ser de ayuda para zanjar las brechas de conocimiento y acceso existentes".

Sección 5: Conclusión

Ante los crímenes y problemas sociales nuevos y emergentes, suele tenderse a crear nuevas leyes y regulaciones como solución. Aunque estén bien intencionadas, esas nuevas leyes a menudo están supeditadas a una tecnología, lo que puede hacer que rápidamente se vuelvan obsoletas y no logren enfrentar las causas que dan origen a la discriminación, en la medida en que buscan aplicar un parche tecnológico. Como se señaló antes, las violaciones a los derechos humanos relacionadas con la tecnología son parte de un continuo, y son frecuentemente una manifestación de discriminación, marginación y desequilibrios de poder que se originan fuera de internet. El sistema interamericano ya cuenta con fuertes mecanismos de protección al derecho a la no-discriminación. Para el entorno digital, que cambia con rapidez, alentamos a la Comisión a que considere formas eficaces de enfrentar la discriminación relacionada con la tecnología, apoyándose en sus sólidos cimientos en el ámbito de los derechos humanos y convocando a especialistas técnicos relevantes.

Instrucciones de APC para la Comisión Interamericana de Derechos Humanos sobre acceso a internet y derechos humanos

4 de agosto de 2014

access@apc.org

Contexto

Internet se ha convertido en una herramienta fundamental para nuestra vida cotidiana. Su uso ha sido incorporado a casi todos los aspectos de la existencia humana moderna. Si bien internet constituye un pozo casi infinito de conocimiento y un medio de comunicación y realización de transacciones para más de dos mil millones de personas, sigue siendo inaccesible para la mayoría de los habitantes del planeta.

La penetración de internet en los hogares a fines de 2014 será de 80% en los países industrializados y apenas 30% en los países en desarrollo, según estimaciones de UIT. A nivel mundial, hay cuatro mil millones de personas que todavía no usan internet y más de 90% de esa

gente vive en el mundo en desarrollo. En cuanto al acceso a la banda ancha, la brecha se perfila según un modelo similar, pero las desigualdades se acentúan mucho más.

Garantizar un acceso más universal a internet empezó a formar parte de las agendas políticas de los gobiernos en los años previos a la Cumbre Mundial sobre la Sociedad de la Información (CMSI). En 2003, esto llevó a los Estados miembro a unirse a las agencias de la ONU y la comunidad del desarrollo para asumir juntos una serie de compromisos a fin de mejorar el acceso a internet. Uno de los compromisos más notables fue la Línea de Acción C2 (Infraestructura de información y comunicación: fundamento esencial para la sociedad de la información[10]). Muchos de los objetivos y esfuerzos subsiguientes de la Línea de acción C2 se centraron en el desarrollo de "estrategias electrónicas" nacionales y el ambiente político y regulatorio necesario para mejorar la asequibilidad y la cobertura del acceso a la infraestructura básica de internet, fomentando, por ejemplo, la inversión en estructuras nacionales de backbone de fibra, interconexión y provisión de establecimientos de acceso público.

En relación a las demás regiones en desarrollo, la situación del acceso a internet en la región de América Latina y el Caribe (ALC) es bastante buena. Sin embargo, persisten numerosos desafíos en cuanto a la cobertura de zonas más remotas y a volver asequibles los servicios de banda ancha en la mayoría de los países. Si bien el porcentaje de usuarios y usuarias de América Latina aumentó 23% el año pasado y representa ahora 8% de la cifra global, la penetración promedio sigue rondando 30% y cae hasta 8% en algunos países. La baja penetración de la banda ancha en los hogares es quizá uno de los principales factores que inciden sobre estas estadísticas.

Acceso a internet y derechos humanos

En la década pasada, se inició el debate en cuanto a la posibilidad de considerar el acceso a internet como un derecho humano básico. Por ejemplo, una encuesta realizada entre 27.973 personas adultas en 26 países por el Servicio Mundial de BBC entre noviembre de 2009 y febrero de 2010 reveló[11] que según casi cuatro de cada cinco usuarios/as y no usuarios/as de internet del mundo entero, el acceso a internet debería ser un derecho fundamental. Del mismo modo, Internet Society (ISOC) realizó en 2012 una serie de encuestas en línea a más de 10 mil usuarios y usuarias de internet procedentes de 20 países. El 83% de las personas encuestadas se mostró clara o relativamente de acuerdo con la afirmación "El acceso a internet debe considerarse un derecho humano básico".

Los gobiernos han adoptado una amplia variedad de marcos regulatorios para el acceso a internet, tanto en base a legislación, como a leyes surgidas de casos. Por ejemplo, varios países establecieron el acceso a internet como un derecho y adoptaron leyes por las cuales el Estado debe garantizar el acceso generalizado a internet, y por las que los gobiernos se ven impedidos de restringir caprichosamente el acceso de los individuos a la información y a internet. Los casos más notables de este tipo son:

[10] http://www.itu.int/wsis/docs/geneva/official/poa.html
[11] http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf

- **Brazil.** En abril de 2014, el gobierno de Brasil adoptó el "Marco Civil[12] donde se establece que el acceso a internet es un requisito para el ejercicio de los derechos cívicos.
- **Costa Rica.** Una sentencia de la Corte Suprema de Justicia de Costa Rica, de julio de 2010, establece que: "Sin temor a equívocos, puede afirmarse que estas tecnologías han impactado el modo en que el ser humano se comunica, facilitando la conexión entre personas e instituciones a nivel mundial y eliminando las barreras de espacio y tiempo. En este momento, el acceso a estas tecnologías se convierte en un instrumento básico para facilitar el ejercicio de derechos fundamentales como la participación democrática (democracia electrónica) y el control ciudadano, la educación, la libertad de expresión y pensamiento, el acceso a la información y los servicios públicos en línea, el derecho a relacionarse con los poderes públicos por medios electrónicos y la transparencia administrativa, entre otros. Incluso, se ha afirmado el carácter de derecho fundamental que reviste el acceso a estas tecnologías, concretamente, el derecho de acceso a la Internet o red de redes."[13]
- **Ecuador.** La Constitución de 2008 reconoce el derecho de acceso universal a las TIC como un derecho de todas las pesonas (art. 16.2)
- **Estonia**. En 2000, el Parlamento de Estonia lanzó un programa extensivo para ampliar el acceso a todo el país. El gobierno justificó su acción diciendo que el acceso a internet es esencial para vivir en el siglo XXI [14].
- **Finlandia**. En julio de 2010, el gobierno anunció que todas las personas de Finlandia debían tener acceso a una conexión de banda ancha de un megabit por segundo y que, para 2015, dicha conexión debería ser de 100 Mbit por segundo[15].
- **Francia**. En junio de 2009, la Corte Suprema de Francia (el Consejo Constitucional) declaró que el acceso a internet es un derecho humano básico en una decisión que derogó algunas secciones de la ley HADOPI, que propone restringir el acceso a quienes continúen descargando material ilícito luego de dos advertencias[16].
- **Grecia.** El artículo 5A de la Constitución de Grecia establece que toda la ciudadanía tiene derecho a participar en la Sociedad de la información y que el Estado tiene la obligación de facilitar la producción, el intercambio, la difusión y el acceso a la información que se trasmite electrónicamente[17].
- **España.** Desde 2011, Telefónica, ex operador estatal monopólico de telecomunicaciones, cuya licencia ya incluía la obligación de brindar servicios de voz universales, también debe garantizar la oferta de un servicio de banda ancha a precio "razonable" de por lo menos un megabit por segundo en toda España[18].

[12]http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
[13]http://200.91.68.20/pj/scij/busqueda/jurisprudencia/jur_texto_sentencia.asp?nValor2=483874&tem1=013141&param7=0&lResultado=3&nValor1=1&strTipM=T&strLib=LIB
[14]http://www.csmonitor.com/2003/0701/p07s01-woeu.html
[15]http://www.cnet.com/news/finland-makes-1mb-broadband-access-a-legal-right
[16]http://www.foxnews.com/story/0,2933,525993,00.html
[17]http://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf
[18]http://www.reuters.com/article/idUSLH61554320091117

El resultado es que no existe una única manera de vincular el acceso a internet a la legislación nacional sobre derechos humanos. Tampoco hay consenso a nivel global en cuanto a que el acceso a internet sea un derecho humano. En cambio, estas iniciativas y otras (ver a continuación) han contribuido a crear la visión emergente actual según la cual, si bien no es necesario que el acceso a internet esté definido en las políticas y leyes nacionales como un derecho fundamental en sí mismo, se debe considerar como un facilitador de muchos otros derechos humanos y se debe proteger de múltiples maneras. En particular, todas las personas deben tener acceso a internet para ejercer y gozar de su derecho a la libertad de expresión y opinión, al igual que otros derechos humanos fundamentales. Por lo tanto, los Estados tienen la responsabilidad de garantizar la disponibilidad generalizada del acceso a internet y no pueden restringir caprichosamente el acceso de los individuos a internet.

Este enfoque fue planteado inicialmente por el Relator Especial de Naciones Unidas para la libertad de opinión y expresión, Frank La Rue, en su informe anual de 2011 para el Consejo de Derechos Humanos de Naciones Unidas.[19] El informe se basa en un año de consultas con los grupos de la sociedad civil, incluyendo varios de las Américas, y analiza "las tendencias y desafíos fundamentales del derecho de todos los individuos a buscar, recibir e impartir información e ideas de todo tipo por Internet".

En su informe, La Rue subraya que "Debe restringirse lo menos posible el flujo de información por internet, excepto en las escasas y limitadas circunstancias, muy excepcionales, que prescriben las leyes internacionales sobre derechos humanos". La Rue también destaca que "toda restricción debe estar claramente prevista por las leyes y debe demostrarse que se trata de la manera necesaria y menos intrusiva disponible a fin de proteger los derechos de los demás". El Relator especial insistió además en que no se necesitan nuevos derechos de acceso a internet, ya que las obligaciones existentes de los Estados de garantizar la libertad de expresión es lo suficientemente amplia como para garantizar la obligación de los mismos a desarrollar planes nacionales de acceso a internet, incluyendo a los grupos vulnerables y marginados.

El informe trata sobre el uso de internet como instrumento para la libertad de expresión y presenta una serie de recomendaciones sobre el trabajo que deberían realizar los gobiernos a fin de asegurar que toda la ciudadanía tenga acceso a internet. En total, el informe contiene 88 recomendaciones para la promoción y protección del derecho a la libertad de expresión en línea, varias de las cuales se refieren al acceso de todas las personas a internet. Otras recomendaciones llaman a los gobiernos a respetar el anonimato en línea, adoptar leyes de protección de la privacidad y los datos, y a descriminalizar la difamación. En particular, las recomendaciones de Frank La Rue se justifican en cuatro párrafos claves del informe:

> 67. A diferencia de los demás medios, Internet permite a las personas buscar, recibir y difundir información e ideas de todo tipo al instante y a bajo costo a través de las fronteras nacionales. Al

[19] Frank La Rue, 2011, " Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión", Consejo de Derechos Humanos de Naciones Unidas. http://ap.ohchr.org/documents/sdpage_e.aspx?b=10&se=116&t=9

ampliar enormemente la capacidad personal de disfrutar el derecho a la libertad de opinión y de expresión, que es un factor coadyuvante de otros derechos humanos, Internet potencia el desarrollo económico, social y político y contribuye al progreso de la sociedad en su conjunto. A ese respecto,
el Relator Especial alienta a otros titulares de mandatos de procedimientos especiales a ocuparse de la cuestión de Internet en relación con sus respectivos mandatos

78. Aunque las medidas de bloqueo y filtrado niegan el acceso de los usuarios a determinados contenidos de Internet, los Estados también han adoptado medidas para interrumpir por completo el acceso a Internet. El Relator Especial considera que la interrupción del acceso de los usuarios a Internet, sea cual sea la justificación aducida, incluso por motivos de violación de la legislación en materia de derechos de propiedad intelectual, es una medida desproporcionada y, en consecuencia, una violación del artículo 19, párrafo 3, del Pacto Internacional de Derechos Civiles y Políticos.

79. El Relator Especial exhorta a todos los Estados a que velen por que el acceso a Internet se mantenga sin interrupción, incluso en momentos de disturbios políticos.

85. En vista de que Internet se ha convertido en un instrumento indispensable para ejercer diversos derechos humanos, luchar contra la desigualdad y acelerar el
desarrollo y el progreso humanos, la meta del acceso universal a Internet ha de ser prioritaria para todos los Estados. En consecuencia, cada uno debe elaborar una política eficaz y concreta en consulta con personas de todos los sectores de la sociedad, entre ellos el sector privado, y con los ministerios gubernamentales competentes, a fin de que Internet resulte ampliamente disponible, accesible y asequible para todos los sectores de la población.

Normas emergentes de derechos humanos

Desde el informe La Rue de 2011, quedó claro que han empezado a surgir nuevas normas legales en relación a los derechos humanos e internet, entre las que se incluyen las relativas al acceso. Por ejemplo, en julio de 2011, el Comité de Derechos Humanos de ONU presentó una nueva Observación General 34, centrada en la elaboración de una nueva guía interpretativa para el Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, que por primera vez incluye referencia específica a internet.[20] La Observación General incluye lineamientos sobre la obligación de los Estados de brindar acceso a la información, para lo cual "Los Estados partes deberían tomar todas las medidas necesarias para fomentar la independencia de esos nuevos medios y asegurar el acceso a los mismos de los particulares".[21]

Resoluciones del Consejo de Derechos Humanos de Naciones Unidas

En base a las recomendaciones y el diálogo subsiguiente sobre el informe, los 47 Estados miembro del Consejo de Derechos Humanos de Naciones Unidas aprobó una Resolución

[20] Comité de Derechos Humanos, "Observación General No 34, Artículo 19 Libertad de Opinión y Libertad de Expresión". CCPR/C/GC/34 español, párrafos 15, 18-37 y 39.
[21] Ibid, párrafo 15.

fundamental[22] en julio de 2012 para incluir la "promoción, protección y disfrute de los derechos humanos en Internet". La Resolución, presentada por Suecia, contó con el apoyo de 70 países en total, tanto miembros, como no miembros del Consejo de Derechos Humanos.

Aunque la Resolución no se refiere al acceso a internet como tema específico, exhorta a los Estados a considerar la formulación y adopción de políticas públicas que afirmen la naturaleza global, abierta e interoperativa de internet, y que "su objetivo fundamental sean el acceso universal y el disfrute de los derechos humanos".

El documento señala que "el ejercicio de los derechos humanos, en particular del derecho a la libertad de expresión, en Internet es una cuestión que reviste cada vez más interés e importancia debido a que el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones" y resuelve que el Consejo de Derechos Humanos:

1. Afirma que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos;

2. Reconoce la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas;

3. Exhorta a los Estados a que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países;

4. Alienta a los procedimientos especiales a que tengan estas cuestiones en cuenta en sus mandatos actuales, según proceda;

5. Decide seguir examinando la promoción, la protección y el disfrute de los derechos humanos, incluido el derecho a la libertad de expresión, en Internet y en otras tecnologías, así como la forma en que Internet puede ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos, de conformidad con su programa de trabajo.

Nueve países de las Américas apoyaron esta resolución: Argentina, Bolivia, Brasil, Costa Rica, Guatemala, Honduras, Mexico, Perú y Uruguay, así como Estados Unidos y Canadá. Además, esta resolución fue citada y se tomaron como referencia las menciones a internet en informes multisectoriales de la Revisión Periódica Universal de Brasil, Colombia, Ecuador y México entre 2011 y 2014.

[22] http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

En junio de 2014 se adoptó otra resolución, esta vez con la aprobación de 82 Estados miembro, que trata específicamente sobre el acceso a internet.[23] La resolución exhorta a los Estados a "promover y facilitar el acceso a internet" y, afirmando el rol de la educación para el desarrollo, urge "a todos los Estados a promover la alfabetización digital y facilitar el acceso a la información de internet, que puede ser una importante herramienta para facilitar la promoción del derecho a la educación".[24]

Estas iniciativas normativas, y otras, han sido más elaboradas a nivel regional, también en las Américas. Por ejemplo, en abril de 2013, en base al trabajo conjunto realizado desde 2011, el Relator Especial de Naciones Unidas para la Libertad de Opinión y Expresión, la Representación para la libertad de medios de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial para la libertad de expresión de la Organización de los Estados Americanos (OEA) y el Relator Especial para la libertad de expresión y el Relator Especial para la libertad de expresión y el acceso a la información de la Comisión Africana de Derechos Humanos y de los Pueblos (ACHPR, por su sigla en inglés) presentaron una "Declaración conjunta sobre protección de la libertad de expresión y la diversidad en la transición digital terrestre". La Declaración, elaborada a partir de la Afirmación conjunta de 2011, también se enfoca en el acceso y los principios que se deben aplicar, también en relación al acceso universal a internet.[25]

El principio del acceso universal, es decir, la necesidad de garantizar una conectividad y acceso a la infraestructura de internet y otros servicios de TIC que sean universales, ubicuos, equitativos, asequibles y disponibles en todo el territorio de cada Estado, ha sido reconocido por los jefes de Estado en las Cumbres de las Américas[26]. Cada Estado tiene que decidir cuáles son los medios más adecuados, según las circunstancias, para garantizar la implementación de este principio. Además, el Artículo III, 1 c) de la Convención Interamericana para la Eliminación de Todas las Formas de Discriminación contra las Personas con Discapacidad establece que los Estados deben comprometerse a implementar "medidas para eliminar, en la medida de lo posible, los obstáculos arquitectónicos, de transporte y comunicaciones que existan, con la finalidad de facilitar el acceso y uso para las personas con discapacidad[27]."

Por último, en las Américas existe el informe más reciente, presentado en diciembre de 2013 por la Relatora Especial Regional para la Libertad de Opinión y Expresión, con un capítulo específico sobre libertad de expresión e internet.[28] El informe reconoce que, si bien la implementación del principio de acceso universal le compete a cada Estado, es necesario considerar estructuras inclusivas de precios, y prestar especial atención a la presencia de

[23] Borrador de la resolución L.24 disponible en: https://www.apc.org/en/pubs/apc-welcomes-human-rights-council-resolution-human

[24] Ibid, cláusulas 3 y 4 respectivamente.

[25] Ver también el informe completo de la Relatora Especial Regional, Catalina Botero (2013) http://www.oas.org/es/cidh/docs/anual/2013/informes/LE2013-esp.pdf

[26] http://www.summit-americas.org/SIRG/2012/041412/mandates_sc_es.pdf

[27] http://www.oas.org/juridico/spanish/tratados/a-65.html

[28] Relatora Especial Regional, Catalina Botero (2013) http://www.oas.org/es/cidh/docs/anual/2013/informes/LE2013-esp.pdf, páginas 493 - 550.

conectividad en todo el territorio de cada país, así como al acceso para las comunidades rurales y otros grupos, además de elaborar políticas para garantizar el acceso equitativo de las mujeres y grupos de personas discapacitadas. Este informe constituye una clara muestra del enorme alcance que ha tenido el discurso sobre acceso a internet y derechos humanos en un período de tiempo muy corto y presagia la necesidad de contar con un asesoramiento especializado y la ayuda de expertos y expertas para el monitoreo de los derechos humanos, así como la documentación, el análisis de mejores prácticas, el activismo y la supervisión del comportamiento de los Estados miembro en relación a los derechos humanos.

Perspectivas y conclusiones

En síntesis, queda claro que se están desarrollando nuevas normas de derechos humanos en relación al acceso a internet y los derechos humanos, incluso en las Américas. La respuesta ante el veloz desarrollo en el área de la tecnología, incluso la creciente adopción de internet por parte de las personas de toda la región, es el desarrollo de normas emergentes de derechos humanos que intentan aplicar los marcos existentes de derechos humanos, en lugar de crear nuevos derechos. Pero hay mucho trabajo por hacer, sobre todo por parte de los mecanismos de derechos humanos.

A pesar de las nuevas resoluciones del Consejo de Derechos Humanos, la Electronic Frontier Foundation (EFF) y otros grupos han observado que algunos Estados no están cumpliendo del todo con sus obligaciones internacionales en materia de derechos humanos, lo que incluye la adopción de las medidas necesarias para que se hagan efectivos esos derechos[29]. En este sentido, la Resolución sólo se ocupa indirectamente del acceso a internet y no descarta la posibilidad de que los países abusen de los derechos humanos en línea. La Resolución cita el Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos que "admite ciertas restricciones del derecho [a la libertad de expresión]" cuando estén previstas por ley por "(a) respeto a los derechos o la reputación de los demás; o (b) para proteger la seguridad nacional o el orden público, o la salud, o la moral públicas".

EFF señala que varios de los 47 Estados miembro del Consejo de Derechos Humanos censuran internet y el derecho de los ciudadanos y ciudadanas a la libre expresión en base a esos pretextos. Muchos Estados miembro han utilizado la propiedad intelectual como justificación para utilizar mecanismos técnicos de censura y, en varios países se han propuesto o aprobado regulaciones de suspensión del servicio de internet para siempre para algunos individuos — este tipo de norma se conoce generalmente como "ley de los tres golpes".

Las leyes que prohiben completamente el uso de internet a un individuo constituyen una clara violación de los derechos humanos y, si bien la Resolución sobre la libertad en internet y otras normas emergentes constituyen pasos positivos en pos de garantizar la aplicación de los

[29]https://www.eff.org/deeplinks/2012/07/un-human-rights-council-resolution-internet-and-human-rights-step-right-direction

derechos humanos en línea, en sí misma no alcanza para definir el alcance de las medidas que deben tomar los gobiernos para asegurar el acceso universal.

En base a las recomendaciones iniciales del informe de Frank La Rue, APC desarrolló una serie de criterios para brindar un marco eficiente, aunque simple, con el fin de evaluar la actuación de los países en relación al acceso a internet. Dichos criterios son los siguientes:

i. Si el Estado cuenta con un plan nacional de acceso;
ii. Si el Estado está fomentando un enfoque multisectorial para desarrollar una política de desarrollo de tecnologías de la información (TI) que mejore el acceso y la asequibilidad de internet;
iii. Si el Estado está desarrollando programas y políticas de asistencia para el acceso universal y el intercambio de conocimientos de TI con otros países;
iv. Si el Estado le suministra un acceso significativo a las minorías y otros grupos marginados, incluso las minorías linguísticas y con capacidades diferentes; y
v. Si el Estado alimenta e implementa, o ha implementado, programas de alfabetización digital/internet tanto dentro como fuera de las escuelas.

Estos criterios se deben utilizar para evaluar la adopción de medidas a fin de promover internet en los países de las Américas, y junto con el trabajo del Relator Especial Regional y otros y otras, requieren una mayor consideración sobre cómo desarrollar una supervisión de derechos humanos y una guía sobre informes para los Estados miembro y los grupos de la sociedad civil. La cuestión clave para Comisión Interamericana de Derechos Humanos es hasta qué punto debe alentar a sus países miembro a adoptar estrategias que garanticen el acceso a internet para todos y todas, desarrollar indicadores de monitoreo e informes, y brindar guía para la interpretación de instrumentos regionales cuando sea necesario (por ejemplo, sobre las obligaciones de acceso de los Estados miembro). En particular, esto podría incluir la consideración de aspectos en torno de la asequibilidad, la presencia de establecimientos de acceso público y el acceso al espectro radial.

Otra posibilidad para apoyar el desarrollo en este sentido es participar en el trabajo del FGI. Uno de los ocho subtemas del próximo encuentro del FGI en Istanbul es “Políticas para fomentar el acceso”. El 9o FGI se propone lograr un mayor y mejor vínculo con otros procesos de gobernanza de internet tales como los resultados de NETmundial y el diálogo en curso a partir de la revisión de la CMSI, CSTD, UIT y el Grupo de trabajo para fomentar la cooperación, entre otros. Esto podría resultar en un marco más universal para centrarse en las cuestiones del acceso. En el segundo día del FGI, una de las sesiones principales será sobre “Políticas que habilitan el acceso, el crecimiento y el desarrollo en internet”. La sesión se hará en forma de mesa redonda, con el objetivo de producir recomendaciones políticas claras y tareas domiciliarias para los y las responsables de la formulación de políticas.

Asociación por los Derechos Civiles

ADC: Libertad de expresión e Internet

1. Identificación del derecho, contenido y problemática/relevancia local y/o regional si la organización a cargo es de corte regional.

El derecho a la libertad de pensamiento y expresión es un derecho que ha sido descripto como la "piedra fundamental" del ordenamiento democrático y una de las más sólidas garantías de la democracia moderna[30]. Él ha sido objeto de generosas interpretaciones por parte de los órganos del sistema interamericano de derechos humanos, que han generado a partir de ellas estándares interamericanos sumamente protectorios de este derecho.

De estos estándares, destacaríamos dos que parecen especialmente relevantes para considerar la situación del derecho en relación a Internet.

En primer lugar, la cuestión de la dimensión *individual* y *social* de la libertad de expresión. La primera se refiere al derecho de cada persona a expresar los propios pensamientos, ideas e informaciones; la segunda al derecho de la sociedad a procurar y recibir cualquier información, a conocer los pensamientos, ideas e informaciones ajenos y a estar bien informada[31].

En segundo lugar, el artículo 13 de la Convención es también generoso respecto del tipo de expresiones que son alcanzadas por la protección que confiere este derecho. Él establece que la libertad incluye informaciones e ideas de toda índole, ya sea "oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección". Este lenguaje del artículo 13 recepta entonces todo tipo de expresiones que ocurren en Internet.

Los estándares interamericanos en materia de libertad de expresión, entonces, ofrecen un marco regional adecuado a la hora de pensar a este derecho frente a su ejercicio en el ámbito digital. La doble dimensión del derecho permite reivindicar su alcance para lidiar con problemas y restricciones presentes en distintos países de América Latina, como consecuencia, en algunos casos, de desigualdades en el acceso a las tecnologías necesarias para conectarse a Internet y, en otros, de decisiones políticas, reglamentaciones legales y decisiones judiciales que tienden a limitar la expresión del los ciudadanos en Internet. Por su parte, el reconocimiento amplio del derecho en todas

[30]CIDH, Informe Anual de la Relatoría Especial para la Libertad de Expresión de 2009, Cap. II, párr. 522.
[31]CIDH, Informe Anual de la Relatoría Especial para la Libertad de Expresión de 2009, Cap. III, párr. 13.

sus expresiones resulta también útil para evaluar formas de ejercer la expresión propias de un medio interactivo y multidireccional como Internet.

En general, las constituciones de América Latina suelen reservar un espacio relevante al derecho internacional de los derechos humanos, y a veces al derecho interamericano que surge de la propia Convención Americana[32].

Una de las primeras constitucionales en hacerlo fue la Constitución del Perú de 1979, que estableció en su artículo 105 que los "preceptos contenidos en los tratados relativos a derechos humanos, tienen jerarquía constitucional. No pueden ser modificados sino por el procedimiento que rige para la reforma de la Constitución". En el mismo sentido, la constitución de Guatemala de 1985 dispuso en su artículo 46 como principio general que "en materia de derechos humanos, los tratados y convenciones aceptados y ratificados por Guatemala, tienen preeminencia sobre el derecho interno." Por su parte, el artículo 5 de la Constitución de Chile establece que el "ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana. Es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes".

Las constituciones creadas en los años noventa también siguieron un camino similar. Por ejemplo, la Constitución de Colombia de 1991 establece en su artículo 93:

> "Los tratados y convenios internacionales ratificados por el Congreso, que reconocen los derechos humanos y que prohíben su limitación en los estados de excepción, prevalecen en el orden interno. Los derechos y deberes consagrados en esta Carta, se interpretarán de conformidad con los tratados internacionales sobre derechos humanos ratificados por Colombia."

En la Argentina, la Constitución Nacional en su artículo 75.22 incorporó --en 1994-- con *jerarquía constitucional* a la Convención Americana de Derechos Humanos y la Corte Suprema de Justicia de la Nación ha sostenido --en numerosos precedentes-- que la Convención es plenamente aplicable y que las interpretaciones de los órganos autorizados del sistema son obligatorias en el derecho interno. Asimismo, la ley 26.032 de 2005 estableció de manera expresa que la "búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de Internet, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión"[33].

[32] Fix-Zamudio, H. (2004). El derecho internacional de los derechos humanos en las Constituciones latinoamericanas y en la Corte Interamericana de Derechos Humanos. Revista Latinoamericana de Derecho, 1(1), 141–180.

[33] Ley 26.032.

Incluso las constituciones más modernas, como las de Venezuela, Bolivia y Ecuador reconocen la primacía del derecho internacional de los derechos humanos en el ámbito interno[34].

En conclusión, el orden jurídico *interno* de una gran mayoría de países en América Latina presta atención a lo que ocurre en el ámbito internacional. Ello significa que, en principio, los estándares interamericanos de protección de la libertad de expresión que emanan del sistema interamericano de derechos humanos, es decir, de la Convención Americana y las interpretaciones que sobre ella emitan los órganos del sistema, son parte del derecho interno en muchos países de América Latina.

2. Marco normativo del derecho en cuestión, regulación específica en la materia a nivel local/regional si se conoce; proyectos de ley en tratamiento o planificación que afecten el derecho para bien o para mal.

A nivel regional, el artículo 13 de la Convención Americana es la regulación de más alta jerarquía en materia de libertad de expresión. En general, esta norma es complementada por normas internas de carácter constitucional que con mayor o menor generosidad también reconocen el derecho a la libertad de expresión.

Otras constituciones incorporan de distintas maneras al artículo 13 a su propio marco normativo interno, ya sea por la incorporación de ciertos tratados internacionales *con jerarquía constitucional* (como es el caso de la Argentina) o mediante la introducción del derecho internacional al derecho interno (como es el caso de Colombia).

A pesar de este reconocimiento convencional y constitucional, lo cierto es que América Latina en los últimos años ha sido el escenario de distintas restricciones a este derecho fundamental, como lo atestiguan los informes de la propia CIDH y las decisiones de la Corte Interamericana. Ya sea que se trate de actos de agresiones, amenazas u hostigamientos a comunicadores sociales, del inicio de causas criminales contra periodistas o medios de comunicación o la imposición de indemnizaciones civiles desproporcionadas, en muchos países de América Latina hemos visto que la plena vigencia de la libertad de expresión exige una sociedad civil comprometida con la defensa del mismo y tribunales dispuestos a resguardar este derecho frente a acciones que tienden a limitarlo. Asimismo, también hemos visto en América Latina formas de *censura sutil* que tienden a restringir el derecho por mecanismos indirectos como el control del acceso a insumos básicos, la distribución de licencias de radiodifusión o la discriminación arbitraria con fondos de publicidad estatales.

Es en ese contexto de amenazas a la libertad de expresión que es posible encontrar medidas que tienden a restringir, actual o potencialmente, el derecho a la libertad de expresión en Internet.

[34]Cfr. Constitución de la República Bolivariana de Veneuzuela de 1999, artículo 23; Constitución de Ecuador de 2008, artículo 424 y Constitución del Estado Plurinacional de Bolivia de 2009, artículo 13.IV.

A continuación nos referiremos a algunos casos paradigmáticos de limitación al derecho a la libertad de expresión en Internet.

Ecuador y la prohibición de los discursos anónimos

Una de las leyes que más ha afectado al discurso en línea en América Latina es la nueva ley de comunicaciones del Ecuador, de junio de 2013. Dicha norma incluye, de manera inédita en la región, a Internet como uno de los espacios sobre los cuales la ley extiende su competencia regulatorio[35].

Además, la ley específicamente regula ciertas prácticas en materia de libertad de expresión propias del mundo digital, como los comentarios de terceros en las páginas de periódicos y foros de Internet. El artículo 14 sostiene, al respecto, lo siguiente:

> "Los comentarios formulados al pie de las publicaciones electrónicas en las páginas web de los medios de comunicación formalmente constituidos, serán responsabilidad de los medios si no verifican la identidad de las personas que formulan dichos comentarios".

La norma equivale, lisa y llanamente, a prohibir el discurso anónimo que se encuentra protegido por el artículo 13 de la Convención Americana. Asimismo, al imponer responsabilidad a medios de comunicación por comentarios de terceros, actúa como fuerte elemento inhibitorio destinado a limitar la participación de los ciudadanos en el debate público y a incentivar prácticas de censura por parte de los medios de comunicación sobre sus propios lectores.

La responsabilidad de los intermediarios en Brasil y Argentina

Tanto en Brasil como en Argentina, en los últimos años, se ha expandido la práctica jurisprudencial de responsabilizar a los intermediarios en el flujo de información en Internet por contenidos producidos por terceros. No se trata, en estos casos, de la creación de reglas específicas como en el caso de Ecuador, sino de la aplicación a Internet de viejos principios del derecho civil que parecen incompatibles con la libre circulación de información en Internet.

En el caso de Argentina, esto es producto de cierta jurisprudencia en los tribunales civiles que tiende a responsabilizar a los intermediarios por contenidos de terceros, especialmente a los motores de búsqueda por los resultados que ellos ofrecen. Las sanciones van desde medidas cautelares obligando a eliminar de los resultados de búsqueda ciertos contenidos --de manera genérica o específica-- hasta indemnizaciones civiles de diferente monto. Estos casos judiciales han recibido respuestas de dos tipos: algunos de ellos han llegado a la Corte Suprema de Justicia y aguardan su resolución (ver siguiente sección). En otros casos, esta problemática ha generado iniciativas de

[35] Ley Orgánica de Comunicación del Ecuador. 21 de junio de 2013. Art. 5.

regulación en el Congreso, como el proyecto 2668-D-2012 que busca crear un modelo de inmunidad condicionada estableciendo --además-- que sólo los jueces pueden ordenar el retiro de contenidos[36].

En Brasil también ha habido muchas demandas contra intermediarios por contenidos producidos por terceros. Una de las acciones judiciales que más han impactado en la circulación de información se dio en el caso *Cicarelli*, donde una demanda generó el bloqueo masivo de *YouTube* en todo Brasil durante varios días (ver siguiente sección). La cuestión de los intermediarios fue abordada por el *Marco Civil de Internet*, el cual dispuso al respecto que los proveedores de servicios de conexión a Internet no pueden ser responsabilizados por contenidos de terceros, y quienes proveen *aplicaciones* sólo pueden ser responsabilizados si no dieran de baja esos contenidos luego de una orden judicial que así lo ordene[37].

Así como vemos esas amenazas, también es posible identificar tendencias positivas que tienden a resguardar el derecho a la libertad de expresión en entornos digitales.

La ley de neutralidad de Chile

La *neutralidad de la red* es un valioso principio de gobernanza de Internet que debe ser resguardado por el Estado mediante regulaciones adecuadas que prohíban la discriminación de datos por parte de los actores involucrados en el tráfico con capacidad de hacerlo. Chile fue el primer país del mundo en hacerlo: la ley No. 20.453 estableció en 2010 el principio de neutralidad en la red para los consumidores y usuarios de internet[38].

El marco civil de Brasil

Brasil, por su parte, ha dado uno de los pasos más audaces hacia la protección de la libertad de expresión --entre otros derechos-- en el entorno digital. Ha optado por una regulación compleja, compuesta de muchos artículos que cubren diversos temas: desde la responsabilidad de los intermediarios a la neutralidad de la red, pasando por cuestiones de acceso y vigilancia de las telecomunicaciones. El *Marco Civil de Internet* constituye uno de los principales esfuerzos de estados latinoamericanos por resguardar los derechos de sus ciudadanos en línea. A medida que se avanza en la implementación de su articulado y se empieza a poner en juego su efectividad, es útil que el resto de los países miren hacia Brasil para aprender de esa experiencia, que fue alcanzada gracias a

[36]Cfr. Proyecto de ley 2668-D-2012. Disponible en:
http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=2668-D-2012.
[37]Ley de Marco Civil en Internet. Disponible en:
http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm.
[38]Ley 20.453 del 26 de agosto de 2010. Disponible en:
http://www.subtel.gob.cl/images/stories/articles/subtel/asocfile/ley_20453_neutralidad_de_red.pdf.

un innovador esquema multisectorial que otros países de la región han comenzado a replicar[39].

3. Jurisprudencia reciente en torno al tema- preferentemente cortes supremas o altos tribunales/casos que se estén litigando en este momento y de cuya definición dependa la interpretación o aplicación de derechos.

A medida que Internet se vuelve un espacio más relevante para el debate público de nuestras democracias, de manera creciente es posible ver cómo los alcances y límites de ese derecho son discutidos por los tribunales. Hay varios precedentes en este sentido pero, consideramos, estamos en una situación donde la jurisprudencia en materia de libertad de expresión en Internet está en plena gestación. Por ello, nos referiremos a casos famosos en los que se puso en juego este derecho y casos que están pendientes de resolución.

Argentina

Ya nos hemos referido a cómo, en la Argentina, muchas personas famosas han demandado a los buscadores de Internet por los resultados que arrojaban las búsquedas de sus nombres. Estas personas solían tener el mismo argumento: esos resultados eran disvaliosos y afectaban su honor y --en muchos casos-- hacían un uso ilegítimo de su imagen. Demandaban a los buscadores por considerarlos partícipes necesarios de la violación de sus derechos. Y tuvieron bastante éxito: muchos jueces del fuero civil de la Ciudad de Buenos Aires concedieron medidas cautelares e indemnizaciones que, por un lado, impedían el acceso a contenidos cuya legitimidad era discutible, abarcaban más de lo necesario y --además-- generaban incentivos de censura en empresas comerciales interesadas, más que nada, en la venta de publicidad.

Dos de esos casos --los casos *Da Cunha* y *Rodríguez*-- llegaron a la Corte Suprema de Justicia. En mayo de 2014, la Corte Suprema argentina realizó dos audiencias públicas en las que se escucharon los argumentos de *amicus curiae* y de las partes en el caso *Rodríguez*. En la Argentina, este tipo de audiencias suelen preceder a la toma de una decisión definitiva, por lo que se espera que en el corto o mediano plazo el tribunal resuelva esta cuestión.

Brasil

Brasil cuenta con uno de los casos más antiguos en materia de libertad de expresión en Internet. En efecto, en 2007 un video de la modelo brasileña Daniela Cicarelli fue subido a YouTube, sin su consentimiento. Ella presentó una demanda exigiendo la retirada del video y el pago de una indemnización de 116.000 dólares por cada día que el video estuviera publicada. Si bien el video fue dado de baja, muchos usuarios no involucrados en la demanda oficial lo volvieron a subir y --antes eso-- el juez del caso ordenó el

[39]Por ejemplo, la Argentina creó a comienzos de 2014 la *Comisión Argentina de Políticas de Internet*, que busca ser un espacio gubernamental en el que desarrollar el modelo multisectorial de gobernanza.

bloqueo del servicio de YouTube, lo que dejó a todo el país sin posibilidades de acceder al servicio de video en línea más popular en todo el mundo.

Colombia

Recientemente, un comentarista del diario *El País* de Cali escribió un comentario en el que llamaba a un funcionario público "semejante rata". Por hacerlo, fue condenado a la pena de año y medio de cárcel y a pagar un multa de 9.5 millones de pesos. Varias voces vinculadas a los derechos humanos en Colombia cuestionaron la sentencia y la misma fue objeto de recursos constitucionales.

4. Condiciones de acceso a internet a nivel local/regional (si los tuvieren).

Si bien América Latina es una de las regiones con mayor crecimiento en términos de conectividad, todavía el acceso a Internet es profundamente inequitativo: sólo el 40 por ciento de la población accede a Internet[40]. Las desigualdades también se manifiestan entre países: mientras algunos --como Argentina, Chile, Uruguay y Colombia-- muestran tasas de penetración por encima del 50 por ciento de la población, otros países muestran tasas sumamente bajas como --por ejemplo-- Nicaragua, Honduras, Cuba o Guatemala (ver Figura 1).

Países	Porcentaje de penetración de Internet en la población
Argentina	67.00%
Chile	59.20%
Uruguay	56.10%
Colombia	55.90%
Costa Rica	43.70%
Panamá	43.40%
Puerto Rico	42.60%
República Dominicana	41.40%
Venezuela	39.70%
Brazil	39.00%
Mexico	36.90%

[40] Internet World Stats, consultado el 10 de junio de 2014.

Peru	34.10%
Ecuador	27.20%
Paraguay	23.60%
El Salvador	20.70%
Bolivia	19.60%
Guatemala	16.50%
Cuba	15.40%
Honduras	13.10%
Nicaragua	11.70%
TOTAL	39.90%

Fig. 1 Penetración de Internet en América Latina. Fuente: Internet World Stats, consultado el 10 de junio de 2014.

REGULACIÓN DE INTERNET Y SU IMPACTO EN EL DERECHO A LA EDUCACIÓN Y EL ACCESO A LA CULTURA EN COLOMBIA.

***Fundación Karisma**

1. Identificación del derecho y marco legal
2. Políticas Públicas
    2.1. Educación
    2.2. Cultura
        2.2.1. Bibliotecas
3. Legislación
    3.1. Ley 1680 de 2013
    3.2. Tratado de Marrakech
    3.3. Ley 1341 de 2009
4. Proyectos de Ley
    4.1. Proyectos que han pasado sin pena ni gloria
        4.1.1. Implementación de un marco jurídico para la universalización de la telecomunicaciones (incluyendo internet)
        4.1.2. La creación de una campaña de alfabetización digital nacional
        4.1.3. La garantía de acceso a internet como derecho fundamental
    4.2. Proyectos que han sido objeto de importantes polémicas
5. Decisiones judiciales
    5.1. Corte Constitucional. Sentencia C-011 de 2013
    5.2. Corte Constitucional. Sentencia T-713 de 2010
    5.3. Corte Constitucional. Sentencia T-550 de 2012
    5.4. Corte Constitucional. Sentencia T-058 de 2013
    5.5. Corte Constitucional. Sentencia T-040 de 2013
    5.6. Corte Suprema de Justicia - Sala de Casación Penal. Proceso n° 33474. Sentencia del día 10 de febrero del año 2010
6. Casos no judiciales
    6.1. Caso de María Luisa Piraquive (Colombia)
    6.2. Caso Documental del Presidente Correa (Ecuador)
    6.3. Casos de documentales (Ecuador y Colombia)
    6.4. Caso Compartir no es Delito (Colombia)
7. Neutralidad de la red en Colombia y problemas de acceso al servicio de internet

1. Identificación del derecho y marco legal

A nivel sustancial, desde el marco constitucional, se establece en Colombia que **la educación** *"es un derecho de la persona y un servicio público que tiene una función social; con ella se busca el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura".*[41] De igual manera, frente al **derecho a la cultura** coloca en cabeza del Estado *"el deber de promover y fomentar el acceso a la cultura de todos los colombianos en igualdad de oportunidades, por medio de la educación permanente".*[42] La Carta de Derechos coloca en rango constitucional y como obligación del Estado la promoción y la garantía del ejercicio del derecho a la educación y al acceso a la cultura.

El margo legal de reconocimiento de los derechos a la educación y la cultura en los países de América Latina existe tanto desde el nivel constitucional interno como en el marco de la suscripción de convenios internacionales sobre derechos humanos. Debe resaltarse que aquellos instrumentos internacionales que hacen referencia a la cultura se encuentran, principalmente, el Pacto Internacional de Derechos Económicos Sociales y Culturales,[43] el Protocolo Adicional a la Convención Americana sobre Derechos Humanos en materia de Derechos Económicos, Sociales y Culturales, el Protocolo Adicional de San Salvador a la Convención Americana sobre los Derechos del Hombre en materia de Derechos Económicos, Sociales y Culturales[44] y la Convención para la Eliminación de Todas las Formas de Discriminación Racial.[45]

En la era digital, el ejercicio de estos derechos fundamentales se encuentra con importantes oportunidades y desafíos. Internet, como espacio universal, sin frontera e interactivo, indiscutiblemente, ha facilitado a docentes, estudiantes, ciudadanas y ciudadanos una amplia variedad de herramientas educativas, contenidos, programas, aplicaciones, etc. Como nunca antes en la historia de la humanidad, las tecnologías digitales, en especial internet, nos ha permitido a todas y todos crear, modificar, compartir y usar multiplicidad de contenidos. Nuestras posibilidades de hacer valer los derechos a la educación y a la cultura son mayores hoy día y, en muchos casos, incluso a un costo mucho menor.

No obstante, el acceso al alcance de un *click* también entra en confrontación con otros derechos, en particular con el derecho de autor. Tensión que requiere un examen profundo, cuyo fin es encontrar un delicado equilibro que, por un lado, no limite indebidamente el ejercicio

[41] Artículo 67. Constitución política de Colombia.
[42] Artículo 70. Constitución política de Colombia.
[43] El artículo 15 del PIDESC garantiza el derecho de todas las personas a participar en la vida cultural y correlativamente establece la obligación del Estado de adoptar medidas para asegurar el pleno ejercicio de este derecho, entre ellas, medidas dirigidas a la conservación, desarrollo y difusión de la cultura.
[44] El artículo 14 reconoce el derecho a los beneficios de la cultura, cuyo contenido comprende, entre otros, el derecho a participar en la vida cultural y artística de la comunidad, y reitera la obligación del Estado de adoptar medidas para el desarrollo y difusión de la cultura.
[45] El artículo 5 establece el derecho de todos a participar, en condiciones de igualdad, en las actividades culturales.

de los derechos a la educación y a la cultura y que, por otro, respete los derechos de los autores sobre sus obras. En un mundo mediado cada vez más por las tecnologías digitales, dicho examen se hace más indispensable. La tendencia legislativa en cuanto a los regímenes de derecho de autor se ha ido inclinando a aumentar la protección de dicho derecho en detrimento, muchas veces, del ejercicio efectivo de nuestros derechos fundamentales.

El adecuado ejercicio del derecho a la educación y al acceso a la cultura en internet es garantía para un cabal acceso al conocimiento. Las oportunidades que nos brinda las herramientas tecnológicas como Internet hay que verlas también como la

> *[C]apacidad de nuevas tecnologías de darnos acceso a la infraestructura, a través de los artefactos de transmisión de la información. La forma como se regulan los artefactos por los cuales se transmite la información ha sido mediante el derecho de autor, que a su vez ha sido un marco jurídico protector de los titulares de estos derechos, bajo una mirada criminalizadora.*[46]

Por esta razón, debemos considerar necesario abordar la normatividad de derechos de autor desde una perspectiva de derechos humanos, toda vez que

> *[E]l énfasis en la cultura en los instrumentos de derechos humanos permite, entre otras cosas, entender los límites de una mirada esencialmente comercial en la materia. Esto favorecería una perspectiva en la cual el sistema de derechos autorales no tenga solo un fin económico.*[47]

2. Políticas Públicas

2.1. Educación

A propósito de la celebración del segundo centenario de la Independencia de Colombia (2019), el Gobierno Nacional se planteó tres lustros antes una agenda de desarrollo para orientar las políticas públicas en diferentes sectores hacia la consecución de metas ambiciosas pero posibles. El documento "Educación: Visión 2019" definía esas políticas para el sector educativo y uno de los programas estratégicos para mejorar la calidad y la competitividad de los colombianos era la "incorporación de las Tecnologías de la Información y la Comunicación (TIC) a los procesos educativos", que se justificaba como:

> *No cabe duda de que saber manejar computadores es una competencia esencial en el mundo de hoy, pero mucho más importante es saber utilizarlos con sentido: para aprender, para solucionar problemas, para mejorar la productividad del trabajo. Las TIC*

[46] Video sobre acceso al conocimiento de Carolina Botero. InternetActiva, Disponible en https://www.youtube.com/watch?v=ZUvH2-U_SSU

[47] Busaniche, María Beatriz. *Propiedad intelectual y derechos humanos. Tensiones existentes entre la Ley 11.723 y el marco constitucional de los derechos culturales en Argentina.* Facultad Latinoamericana de Ciencias Sociales (FLACSO). Tesis de Maestría en Propiedad Intelectual. Buenos Aires, Argentina. Junio, 2013, pág. 140.

no sólo ponen al alcance de docentes y estudiantes grandes volúmenes de información, sino que promueven el desarrollo de destrezas y habilidades esenciales como son la búsqueda, selección y procesamiento de información, así como la capacidad para el aprendizaje autónomo. También amplían las fronteras del aprendizaje al poner a disposición nuevos recursos así como la forma para aprender con otros, incluyendo comunidades remotas. Dicho de otra manera, las TIC son una herramienta esencial para tener acceso a la sociedad del conocimiento. El grado en que los países incrementen su infraestructura de TIC y se apropien de ellas contribuirá a determinar la calidad de vida de los ciudadanos, las condiciones de trabajo y la competitividad global de la industria y los servicios.

Aunque en dicho documento no se hablaba en concreto de internet, la visión de las TIC como un potenciador de la educación era evidente y suponía continuar los programas de distribución de computadores para las escuelas que, además, hablaba de la necesidad de crear contenidos, distribuirlos y usarlos.[48] El Ministerio de Educación operativizó esta política a través de del "Programa Nacional de Uso de Medios y TIC",[49] que también se ha visto apoyado por otros organismos públicos, especialmente el Ministerio de las Tecnologías de la Información y las Comunicaciones (en adelante, MinTIC), y ha generado programas de capacitación a docentes, desarrollado una "Estrategia Nacional de Recursos Educativos Digitales", fortalecido el portal de contenidos digitales "Colombia Aprende", proveyendo recursos públicos para el desarrollo de proyectos de investigación, y mejorado el acceso a la infraestructura tecnológica.[50] Los proyectos son ambiciosos y también son objeto de importantes críticas como:

- La producción y puesta a disposición de contenidos apuesta por el acceso público (leerlos, usarlos), no abierto (permisos adicionales como copiar, modificar, imprimir, etc.). Que sean públicos ya es más amplio que lo que se puede hacer con contenidos sujetos al sistema tradicional de derecho de autor (todos los derechos reservados). No obstante, las usuarias y los usuarios se encuentran limitados de aprovechar el potencial

[48] Esta iniciativa ha sido propulsora de un proyecto del MinTIC , que desde el año pasado distribuye tabletas en las escuelas.

[49] En concreto, se debe mencionar el Conpes 3670, que establece la ampliación y formación de alto nivel en relación con las TIC dentro del ámbito escolar mediante prácticas educativas que se apropien adecuadamente de las tecnologías a través del portal de internet del Estado colombiano "Colombia Aprende", sobre asignaturas como matemáticas, ciencias naturales y lenguajes. Asimismo, el documento establece que se ampliará el uso de las tecnologías con el objetivo de producir y distribuir contenidos digitales en educación básica y superior, la capacitación de docentes en uso y desarrollo de contenidos educativos digitales, y plantea la creación de un *Centro de Innovación Educativa Nacional (CIEN)*, coordinado por el Ministerio de Educación Nacional. Este último documento también señala lineamientos para cumplir con la meta del actual Gobierno Nacional de "llevar internet a todo el país". Para ello se pretenden adelantar, fortalecer y seguir desarrollando programas y planes tales como los kioskos vive digital, el proyecto nacional de conectividad de alta velocidad, entre otros, que pretenden dotar de acceso a internet a todos los municipios del país y, en especial, a las zonas rurales y resguardos indígenas. Así, se espera lograr un servicio universal de las tecnologías a lo largo del país.

[50] Informe *Gasto público en la educación de América Latina ¿Puede servir a los propósitos de la Declaración de París sobre los Recursos Educativos Abiertos?* Elaborado por Amalia Toledo de la Fundación Karisma, comisionado por la UNESCO, 2014, pág. 43 y siguientes. Disponible en http://www.unesco.org/new/fileadmin/MULTIMEDIA/FIELD/Montevideo/pdf/CDCI1-Karisma-ES.pdf.

de las TIC o de lo que pueden pedir cuando los recursos son producidos con dinero público.

- El suministro de tabletas que se ha hecho en los últimos meses es una acción que ha sido fuertemente criticada, entre otras cosas, porque estos equipos no aparecen asociados a ningún proceso pedagógico o de apoyo a las y los docentes, ni se producen contenidos educativos aptos para los mismos.[51]

Existe la sensación de que aunque las mejoras en el acceso a las TIC en Colombia son evidentes y pese a los grandes esfuerzos, su uso sigue siendo limitado y reducido al modelo de educación tradicional, sin que se esté aprovechando para la innovación en pedagogía y el aprendizaje.[52] Un análisis más completo de este tipo para Colombia, pero también para Argentina, Paraguay, Chile y Uruguay, puede encontrarse en el Informe Gasto público en la educación de América Latina ¿Puede servir a los propósitos de la Declaración de París sobre los Recursos Educativos Abiertos?

En materia de educación superior, el Ministerio de Educación colombiano y Colciencias, junto con otros 8 países, formaron parte de la iniciativa regional La Referencia. Esta iniciativa busca responder a la necesidad de visibilizar la información científica como un insumo crucial para el desarrollo científico y tecnológico de los países.[53] Además, sirve para potencializar el ejercicio de los derechos a la educación, al acceso al conocimiento y a la ciencia de la ciudadanía. La Referencia tiene como fin último recoger y divulgar en un mismo sitio la producción científica de la región, planteando la producción científica (artículos publicados en revistas científicas y tesis de postgrado) como un bien público regional. Aunque no es una política estatal, la participación de las autoridades de ciencia de 9 países de la región (y abierta a la afiliación de otros) seguramente supondrá un importante impulso en la región.

Ahora bien, también desde el Ministerio de la Tecnología de la Información y las Comunicaciones se han desarrollado lineamientos de política pública, que buscan impactar en temas de educación y cultura a través de programas para lograr el acceso a internet y el uso educativo de las TIC. Estos documentos son denominados documentos CONPES (realizados y presentados por el Consejo Nacional de Política Económica y Social del Departamento Nacional de Planeación).

En este sentido, las directrices de política pública sobre el acceso a internet y uso de TIC en el fortalecimiento del sector educativo se consagran en el Documento CONPES 3769 del 16 de septiembre de 2013 y el Documento CONPES 3670 del 28 de junio del 2010. El primero de ellos reconoce la importancia de ampliar los programas de telecomunicaciones sociales y de

[51] Entre los logros del Plan Vive Digital del Gobierno Nacional, se destaca la entrega de dispositivos (computadores y tabletas) para instituciones públicas de educación. Entre los años 2010-2014 ha alcanzado cerca de los dos millones. Véase http://www.vivedigital.gov.co/logros-plan/logro.php?lg=11.

[52] Ospina Mejía, Oswaldo (2012). "TIC en educación: más allá de su integración en el currículo". Disponible en http://www.colombiadigital.net/entorno-tic/especial-del-mes/especial-marzo/item/1467-tic-eneducaci%C3%B3n-m%C3%A1s-all%C3%A1-de-su-integraci%C3%B3n-en-el-curr%C3%ADculo.html.

[53] La región está bastante rezagada como lo demuestra el mapa http://www.nature.com/srep/2012/121129/srep00902/fig_tab/srep00902_F1.html.

implementar 800 tecnocentros nacionales. El segundo, por su parte, establece los lineamientos de política sobre los programas de acceso y servicio universal a las TIC. Queda, en todo caso, una discusión centrada más sobre la visión de infraestructura en internet, que del ejercicio pleno del derecho a la educación en el entorno digital.

Aunque hasta aquí hemos descrito el caso colombiano, el panorama será posiblemente muy similar en otros países de la región en que, especialmente el derecho a la educación, se está vinculando fuertemente con políticas de agenda digital.[54]

2.2. Cultura

Antes hemos visto que, al menos, existe una visión de proyectar una política pública sobre educación y tecnologías. Por el contrario, en materia de cultura y su relación con internet es casi inexistente el desarrollo institucional y de políticas públicas. Sin embargo, podemos resaltar dos CONPES:

El Documento CONPES 3162 del 10 de mayo del año 2002, en donde se expone *la política orientadora del Plan Nacional de Cultura de 2001-2010*, establece que "las redes de instituciones y servicios culturales (bibliotecas, museos y archivos) no están suficientemente conectadas. Además, la mayoría del sector no se ha apropiado de las nuevas tecnologías para acceder y generar información". La propuesta consiste en que el Gobierno Nacional, en cabeza del Ministerio de Cultura, articule la agenda de conectividad del sector cultura aprovechando las tecnología de la información existentes, como internet.

Igualmente, esta política pública resalta la necesidad de generar alianzas con el sector comunicaciones, fomentando la televisión pública cultural y la cinematografía, considerando que son elementos que permiten fortalecer la memoria e historia del país a través de la democratización de las nuevas tecnologías y la formación de centros de producción comunitaria.

Por otra parte, el Documento CONPES 1063 del 26 de abril de 2010, sobre *la política nacional de promoción de las industrias culturales del país*, se enfoca más en generación de nuevos modelos de negocio utilizando las TIC. Así, propone la articulación con el MinTIC para fortalecer procesos de financiamiento, desarrollo empresarial y aprovechamiento del potencial cultural local a través de programas como MiPyme Digital.

Como vemos, no existe lineamiento de política pública que trata el tema de acceso a la cultura a través de las TIC o su garantía y ejercicio pleno en el entorno digital. El enfoque apunta a una ruta para cubrir la insuficiencia de articulación tecnológica en el sector cultura (que por demás, se trata de un lineamiento del año 2002) y al fomento empresarial utilizando las tecnologías.

[54] Es el caso de la Estrategia Digital Nacional que habla de acceso a cultura, salud, educación, etcétera, a través de las tecnologías de la información. Para consulta, véase http://www.pediatria.gob.mx/rencue_estradigi.pdf.

2.2.1. Bibliotecas

En el sector cultural quizá el espacio donde mejor coinciden la tecnología con el ejercicio de derechos como la educación y el acceso a la cultura es en las bibliotecas. Las bibliotecas enfrentan importantes retos derivados del potencial de las Tecnologías para la Información y las Comunicaciones en el desarrollo de su misión. Así, en el Documento CONPES 3162 se contemplan las bibliotecas públicas como instituciones fundamentales incluidas en las políticas nacionales de información, cultura y democratización del conocimiento.[55]

Siguiendo con la exposición de documentos de política pública, se debe resaltar que, si bien no tiene relación con internet, existe un lineamiento relacionado con bibliotecas y el acceso a la cultura. Éste es el Documento CONPES 3222 del 24 de abril del año 2003 sobre lineamientos del Plan Nacional de Lectura y Bibliotecas. Allí se consagra que las bibliotecas como "escenarios fundamentales para el desarrollo de una sociedad [...r]esultan indispensables en la promoción de la lectura y el mejoramiento de la calidad de la educación al poner al servicio de las comunidades los libros y demás servicios culturales y educativos".

Sin duda

> *La constante evolución de las tecnologías de la información y comunicaciones hace que las instituciones culturales afronten nuevos retos, y oportunidades con relación al acceso a la información, la formación de públicos, la organización física y tecnológica de espacios. En breve, las tecnologías están transformando el lugar de la biblioteca en el mundo y el mundo de las bibliotecas[56].*

Sin embargo, en Colombia las bibliotecas tienen problemas legales para desarrollar su misión porque solo hay una excepción legal al derecho de autor que las beneficia (copia para preservación).[57] Más aún, bajo algunas interpretaciones sobre el préstamo público se ha dicho que este depende de la voluntad del autor.[58] Esta situación hace que el marco legal de las

---

[55] Jaramillo, Orlanda; Álvarez Zapata, Didier & Moncada, Daniel. Políticas públicas para bibliotecas públicas: una propuesta de soluciones locales a problemas globales. *Investig. bibl* [online]. 2005, vol.19, n.39, pags. 13-27. ISSN 0187-358X. Disponible en
[55]http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2005000200002&lng=es&nrm=iso.

[56] Tomado de los encuentros **Contexto Digital,** realizados cada año por el Banco de la República y la Biblioteca Nacional, en donde expertos nacionales e internacionales aportan sus conocimientos en las distintas líneas de desarrollo del ámbito digital que están relacionadas con la labor cultural colombiana. Disponible en http://www.banrepcultural.org/contexto-digital/inicio.

[57] **Artículo 38º (Ley 23 de 1982)-** Las bibliotecas públicas pueden reproducir para el uso exclusivo de sus lectores y cuando ello sea necesario para su conservación, o para el servicio de préstamos a otras bibliotecas, también públicas, una copia de obras protegidas depositadas en sus colecciones o archivos que se encuentran agotadas en el mercado local. Estas copias pueden ser también reproducidas, en una sola copia, por la biblioteca que las reciba en caso de que ello sea necesario para su conservación, y con el único fin de que ellas sean utilizadas por sus lectores. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431.

[58] Al respecto, el *Manual de derecho de autor* (2010), publicado por la Dirección Nacional de Derecho de Autor, cita que "la facultad exclusiva del autor o del titular del derecho a autorizar la puesta a disposición del público, de una obra o de sus copias." Pág. 42 Disponible en http://www.derechodeautor.gov.co/documents/10181/331998/Cartilla+derecho+de+autor+(Alfredo+Vega).pdf/e99b0ea4-5c06-4529-ae7a-152616083d40.

bibliotecas en el mundo análogo esté desactualizado y, en consecuencia, ni qué decir de la situación para el mundo digital.

En Colombia, las bibliotecas y las/os bibliotecólogas/os se han convertido en uno de los grupos de la sociedad civil que, colectivamente, están pidiendo información, comprensión y espacios de participación para buscar equilibrios con la misión de su oficio, relacionada con derechos como educación, cultura y acceso a la información. Están participando en discusiones de política pública sobre obras huérfanas, excepciones y limitaciones, depósito legal digital, etcétera.

La participación del GRULAC o Grupo de América Latina y el Caribe en la OMPI dentro de la agenda para el desarrollo, que tiene como uno de sus puntos la creación de garantías en el mundo para este oficio (bibliotecas y archivos), ha sido clave. El trabajo de GRULAC busca impulsar el diseño de un documento jurídicamente vinculante para los Estados, que brinde beneficios a bibliotecas y archivos para solucionar, en parte, los problemas que un sistema centrado en la protección al derecho de autor ha generado en la defensa y protección de derechos humanos, como el del acceso a la cultura.

Más allá de este empuje regional (en el que son más activos países como Brasil, Ecuador y Uruguay, que otros de la región), en Colombia lo que vemos son iniciativas muy puntuales para aprovechar las tecnologías y su potencial para generar acceso al conocimiento, a la cultura. Este es el caso de proyectos de bibliotecas digitales como:

La Biblioteca Virtual

La ***Biblioteca Digital*** de la Biblioteca Luis Ángel Arango, creada en el año 1996, contiene obras

> *[E]n su mayoría sobre Colombia o de autores colombianos, que pueda ser consultada por Internet desde cualquier parte del país o del mundo. Contiene materiales en diferentes formatos, organizados en colecciones temáticas. En ella puede encontrar libros, imágenes, archivos sonoros y de video, páginas interactivas, exhibiciones en línea, proyectos temáticos, y materiales educativos.*[59]

La Biblioteca Virtual establece que la reproducción de las obras allí contenidas es permitida y gratuita. Sin embargo, el uso de las obras se limita a que sea un solo ejemplar para uso privado y sin fines de lucro.[60]

La biblioteca digital también contiene la ***Hemeroteca Digital Histórica***, "en donde se encuentran digitalizados una serie periódicos del siglo XIX (hasta el momento más de 150) [...]

[59] Tomado de la página explicativa de la biblioteca del Banco de la República. Disponible en http://www.banrepcultural.org/blaavirtual/quees.
[60] A esta biblioteca digital se puede acceder en el siguiente enlace http://www.banrepcultural.org/blaavirtual/indice.

Hay una amplia diversidad de periódicos, desde prensa política y económica, hasta prensa literaria y humorística".[61]

Biblioteca Digital de la Biblioteca Nacional de Colombia

Esta Biblioteca compila obras que contiene patrimonio bibliográfico y documental que se encuentran en la Biblioteca Nacional, la Biblioteca Luis Ángel Árango, la Universidad Nacional de Colombia, la Biblioteca Pública Piloto de Medellín y el Archivo Histórico de Medellín. Se ha establecido que este trabajo colaborativo tiene como objetivo *"concentrar en un único espacio web las colecciones digitales realizadas por instituciones culturales de carácter público o privado para facilitar la búsqueda, investigación y acceso a colecciones digitales"*.[62]

Allí no solo se encuentran digitalizadas obras de carácter histórico, sino también colecciones y exposiciones virtuales, mapas, videos, prensa, partituras de música, entre otros. Incluso en el marco del trabajo de la Biblioteca, se tiene un *Laboratorio Digital*[63] que cuenta con diversos servicios para la ciudadanía, tales como infraestructura tecnológica, talleres gratuitos y bases de datos especializados y cursos virtuales.[64]

Biblioteca Digital de Bogotá

A finales del año 2013, el Ministerio de Cultura y la Secretaría de Cultura del Distrito de Bogotá, junto a la Biblioteca Nacional de Colombia, comenzaron la construcción de un proyecto denominado ***Biblioteca Digital de Bogotá***. El mismo fue propuesto como un espacio digital en donde se han venido recopilando obras literarias, fotografías, mapas, obras de teatro, entre otras, que tuvieran relación con la ciudad de Bogotá, o que hubiesen sido escritas o creadas por autores bogotanos. Se pretende que esta biblioteca digital sobre Bogotá sea una alternativa que facilite el conocimiento, la preservación de la memoria e información histórica sobre la capital, en donde cualquier persona, desde cualquier dispositivo, pueda acceder a estas obras de manera gratuita.

La Biblioteca Digital de Bogotá cuenta, principalmente, con obras que se encuentran en el dominio público o cuyos derechos están en cabeza del Distrito de Bogotá o de la Biblioteca Nacional de Colombia. Sin embargo, no todas las obras que formarán parte de la colección tienen estas calidades, puesto que en algunos casos sus autores o titulares aún están vivos, por lo tanto, sus derechos siguen vigentes. De esta manera, se está gestionando el uso particular de dichas obras a través del licenciamiento *Creative Commons*, en el que la Fundación Karisma ha venido prestando asesoría legal frente a temas de derecho de autor.

[61] Disponible en http://www.banrepcultural.org/blaavirtual/hemeroteca-digital-historica/all.
[62] Descripción tomada de la página web de la Biblioteca Digital, cuyo enlace se menciona en el párrafo siguiente.
[63] Para conocer más sobre el trabajo que adelanta el Laboratorio Digital, se puede acceder en el siguiente enlace http://www.bibliotecanacional.gov.co/content/LABN.
[64] A esta biblioteca digital se puede acceder en el siguiente enlace http://www.bibliotecanacional.gov.co/content/biblioteca-digital.

Vale señalar que este proyecto aún se encuentra en desarrollo.[65] El fin último de esta biblioteca es que con la colección de distintas obras sobre la capital de la República se facilite y se preserve la memoria de la ciudad, sus autores y se contribuya a garantizar el acceso a la cultura bogotana.

3. Legislación

En la región, a excepción de Brasil, que a través del "Marco Civil" estableció una regulación de Internet desde una aproximación en derechos humanos, en general los desarrollos legales sobre Internet (siguiendo la tendencia mundial) han estados mediados por discursos basados en el miedo y fragmentando en temas.[66] Colombia no ha sido la excepción. Sin embargo, en el último año hemos visto que el cruce del ejercicio de derechos humanos e Internet, particularmente en lo relacionado con educación y cultura, ha resistido tal tendencia al menos en temas muy puntuales.

Durante la última legislatura del Congreso Colombiano (2013-2014), el *Grupo de Derecho, Internet y Sociedad* de la Fundación Karisma estuvo realizando un monitoreo legislativo sobre los proyectos de ley que impactan los derechos de la ciudadanía en el entorno digital. Tal monitoreo ha permitido dar seguimiento a iniciativas que de alguna manera pretendían regular el ejercicio de derechos y el acceso a internet, el manejo de datos sensibles de los ciudadanos y ciudadanas, y relativos a la competencia e infraestructura de las telecomunicaciones.[67]

3.1. Ley 1680 de 2013

En noviembre de 2013 entró en vigor la Ley 1680 de 2013, que busca "garantizar a personas ciegas y con baja visión el acceso a la información, a las comunicaciones, al conocimiento y a las tecnologías de la información y las comunicaciones". Dicha ley pretende hacer efectiva la inclusión social de más de 1.3 millones de colombianas y colombianos con limitaciones visuales que solo contaban con un libro en formato accesible por cada mil libros publicados para las personas que ven.[68] Para la consecución de este objetivo, la ley dispone como obligación del Estado la adquisición de un software lector de pantalla a través de una licencia país. Este software deberá ser implementado en todas las entidades públicas del país, incluyendo bibliotecas públicas, establecimientos educativos públicos y centros culturales, y los establecimientos abiertos al público que presten servicios de internet o telecentros en al menos un terminal.

---

[65] Al encontrarse en desarrollo, la página web del proyecto se encuentra en versión beta y no está disponible al público.
[66] Para más información, se puede consultar la columna de opinión de Carolina Botero en el diario *El Espectador*, del 24 de abril de 2014. Disponible en http://www.elespectador.com/opinion/marco-civil-abre-netmundial-columna-488777.
[67] Para conocer más de esta iniciativa, véase http://karisma.org.co/?p=4295.
[68] Censo General 2005: Discapacidad, personas con limitaciones permanentes. 2006. pág. 33. Recuperado el 2 de septiembre de 2012 del sitio web del Departamento Administrativo Nacional de Estadística (DANE), disponible en http://www.dane.gov.co/files/censo2005/discapacidad.pdf.

De igual manera, esta ley establece como un deber del Estado y de los particulares que ejerzan funciones públicas que las páginas web cumplan con normas técnicas y directrices de accesibilidad y usabilidad que defina el MinTIC.

Con el fin de salvaguardar la autonomía e independencia de las beneficiarias y beneficiarios, el ejercicio de sus derechos, en particular a la educación y a la cultura, y el funcionamiento del software, la ley también prevé una excepción y limitación al derecho de autor. Tal excepción permite que personas con discapacidad visual puedan hacer formatos accesibles de las obras ya publicadas, que pueden ser distribuidos, comunicados al público –incluso a través de Internet– y que las obras puedan ser traducidas, adaptadas o transformadas al modo, medio o formato que elijan, sin que ello constituya una infracción al derecho de autor. Conviene mencionar que no es del todo claro si las bibliotecas, archivos y universidades están facultadas a realizar directamente las acciones antes mencionadas, toda vez que la ley solo menciona a las beneficiarias y beneficiarios.

Dando alcance a la Ley 1680 de 2013 y en desarrollo del Plan Vive Digital adelantado por el MinTIC, el gobierno colombiano a través de una licitación pública adquirió una licencia país por cuatro años del software de lectura de pantalla Jaws y del magnificador Magic, que se ha denominado como el programa ConVerTIC. El software adquirido puede ser instalado "por cualquier persona natural o jurídica en todo el territorio nacional, con descarga ilimitada, actualizaciones permanentes y soporte sin costo alguno" durante los cuatro años del programa, previo a un registro en línea.[69] De acuerdo con la información disponible en la página de *ConVerTIC*, a la fecha, el software ha sido descargado aproximadamente 85.919 veces. El MinTic está efectuando capacitaciones sobre el uso del software y gestiona una campaña de promoción del mismo.

3.2. Tratado de Marrakech

Aunque Colombia suscribió el *"Tratado de Marrakech para facilitar el acceso a las obras publicadas para las personas ciegas, con discapacidad visual o con otras dificultades para acceder al texto impreso"* de la Organización Mundial de la Propiedad Intelectual el pasado 28 de junio de 2013, aún no lo ratifica. Pese a las consultas realizadas por parte de la Fundación Karisma a la Cancillería, el proceso de ratificación aún se encuentra en discusión interna y no ha sido posible establecer cuándo se presentará ante el Congreso colombiano.

La ratificación de este tratado supondría la necesidad de modificar en algunos aspectos la recién adoptada Ley 1680 de 2013, principalmente en lo que se refiere a las beneficiarias y beneficiarios, toda vez que los definidos por el tratado abarca a las personas ciegas, con discapacidad visual y también a aquellas que no pueden acceder al texto impreso (por ejemplo, aquellas que no pueden sostener un libro). Dicho instrumento es mucho más amplio que la ley nacional, que solo contempla a las personas ciegas y con baja visión.

[69] Para consultar más información sobre el Programa ConverTIC, véase http://www.vivedigital.gov.co/convertic/,

A su vez, deberá complementarse la excepción y limitación al derecho de autor en lo que se refiere al intercambio transfronterizo de ejemplares y la elusión de medidas tecnológicas de protección que establece el mencionado tratado. En la región, 15 Estados ya han suscrito este instrumento, sin que hayan ratificado el mismo.[70] Se sabe que en Uruguay el proceso de ratificación se encuentra en un estado avanzado.[71] En el mundo, al día de hoy, India ha ratificado el Tratado; en Latinoamérica, El Salvador terminó el proceso interno de ratificación del tratado.[72]

3.3. Ley 1341 de 2009

Por otro lado, en Colombia se cuenta con la Ley 1341 de 2009, que establece los principios rectores frente a la formulación de políticas públicas sobre asuntos relacionados con las Tecnologías de la Información y las Comunicaciones, y el acceso a la sociedad de la información. En virtud de esta legislación, se consagra como principio orientador la obligación del Estado de priorizar el uso y acceso a las TIC en la producción de bienes y servicios relacionados con la educación. En este sentido, se establece que los servicios básicos de las TIC deberán estar a disposición para el ejercicio pleno del derecho a la educación, en especial para las poblaciones más vulnerables, es decir, personas de los estratos socioeconómicos más desfavorecidos y las poblaciones rurales, con el fin de que las TIC sean un mecanismo para el alcance de una educación integral.

Frente a la promoción de uso y acceso de las TIC, esta ley establece que se deberá configurar una articulación entre el MinTIC y el Ministerio de Educación Nacional, con el objetivo de poner en marcha planes de alfabetización digital, capacitación a establecimientos educativos y la inclusión de las TIC en todo el sistema educativo nacional.

4. Proyectos de Ley

En el cruce entre derechos y tecnología podemos hablar de dos tipos de proyectos de ley: (1) los que pasan sin pena ni gloria, y (2) los que han sido objeto de fuertes debates y una gran coyuntura.

4.1. Proyectos que han pasado sin pena ni gloria

Durante el periodo legislativo 2010-2014, en el Congreso de la República se presentaron iniciativas que aunque no tenían como eje principal la garantía del derecho a la educación y el acceso a la cultura, su implementación sí habría afectado estos derechos de manera favorable

[70] Para más información sobre los Estados que han suscrito y ratificado el Tratado de Marrakech, véase http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=843.
[71] Comunicado de prensa de la Presidencia de la República de Uruguay. Declaración del ministro de Educación y Cultura (MEC), Ricardo Ehrlich. Disponible en http://www.presidencia.gub.uy/comunicacion/comunicacionnoticias/tratado-de-marrakech.
[72] Así lo informa la Asamblea Legislativa de El Salvador, véase http://www.asamblea.gob.sv/noticias/archivo-de-noticias/asamblea-legislativa-pionera-en-el-mundo-y-primera-en-america-latina-en-ratificar-tratado-de-marrakech.

en el entorno digital. Sin embargo, los proyectos que reseñamos pasaron por el congreso colombiano sin pena ni gloria, en la medida en que fueron archivados por falta de debate legislativo.

Los proyectos de ley que se presentaron fueron los siguientes:

4.1.1. Implementación de un marco jurídico para la universalización de la telecomunicaciones (incluyendo internet)

Este proyecto buscaba garantizar el acceso a internet para poblaciones vulnerables a través de conexiones comunitarias. El mismo es importante en la medida en que hoy por hoy el ejercicio de muchos derechos se relaciona con el acceso a Internet. Por ejemplo, cada día es más común que los trámites para acceder a cupos en las escuelas o al carnet que garantiza la prestación del servicio de salud pasen por un trámite en línea.

4.1.2. La creación de una campaña de alfabetización digital nacional

La propuesta, en este caso, era que el servicio social que las y los estudiantes del nivel 11 de la educación media deben hacer como requisito de grado pudiera cumplirse alfabetizando a personas mayores de 40 años en el uso de Internet y las nuevas tecnologías.

4.1.3. La garantía de acceso a internet como derecho fundamental

Esta iniciativa pretendía la masificación del uso del servicio de internet. Así, buscaba establecer el "acceso a internet" como un derecho de rango constitucional. Es importante resaltar que el proyecto no fue suficientemente considerado, ni siquiera fue debatido una vez (aunque era la segunda vez que se presentaba un proyecto así en el Congreso).

Iniciativas de este tipo también han tenido curso en la región. No obstante, solo en México se observa un avance legislativo. Por ejemplo, la reforma constitucional de 2013 modificó su artículo 6, estableciendo el acceso a internet como un derecho humano.[73] También hay que resaltar el caso de Costa Rica y un fallo de la Corte que estableció el acceso a internet como un derecho fundamental.[74]

Los pocos ejemplos de proyectos de ley antes reseñados –que como dijimos fueron archivados– tenían vocación de ampliar y ofrecer un marco garantista para el ejercicio de derechos humanos en los entornos digitales. No obstante, este panorama nos permite concluir que las iniciativas legislativas sobre estos derechos son escasos y los pocos que se presentan

[73] Sobre la iniciativa de reforma constitucional en México, véase http://eleconomista.com.mx/entretenimiento/2013/01/07/promueven-establecer-acceso-internet-como-derecho-humano.

[74] Sobre el fallo de Costa Rica, véase http://www.nacion.com/2010-09-08/ElPais/NotasSecundarias/ElPais2514038.aspx o http://www.gacetaconstitucional.com.pe/noticias-const/VerDetNotRot.php?idnot=203.

no cuentan con la suficiente voluntad política para convertirse en ley. En cambio, los proyectos más comunes están relacionados a redes y servicios de telefonía móvil, a la regulación de la competencia entre las empresas que prestan estos servicios y a infraestructura de telecomunicaciones.

4.2. Proyectos que han sido objeto de importantes polémicas

En este ámbito, el ejemplo central ha sido un conjunto de 4 proyecto de leyes, conocidas a nivel nacional como la saga de la **Ley Lleras**, que se han presentaron entre los años 2011 y 2013 y cuyo eje transversal es la reforma al derecho de autor como obligación del Tratado de Libre Comercio (TLC) entre Colombia y los Estados Unidos. A continuación reseñamos los 4 proyectos de leyes.

- **Ley Lleras 1:** Para exponer el tema usaremos esencialmente el texto de la Fundación Karisma, realizado por Carlos Cortés, *"El debate pendiente en Colombia sobre la protección de derechos de autor en Internet, el caso de la 'Ley lleras".*[75]

  El lunes 4 de abril de 2011, el entonces Ministro del Interior y de Justicia, Germán Vargas Lleras, llegó a la Secretaría General del Senado, acompañado por un grupo de artistas, para presentar un proyecto de ley, que en las redes sociales sería conocido como la Ley Lleras. En ese puesta en escena el Ministro aseguró que castigaría fuertemente a los piratas. Sin embargo, 16 de los 19 artículos versaban sobre la creación de un mecanismo extrajudicial de retiro de contenidos digitales –videos, música, textos–, que suben o transmiten las usuarias y los usuarios, que supuestamente infringen los derechos de autor. La amenaza de cárcel a los piratas, a la que se refería Vargas Lleras, estaba en uno de los artículos finales del proyecto. Pero realmente no estábamos ante un nuevo delito, sino que en el proyecto se repetía –si acaso de manera más específica– lo que ya estaba vigente en el Código Penal colombiano.

  Cortés afirma que:

  > *[A]l presentar el proyecto de ley rodeado de artistas, Vargas Lleras no sólo estaba tratando de blindar de legitimidad la reforma –que hacía parte de las obligaciones adquiridas en el Tratado de Libre Comercio–, sino que también le daba un enfoque distinto al que realmente tenía. Antes que meterse en la espinosa discusión sobre el equilibrio de derechos fundamentales en Internet, el gobierno quería mantener el debate en términos de la subsistencia de nuestros músicos, actores y productores.*[76]

[75] Este documento puede consultarse en http://karisma.org.co/wp-content/uploads/2013/04/Paper1ElCasoLeyLleras.pdf.
[76] Ibíd.

El proyecto de ley se hundió en el segundo debate, más por falta de voluntad política frente a un proyecto que había perdido el favor popular y se había convertido en una "papa caliente", que por una discusión de fondo de los temas que trataba. En el caso de la 'Ley Lleras', los promotores invocaron la ayuda del Congreso para frenar la piratería, un daño que jamás acreditaron. E incluso suponiendo que el daño existiera, la pertinencia e idoneidad de la solución que propusieron para detenerlo era reprochable a la luz de otros derechos fundamentales. Bloquear contenidos en un medio de dos vías como es Internet, el medio en que la gente se informa, consume contenidos y los comparte, no es cuestión menor, teniendo el potencial de afectar derechos como el de educación, el acceso a la cultura y a la ciencia, a la información, etcétera.

El debate sobre la protección de los derechos de autor en Internet se planteó sobre supuestos que deben examinarse para el caso colombiano, como la piratería y su relación con el uso de Internet, la cuantificación de los daños, los usos permitidos de material protegido y el florecimiento de la cultura libre en el país. Dar este debate no implica, de ninguna manera, hacer una apología a la piratería o desconocer el Tratado de Libre Comercio con Estados Unidos.

- **Ley Lleras 2**. En 2012, el gobierno colombiano presentó un nuevo proyecto de ley que, en este caso, se refería al resto de obligaciones pendientes del capítulo de propiedad intelectual del TLC con EEUU (diferentes del mecanismo para retiro de contenidos de Internet). En esta oportunidad, el Congreso aprobó en 20 días tal reforma. De la aprobación de esta ley dependía que el TLC con EEUU entrara en efecto. No obstante, durante la corta discusión que hubo respecto a esta iniciativa, la sociedad civil planteó la necesidad de una reforma integral en donde se consideraran, de un lado, las obligaciones con EEUU y, de otro, las necesidades de la sociedad colombiana en la nueva era digital. El argumento estaba apoyado en el reconocimiento de que por medio de acuerdos comerciales internacionales se promoviera el fortalecimiento de los regímenes de derechos de autor, pero siempre dentro de un margen de libertad de acción para que los socios comerciales legislaran sobre los equilibrios necesarios (excepciones y limitaciones) que permitan salvaguardar otros derechos, entre ellos el de educación y cultura) dentro del dicho sistema. La exigencia de la sociedad civil de hacer ajustes, y especialmente de incluir excepciones y limitaciones necesarias para actualizar el sistema legal, fue ignorada. Con argumentos de forma y fondo se presentaron demandas ante la Corte Constitucional. La ley 1520 de 2012 fue declarada inexequible por la Corte Constitucional con argumentos de forma.

- **La Ley lleras 3.** En el segundo semestre de 2012, con el fin de allanar el camino para presentar una vez más el proyecto de cuyo contenidos se había conocido como *Ley lleras 1*, se inició el trámite de un proyecto de ley presentado por el representante Posada con el apoyo de la Dirección Nacional de Derecho de Autor. El proyecto proponía cinco excepciones que se habían identificado como las más necesarias. No obstante, dado que los textos no fueron conciliados con las comunidades beneficiarias

antes de entrar al Congreso y presentaron diversos problemas –sobre todo con los parodistas–. El proyecto, una vez más, quedó sepultó.

- **Ley Lleras 4.** Finalmente, el último proyecto de ley, que buscaba subsanar los problemas de trámite del proyecto Ley Lleras 2, fue presentando en 2013. El texto presentado que se presentó en aquel entonces era idéntico al segundo, reavivando las criticas que exigían considerar un espectro más amplio de derechos de las usuarias y los usuarios sin no limitarse únicamente a las necesidades de los titulares. En esta ocasión y debido al trabajo de la sociedad civil, el gobierno decide abrir espacio de socialización, cuyo fin era recoger comentarios, críticas y propuestas al respecto, impidiendo que el proyecto avanzara en el Congreso.

Hasta la fecha las obligaciones pendientes del TLC no han regresado al Congreso. Pese a que la sociedad civil y otros actores interesados consiguieron abrir el proceso (al menos en lo relacionado con Ley Lleras 2 y 4) para comentarios, la reforma pendiente a la legislación nacional de derecho de autor sigue más mediada por las presiones por el cumplimiento de compromisos internacionales que por la consulta interna para restablecer el equilibrio entre derechos.

5. Decisiones judiciales

No existen en Colombia suficientes fallos judiciales que den cuenta de la relación entre internet y los derechos a la educación y al acceso a la cultura. Sin embargo, hemos rastreado algunos casos que de una u otra forma abordan controversias sobre el ejercicio de derechos humanos en entornos digitales, sin que necesariamente haya una conexión directa con los derechos a la educación y el acceso a la información.

5.1. Corte Constitucional. Sentencia C-011 de 2013

MP. ALEXEI JULIO ESTRADA: Sentencia de inconstitucionalidad de la ley Lleras 2

La sentencia interesa en la medida en que se refiere al proceso legislativo conocido como Ley Lleras, pero no en su esencia en la medida en que no hay pronunciamientos sustanciales. La Ley 1520 de 2012, conocida como la Ley Lleras 2, tenía el objetivo de implementar las obligaciones adquiridas por Colombia en virtud del Tratado de Libre Comercio suscrito con Estados Unidos en materia de propiedad intelectual. Dicha ley fue declarada inexequible por la Corte Constitucional debido a vicios de trámite en el proceso legislativo.

La Corte Constitucional, en sede de tutela, ha conocido de algunos pocos casos en donde se han dirimido conflictos relacionados con la responsabilidad de los intermediarios en internet, correos electrónicos y el uso de redes sociales.[77] Los casos que se mencionan, consisten en

[77] En sede de tutela se refiere a casos contenciosos, que la Corte ha conocido y resuelto en razón a acciones de tutela interpuestas por las ciudadanas y ciudadanos por ver vulnerados sus derechos fundamentales. La Corte

situaciones en donde se alude la afectación del derecho a la educación en relación al uso de redes sociales y la exposición de datos personales sensibles. Por tanto, constituyen precedentes judiciales relevantes con respecto al ejercicio de derechos en el entorno digital en Colombia. Los casos son los siguientes:

5.2. Corte Constitucional. Sentencia T-713 de 2010

MP. MARÍA VICTORIA CALLE: Una institución educativa impone una matrícula condicional a un estudiante por unirse a un grupo de la red social Facebook, que apoyaba una solicitud de cambio de la rectora de la institución educativa.

Problema jurídico: ¿Viola una institución educativa el derecho al debido proceso, **a la educación** y a la igualdad de un estudiante, al habérsele adelantado un proceso en el que se le habría impuesto una sanción [matrícula condicional] por haber ingresado a un grupo en una red social que tenía por objeto atacar y difamar a la Rectora del Colegio donde estudiaba, a pesar de que el Colegio afirma no haber impuesto tal sanción?

Fundamentos de derecho: Los trámites sancionatorios en los contextos escolares deben respetar el derecho al debido proceso, so pena de que la misma quede sin validez y legitimidad por tal razón y por afectar el derecho fundamental a la educación. La amenaza de la imposición de una sanción por parte del colegio constituiría una violación a las reglas del debido proceso, por constituir medios de coacción y amedrentamiento, dependiendo del grado de afectación que tenga sobre un estudiante. Si se trata de una amenaza cierta, que se emplea para intimidar a un estudiante ilegítimamente en medio de un proceso, por ejemplo, se tratará de una violación a sus derechos fundamentales.

Decisión: Se concede el amparo solicitado al derecho a la educación, ordenándose al Colegio a que reciba al estudiante en su plantel educativo, si tal fuera su decisión. En tal caso, el Colegio debía tomar las medidas adecuadas y necesarias para asegurar que el estudiante pudiese culminar cabalmente sus estudios.

5.3. Corte Constitucional. Sentencia T-550 de 2012

MP. NILSON PINILLA PINILLA: Libertad de expresión y difusión del pensamiento en las redes sociales a través de internet.

Problema jurídico: ¿Vulneró una universidad los derechos al debido proceso, al libre desarrollo de la personalidad, a expresar y difundir los propios pensamientos y al trabajo del estudiante al habérsele adelantado un proceso disciplinario que concluyó con sanción de expulsión, como consecuencia de su conducta, por incluir en la red social Facebook

---

también conoce de acciones de inconstitucionalidad, que se trata de demandas que pueden ser interpuestas por cualquier persona, cuando consideran que una norma dentro del ordenamiento jurídico resulta contraria a los mandatos constitucionales.

comentarios en contra del Rector y la Secretaria Académica de la Facultad de Ciencia Política y Relaciones Internacionales de dicha universidad?

Fundamentos de Derecho: La opinión difundida por un medio de comunicación puede afectar los derechos fundamentales al buen nombre, a la intimidad u otros cuando se presentan más que una generación del debate, se demuestre la intención clara de ofender sin razón alguna o un ánimo de persecución desprovisto de toda razonabilidad.

La gravedad de la expresión proferida "no depende en ningún caso de la impresión personal que le pueda causar al ofendido, así como tampoco de la interpretación que éste tenga de ella, sino del margen razonable de objetividad que lesione el núcleo esencial del derecho". La libertad de expresión se aplica en internet del mismo modo que en otros medios de comunicación.

La Corte Constitucional concluye que las redes sociales no pueden garantizar un lugar para la difamación, el denuesto, la grosería, la falta de decoro y la descalificación.

Decisión: Se niega el amparo solicitado, toda vez que la expresión del demandante no estaba protegida por el derecho a la libertad de expresión. La Corte estimó que la expresión del estudiante fue ostensiblemente descomedida, irrespetuosa e injusta con la Universidad que le había capacitado y con las autoridades académicas que cumplían con sus deberes.

5.4. Corte Constitucional. Sentencia T-058 de 2013

MP. ALEXEI JULIO ESTRADA: Derecho a la educación, al *habeas data* y al buen nombre

Problema jurídico: ¿Desconoce una Universidad el derecho al *habeas data*, **a la educación** y al buen nombre al expedir las certificaciones académicas con anotación sobre los procesos disciplinarios adelantados en contra de la ex alumna por plagio, así como de las sanciones de suspensión del semestre académico y la expulsión de la Universidad?

Fundamentos de derecho: El consentimiento del titular de la información sobre el registro de sus datos se encuentra ligado a la necesidad de que aquel cuente con oportunidades reales para ejercer sus facultades de rectificación y actualización durante las diversas etapas de dicho proceso, que resultan vitales para salvaguardar los derechos a la intimidad y al buen nombre.

El objeto protegido del *habeas data* es el poder de control que tiene el titular de la información sobre quién y cómo administra la información que le concierne. Incluye también el poder del titular de conocer, actualizar, rectificar, autorizar, incluir y excluir información personal cuando sea objeto de administración en una base de datos. La autodeterminación informática es la facultad de la persona a la que se refieren los datos para autorizar su conservación, uso y circulación.

Decisión: La Corte tutelan los derechos fundamentales al habeas data, a la educación y al buen nombre de la demandante, ordenando a la Universidad que proceda a expedir una certificación de estudio a la tutelante, cuyo contenido se refiera únicamente a los detalles del programa académico, las asignaturas cursadas y las calificaciones obtenidas. De esta forma, la Corte asegura que no se consigne ningún elemento que le permita a un tercero inferir que estuvo la estudiante procesada y sancionada disciplinariamente por plagio.

5.5. Corte Constitucional. Sentencia T-040 de 2013

MP. JORGE IGNACIO PRETELT: Improcedencia de rectificación de información por parte de Google por cuanto presta servicio de búsqueda de información que hay en la red.

Problema jurídico: ¿Vulneraron la Casa Editorial El Tiempo S.A. y Google Colombia Ltda. los derechos fundamentales de *habeas data*, buen nombre, honra y dignidad humana al accionante al no eliminar de sus archivos y registros el artículo denominado "Los hombres de la mafia de los Llanos", en el que se nombra al mismo como integrante del cartel de estupefacientes?

Fundamentos de derecho: El derecho fundamental de *habeas data* invocado por el actor no era aplicable al caso, toda vez que la discusión se centraba en la información periodística difundida por un medio de comunicación en el ejercicio de la libertad de expresión, y en su rectificación, no de una información de una base de datos o archivos.

Los medios de comunicación como partícipes principales de la circulación de información deben ejercer su actividad conforme a la responsabilidad social que les exige la Constitución Política. Lo anterior implica que deben emitir información veraz e imparcial, distinguir los hechos de opiniones y, en caso dado, realizar las rectificaciones que se solicitan con fundamento.

Toda información presentada sin la suficiente exactitud, y que permite verificar la verdad de los hechos y evitar la confusión al lector, desconoce el principio de veracidad. En ese caso, procede un derecho de rectificación para exigir la protección de los derechos al buen nombre y a la honra.

Decisión: La Corte concede el amparo solicitado y ordena a la Casa Editorial El Tiempo S.A. que, manteniendo la noticia con la nota previa ya incluida, proceda a modificar el título de la noticia de modo que no induzca al error sobre la generalidad de los hechos que se describen. Asimismo, solicita que al final del artículo se modifique la frase que presenta el listado de quienes tienen investigación por los hechos referidos por el de *"personas presuntamente vinculadas"*. Por último, requirió incluir en la noticia un relato sucinto de los hechos y razones por las cuales se incluyó el nombre del demandante al final de la publicación y su relación con el contexto descrito en la noticia.

5.6. Corte Suprema de Justicia - Sala de Casación Penal. Proceso n° 33474. Sentencia del día 10 de febrero del año 2010

MP. MARÍA DEL ROSARIO GONZÁLEZ DE LESMOS: Definición de competencia en delitos cometidos en el ciberespacio.

Problema jurídico: ¿Cuál es el criterio que se debe aplicar para determinar la competencia en el caso de cometerse un delito a través del ciberespacio, en particular a través de la red social de Facebook?

Fundamentos de hecho: Cuando la conducta imputada se configure en el ciberespacio, utilizando redes sociales como Facebook, cuya cobertura es mundial y transnacional, no puede aplicarse el factor territorial para determinar la competencia del juez de conocimiento, por tanto, se debe acudir al artículo 43 del Código de Procedimiento Penal. En ese caso, la competencia del juez de conocimiento se fija entonces por el lugar donde se formule la acusación por parte de la Fiscalía General de la Nación, que será en donde se encuentren los elementos fundamentales de la acusación.

Decisión: La Corte define la competencia para el Juzgado Tercero Penal del Circuito Especializado de Bogotá, en razón a que la Fiscalía encontró que los elementos fundamentales de la acusación se encuentran en esta ciudad.

6. Casos no judiciales

También vale la pena resaltar casos, que si bien no han llegado a los estrados judiciales o aún están en proceso, han estado relacionados con internet y derechos como la libertad de expresión y al acceso a la información, en donde, aludiendo infracciones al derecho de autor, se han presentado el bloqueo de contenidos en internet. Los casos son los siguientes:

6.1. Caso de María Luisa Piraquive (Colombia)

Los primeros días del mes de febrero de 2014 se conoció a través de Youtube un video de la señora María Luisa Piraquive, fundadora del partido MIRA y de la Iglesia Ministerial de Jesucristo Internacional, en donde se escuchan distintas expresiones peyorativas contras las personas con discapacidad como *"que al púlpito no deben subir discapacitados"*.[78]

Dicho video fue retirado por Youtube en razón a reclamos de derecho de autor por parte de la Iglesia. Esto conllevo a que se registraran los primeros bloqueos de contenidos en internet al Diario La Patria, periódico de la ciudad de Manizales que dio a conocer el video, y a otras

[78] Para conocer el video que contiene las declaraciones censuradas, véase https://www.youtube.com/watch?v=VWmse-OmbNY.

cuentas que también difundieron el mismo. Por último, también fue bloqueado el video de la parodia titulada *"DiscriMIRAción"*,[79] realizada por el sitio web de parodias internautismo crónico.

Estos bloqueos se dieron en virtud de la legislación estadounidense *Digital Millennium Copyright Act* (DMCA), dado que Youtube es una empresa registrada en EEUU y es esta la ley aplicable. Dicha normativa requiere a que cualquier prestador de servicios en internet, que haya sido notificado por un titular de derechos sobre la violación a su derecho de autor por un contenido online, lo remueva de internet.

En este caso concreto, Carolina Botero ha dicho

> *[N]o son argumentos de infracción al derecho de autor los que motivan el bloqueo, lo que buscan es que no circule un video de una personalidad pública cuyos comentarios han generado la discusión sobre posibles infracciones al marco jurídico colombiano. Esto va más allá del derecho de autor si vemos lo que ha dicho la Corte Interamericana de Derechos Humanos sobre que hay especial protección respecto de las opiniones o informaciones sobre asuntos en los cuales la sociedad tiene un legítimo interés de mantenerse informada, de conocer lo que incide sobre el funcionamiento del Estado, o afecta derechos o intereses generales o le acarrea consecuencias importantes.*[80]

6.2. Caso Documental del Presidente Correa (Ecuador)

Este caso, al igual que el anterior, hace referencia a un bloqueo de contenidos en internet en virtud del DMCA. En esta oportunidad, el canal público "Ecuador Televisión", aludiendo infracción a sus derechos de autor, solicitó a Youtube el retiro de un video titulado *Rafael Correa: retrato de un padre de la Patria*, de los periodistas Santiago Villa y Gonzalo Guillen. Este video es un documental crítico sobre el presidente ecuatoriano que, entre otras cosas, denuncia posible nexos entre éste y la guerrilla colombiana de las FARC.[81]

6.3. Casos de documentales (Ecuador y Colombia)

Si bien este caso no está relacionado con Internet, sí se refiere al derecho al acceso a la cultura en medios masivos de comunicación. Asimismo, entendemos que puede hacerse extensible a la red. El primer caso trata de un documental titulado *La muerte de Jaime Roldós*, que cuenta la vida y muerte de este político y activista ecuatoriano, quien murió en circunstancias poco claras. La controversia se desató cuando, al momento de proyectar el documental en las salas de cine del país Supercines S.A., una de las mayores salas de proyección de películas de Ecuador se censura el documental en todas sus instalaciones. Esta empresa argumentó que, "*s*on una empresa de entretenimiento y no de comunicaciones" y que

[79] Para ver la parodia *"DiscriMIRAción*", véase https://www.youtube.com/watch?v=ZS2tdHIunY8.
[80] Columna de opinión de Carolina Botero. Diario *El Espectador* del 6 de febrero de 2014. Disponible en http://www.elespectador.com/opinion/libertad-de-expresion-vs-derecho-de-autor-columna-473357.
[81] Cortés Castillo, Carlos. "La DMCA, como forma de censura. el caso del documental del presidente Correa", *Dokumentos,* 3 de abril de 2013. Disponible en
[81]http://openbusinesslatinamerica.org/2013/04/03/la-dmca-como-forma-de-censura-el-caso-del-documental-del-presidente-correa/.

debido al alcance del contenido del mismo, catalogado por muchos como “fuerte políticamente” era una tema álgido para la historia de Ecuador.

Luego de la masiva crítica por parte de la ciudadanía y de la comunidad de artistas ante esta actuación de Supercines S.A., el Ministro Coordinador de Conocimiento y Talento Humano, Guillaume Long, envió una solicitud a la Superintendencia de Control de Poder de Mercado para que investigara a Supercines S.A.[82] Long aludía que la negativa a la proyección resultaba lesiva por responder a intereses políticos que terminaron por afectar la difusión del material. La Superintendencia citó a una audiencia reservada y confidencial al representante legal de la compañía, además de la presencia de un delegado de la Presidencia de la República.[83]

A la audiencia no acudieron los productores y el resultado fue una recomendación,invitando al Ministerio Coordinador de Conocimiento y Talento Humano y al Consejo Nacional de Cinematografía generar un diálogo con los operadores económicos propietarios de salas de cine en aquellas ciudades en las que sean el único proveedor de dicho servicio, para llevar adelante acciones que permitan la proyección de películas de producción nacional, coadyuvando, de esa manera, al desarrollo de la industria cinematográfica nacional.[84]

En un caso similar en Colombia, en diciembre de 2013, Cine Colombia canceló un acuerdo para pasar el tráiler del documental *No hubo tiempo para la tristeza*, arguyendo que las imágenes eran muy fuertes. El documental muestra los resultados del informe *Basta Ya*, realizado por el Centro de Memoria Histórica. Allí se muestra las memorias de varias víctimas del conflicto armado en Colombia de los últimos 50 años, y estadísticas e investigaciones rigurosas en torno al tema.[85]

6.4. Caso Compartir no es Delito (Colombia)

Un joven biólogo colombiano actualmente está enfrentando un proceso penal por compartir una tesis de maestría en internet. Todo comenzó cuando Diego Gómez, estudiante de biología de la Universidad del Quindío, encontró una tesis en un grupo de la red social Facebook sobre las salamandras del género *Bolitoglossa* en Colombia, y luego la colgó en la plataforma Scribd. Tiempo después, el autor de la tesis demandó penalmente a Diego Gómez por el delito de infracción al derecho patrimonial de autor y derechos conexos (artículo 271 Código penal

[82] Para conocer más detalles del contenido de la carta enviada por el Ministro, véase http://www.telegrafo.com.ec/al-hilo-de/item/supercines-explica-el-porque-no-quiere-proyectar-la-muerte-de-jaime-roldos.html.

[83] Para conocer más sobre la audiencia y el caso, véase http://www.scpm.gob.ec/la-superintendencia-de-control-del-poder-de-mercado-se-reunio-con-la-empresa-supercines-s-a/.

[84] Para conocer más sobre la Recomendación No. SCPM-DS-004-2014, véase http://www.scpm.gob.ec/recomendacion-no-scpm-ds-004-2014-la-superintendencia-de-control-del-poder-de-mercado-emitio-una-recomendacion-para-lograr-la-transparencia-en-el-mercado-del-sector-cinematografico/.

[85] Se puede ver más información al respecto en el siguiente enalce http://www.caracol.com.co/noticias/entretenimiento/cine-colombia-censuro-trailer-de-centro-de-memoria-historica/20131227/nota/2044459.aspx.

colombiano). El estudiante enfrenta a una pena privativa de la libertad de 4 a 8 años de prisión y una multa de hasta 616.000.000 millones de pesos.[86]

7. Neutralidad de la red en Colombia y problemas de acceso al servicio de internet

Aunque no es un tema directo de este informe, sí creemos que estos elementos son necesarios para hacer efectivo el derecho a la educación y el acceso a la cultura.

En Colombia el principio de *Neutralidad de la Red* está contemplada dentro de la Ley 1450 de 2011, que formalmente introduce el Plan Nacional de Desarrollo 2010-2014. En su artículo 56 se establece que los prestadores del servicio de internet (ISP) "no podrán bloquear, interferir, discriminar, ni restringir el derecho de cualquier usuario de Internet, para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de Internet".[87] Sin embargo, en el mismo artículo se acepta que es posible segmentar el mercado y, por tanto, las ISP "podrán hacer ofertas según las necesidades de los segmentos de mercado o de sus usuarios de acuerdo con sus perfiles de uso y consumo".[88]

Dentro de este mismo articulado, se plantea que la Comisión de Regulación de Comunicaciones (CRC) regulará los términos y condiciones de aplicación relacionados al tema de neutralidad.

La regulación, consignada en la Resolución 3502 de 2011 de la CRC, contempla que "los proveedores de redes y servicios de telecomunicaciones podrán ofrecer planes de acceso a Internet donde se limite el acceso a los tipos genéricos de servicios, contenidos o aplicaciones, según las necesidades de los segmentos de mercado o de sus usuarios de acuerdo con sus perfiles de uso y consumo, garantizando en todo momento el derecho del usuario a elegir al proveedor específico del contenido, aplicación o servicio".[89] En la misma regulación se establece que las ISP siempre deben ofrecer una alternativa o plan tarifario que no considere las limitaciones.

En la práctica, la oferta de planes segmentados ha llevado a un incumplimiento de los principios de neutralidad de la red. Las ISP ofrecen planes de solo acceso a redes sociales (Facebook, Twitter y MySpace), solo chat (Joyn, Whatsapp, Yahoo Messenger, Gtalk), solo correo electrónico (Hotmail, Gmail, Yahoo Mail), una combinación de estos planes o un plan ilimitado.[90] Los primeros claramente ofrecen acceso a fragmentos de Internet, no a todos los

[86] Para más información sobre el caso y la campaña de apoyo de la Fundación Karisma, véase http://www.karisma.org.co/compartirnoesdelito/.
[87] Ley 1450 de 2011, pags 19-20. Disponible en https://www.dnp.gov.co/LinkClick.aspx?fileticket=tYD8BLf-2-g%3d&tabid=1238.
[88] Ibíd.
[89] Resolución 3502 de 2011. Disponible en http://www.crcom.gov.co/?idcategoria=62667#.
[90] Tomamos como referencia los planes ofertados por Claro, la compañía que tiene la mayoría del mercado tanto de internet móvil como de internet cableado en el país. Información recuperada de la página

contenidos de la red sin ninguna limitación. Cada uno de estos planes contempla una cantidad máxima de MB o GB de consumo que tienen una vigencia predeterminada y presentan la opción de Cobro Frecuente, lo que permite que se pueda pagar un cargo fijo mensual por estos servicios.

Aun cuando las mismas ISP aclaran en sus ofertas que estos planes segmentados no incluye navegación, lo cierto es que el MinTIC sí puede considerarlos para sus índices de penetración de internet y número de suscriptores en el país. En comunicación privada referida por el Ministerio ante una solicitud de información vía derecho de petición de parte de la Fundación Karisma, afirman que consideran cualquier plan de datos como acceso a internet, por tanto, estos planes fragmentados hacen parte de las cifras si los usuarios "pagan un cargo fijo mensual por el servicio de acceso a internet". En todos los casos, para las estadísticas las ISP deben reportar "el tráfico generado incluido en el plan y los ingresos por cargo fijo mensual".[91]

Claramente, quienes tienen planes de acceso segmentado enfrentan barreras para acceder a la información y el conocimiento. Esa limitación, obviamente, tiene consecuencia en cuanto al ejercicio de la libertad de expresión y, en general, al ejercicio de los derechos humanos en medios digitales.

---

http://www.claro.com.co/wps/portal/co/pc/personas/movil/catalogo-promociones/promocion/paquetes-de-datos#tab-2 (consultado el 11/07/2014).

[91] **"MinTIC respondió a un derecho de petición enviado por la Fundación Karisma (Radicado 574260) el día 30 de octubre de 2013, indicando que:** *"un acceso a internet corresponde a la conexión que tiene un/a usuario/a para acceder a Internet independientemente del uso que haga sobre dicha conexión, por ello [...] los proveedores reportan para los índices de penetración a internet todos/as aquellos/as suscriptores/as que han realizado un contrato para la prestación del servicio de datos o acceso a internet y sobre el cual mensualmente paga una tarifa fija".*

ONG Derechos Digitales es una organización no gubernamental cuya misión es promover la defensa y protección de los derechos fundamentales en el entorno tecnológico.

El Derecho a la Privacidad en Latinoamérica: normativa y jurisprudencia

Documento preparatorio para presentación en audiencia ante la Corte Interamericana de Derechos Humanos

Fecha:	8 de agosto de 2014
Autores:	J. Carlos Lara Gálvez
	Paula Jaramillo Gajardo
	Danny Rayman Labrin
E-mail:	info@derechosdigitales.org
Teléfono:	(56-2) 26323660
Dirección:	Diagonal Paraguay 458 Piso 2
	Santiago de Chile

Tabla de contenidos

Introducción 51

Capítulo I Derecho a la Privacidad 52

1. Identificación del derecho a la privacidad 52
2. Contenido del derecho a la privacidad 53
3. Problemática y relevancia regional de la privacidad 55

Capítulo II Marco Normativo 56

1. Generalidades 56
2. Regulación específica 57
   - 2.1. Argentina 57
   - 2.2. Bolivia 64
   - 2.3. Brasil 67
   - 2.4. Chile 68
   - 2.5. Colombia 70
   - 2.6. Costa Rica 71
   - 2.7. Ecuador 72
   - 2.8. El Salvador 74
   - 2.9. Guatemala 75
   - 2.10. Honduras 77
   - 2.11. México 78
   - 2.12. Nicaragua 80
   - 2.13. Panamá 81
   - 2.14. Paraguay 83
   - 2.15. Perú 84
   - 2.16. República Dominicana 87
   - 2.17. Uruguay 89
   - 2.18. Venezuela 91
3. Proyectos de ley 92
   - 3.1. Argentina 92
   - 3.2. Brasil 92
   - 3.3. Chile 93
   - 3.4. Honduras 93

Capítulo III Jurisprudencia 93

1. Argentina 93
1.1. Derecho a la Intimidad 93
1.2. Derecho de Intimidad vs. Libertad de Expresión 94
1.3. Habeas Data y Privacidad 101
2. Chile 101
2.1. Vida Privada e Inviolabilidad de las Comunicaciones 101
2.2. Vida Privada y Protección de Datos 106
3. Colombia 109
3.1. Habeas Data y Lista Negras 109
4. Costa Rica 111
4.1. Derecho a Intimidad y Cámara de Vigilancia 111
4.2. Derecho a Intimidad e Información en Internet 112
4.3. Derecho de Intimidad y Datos Personales 113
4.4. Derecho a la Intimidad y Computadores de Funcionarios Públicos 115
5. México 122
5.1. Derecho a la Privacidad y Geolocalización de Teléfono Móvil 122
5.2. Inviolabilidad de Comunicaciones Privadas y Datos Almacenados en Teléfono Celular 135
6. Uruguay 139
6.1. Habeas Data y Cámaras de Vigilancia 139
Capítulo IV Condiciones de Acceso a Internet 142
1. La penetración de internet en Latinoamérica 142
2. El acceso de banda ancha 143
3. El acceso a internet móvil 144
4. La velocidad en el acceso a internet 146
Conclusiones 147

Introducción

El presente documento pretende entregar una mirada acerca de la privacidad en Latinoamérica, entendida como derecho, desde la perspectiva de las legislaciones más representativas del continente.

Con ese fin, lo primero será contextualizar un concepto de privacidad, acercándonos a sus orígenes y contenido, para luego decantar en el análisis de la problemática y relevancia asociada a este derecho.

En un segundo capítulo, analizaremos la normativa relacionada con la privacidad en Latinoamérica, para lo cual comenzaremos por aquella contenida en los tratados internacionales aplicables en el continente, pasando por las Cartas Fundamentales de los países que hemos sometido a análisis, y las leyes particulares que se han dado cada uno de ellos. Para finalizar esta sección, se hará mención a los proyectos de ley que inciden en materia de privacidad, y que se encuentran actualmente en debate en los países a que nos referimos.

A continuación, realizaremos un análisis de la jurisprudencia emanada de los altos tribunales de algunos países latinoamericanos, en los que la interpretación y aplicación que se ha hecho del derecho a la privacidad, así como también el uso de ciertas tecnologías, han jugado roles fundamentales, permitiéndonos una aproximación a la forma en que se abordan estos asuntos en el orden interno.

Finalmente, el capítulo IV entregará información acerca de las condiciones de acceso a Internet existentes en los países del continente, la que resulta relevante para determinar el impacto del derecho a la privacidad en el entorno digital.

Capítulo I
Derecho a la Privacidad

1. Identificación del derecho a la privacidad

El origen del concepto "derecho a la privacidad" se remonta al "right to privacy" del *common law* anglosajón, que fue definido a fines del siglo XIX como un derecho a estar y permanecer solo[92], en oposición a someterse al escrutinio público. Surgió como una forma de hacer frente al hostigamiento, por parte los medios de comunicación social de la época, para guardar reserva respecto de aquel aspecto de la vida personal que legítimamente podía ser excluido de la injerencia de la prensa. Este primer concepto de privacidad fue recogido y desarrollado gradualmente en las décadas posteriores, especialmente en Estados Unidos.

Huelga consignar que este "right to privacy" del derecho anglosajón guarda marcadas diferencias con el "derecho a la privacidad" de la tradición jurídica de derecho civil, presente en los países latinoamericanos, ya que el primero tiende a proteger al ciudadano tanto frente al actuar del estado como también de otros privados, entre los que se incluyen los medios de comunicación. Además si bien el "right to privacy" anglosajón no goza de reconocimiento a nivel constitucional –lo que constituye una notoria diferencia con lo que sucede a nivel latinoamericano, como veremos más adelante-, su desarrollo jurisprudencial ha sido profuso, llevándolo a amparar a una gran cantidad de bienes jurídicos entre los que encontramos la libertad de asociación, las libertades sexuales y libertad de información, entre otros, extendiéndose mucho más allá que sólo a la vida privada y la intimidad, como suele suceder en este lado del mundo.[93]

Continuando con el desarrollo histórico del derecho, cabe señalar que la idea de vida privada concitó especial interés a partir del desarrollo de la informática a mediados del siglo XX. El potencial de las herramientas informáticas para recolectar, procesar y analizar información, parecía poner en riesgo la vida privada de los individuos, lo que impulsó las demandas por normas específicas que regularan la recolección y el manejo de información personal. El avance tecnológico dejó en evidencia que no era suficiente el derecho a la privacidad entendido como el derecho a excluir la injerencia de terceros, sino que se hacía necesario ampliar su protección, incorporando una dimensión positiva que permitiera al titular controlar la información personal que le compete.

Se amplió así la concepción de información privada desde un espacio libre de intromisión ajena, a uno donde los titulares de la información pudieran tomar parte en su control, activamente; con la privacidad, ya no se aludía a una figura de "espacio reservado" fuera de intromisiones de terceros, sino que a la capacidad del titular de los datos de decidir por sí el control del destino de los mismos. Esta aspiración de reconocimiento jurídico para ese control sobre la información personal dio lugar al desarrollo del concepto de datos personales y a la regulación de su

[92] WARREN, Samuel y Louis BRANDEIS, "The right to privacy", en *Harvard Law Review,* Vol. IV, n. 5, 1890. Trad. "El derecho a la vida privada", Ed. Civitas, Madrid, 1995, p. 25.

[93] SALDAÑA, María Nieves. "The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario del legado de Warren y Brandeis". En: *Revista de Derecho Político.* N. 85, pág. 195-240, septiembre-diciembre 2012.

tratamiento, de manera separada y –mayormente- independiente del concepto de la vida privada y de la protección de las comunicaciones privadas.

En suma, a través del derecho a la privacidad se reconoce la existencia de un interés jurídicamente protegido a la no intromisión en la vida propia, sea a nivel corporal, como también familiar y espacial, y del mismo modo sobre la información relativa a una persona. Los contornos de tal interés han variado significativamente a través del tiempo[94], pero siempre se le vincula a una manifestación jurídica del respeto y protección que se debe a cada persona, protegiendo la dignidad y libertad humanas, por medio del reconocimiento a su titular de un poder de control sobre aquel ámbito del que no participan otras personas.

Finalmente cabe mencionar que se trata de un derecho que se encuentra elevado a la categoría de derecho humano o fundamental, tal como dan cuenta de ello numerosos tratados internacionales, algunos de los cuales –los que inciden en el quehacer latinoamericano- serán abordados en el capítulo siguiente, a propósito de la normativa aplicable.

Por el momento, basta señalar que se ha dicho que "la privacidad es un derecho humano básico. Esta sirve de fundamento a la dignidad y a otros valores tales como la libertad de asociación y la libertad de expresión. La privacidad se ha vuelto uno de los derechos humanos contemporáneos más importantes".[95]

2. Contenido del derecho a la privacidad

Para aproximarnos a un concepto de privacidad, el primer paso es reconocer que este no es unívoco, sino que responde más bien a un fenómeno difuso con diversas dimensiones o acepciones, las que varían enormemente de acuerdo al contexto y al medio.

En efecto, este ha sido considerado como uno de los derechos humanos más difíciles de definir,[96] ya que se trata de un concepto dinámico, que evoluciona constantemente debido a percepciones culturales y también relacionadas con el avance tecnológico; y al que se asocia a una gran cantidad de conceptos, fenómeno que se aprecia tanto en las normativas nacionales como internacionales, tal como veremos más adelante.

Por lo anterior resulta necesario señalar que, en este trabajo, se reunirán bajo la denominación de "privacidad" a un conjunto de intereses, que comprenden: la vida privada, la intimidad, la inviolabilidad de las comunicaciones privadas y del domicilio, y la protección de los datos personales, según sea la forma en que las distintas legislaciones hagan mención a ella.

Doctrinariamente se suele señalar que la privacidad es un derecho de la personalidad, relativo al cuerpo, a la afectividad y a lo que se desea que no sea conocido por otros; y que consiste en la posibilidad de negar el acceso o conocimiento a ciertos ámbitos de la vida –lo que se conoce como "autodeterminación informativa". Como ya mencionamos anteriormente, se agrega que se trata de un concepto social, o cultural, en constante evolución.

---

[94] Seguimos en este punto a CERDA SILVA, Alberto. "Autodeterminación informativa y leyes sobre protección de datos". *Revista Chilena de Derecho Informático, Nº 3 (2003). Centro de Estudios en Derecho Informático, Universidad de Chile.*

[95] PRIVACY INTERNATIONAL. *Una Guía de Privacidad para Hispanoparlantes*. En: https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes

[96] Ibídem.

Para contribuir a delimitar el concepto de privacidad, resulta sumamente útil clasificar las distintas actividades humanas vinculadas a este interés, así encontramos:

1. *Privacidad corporal*, que apunta a la protección física de las personas ante procedimientos invasivos. Desde el punto de vista de su vulneración, se vincula a la intimidad y a la integridad física. Se asocia esta privacidad también a datos personales de carácter biométrico o de salud.
2. *Privacidad territorial*, que se refiere a la fijación de límites a la intromisión en los espacios o medios domésticos, y otros tales como el centro laboral o, incluso, el espacio público.

   En este contexto, las nuevas tecnologías tienen un gran impacto a través de los medios de registro de información, que debido al nivel de miniaturización, conectividad y ubicuidad existente, son capaces de inmiscuirse en la esfera privada de las personas, considerando su domicilio, sus conductas en lugares públicos y en su lugar de trabajo, sin filtro ni límites.

   Se vincula a la vida privada y a la inviolabilidad del hogar y de las comunicaciones privadas.
3. *Privacidad comunicacional*, referida a la seguridad y privacidad del correo (físico o electrónico), el teléfono, u otras formas de comunicación privada.

   Internet sirve de soporte a numerosas formas y medios de comunicación, que operan tanto en tiempo real (sistemas de conferencia de voz, vídeo, chat, texto, VNC, etc), como asincrónicamente (foros, correo electrónico, etc). Esas plataformas son susceptibles de interceptación, lo que hace esencial la creación de controles legales y judiciales a esa intervención por agentes públicos, y de reglas que impidan a quienes tienen acceso a esos datos a usarlos, entregarlos de forma indebida, o abusar de su capacidad técnica en perjuicio de las personas a quienes concierne esa información.
4. *Privacidad de la información*, también conocida como "protección de datos personales" y desarrollada en algunas latitudes dentro de una garantía legal de autodeterminación informativa (tanto sobre datos públicos como sobre información sensible).

   Si bien su concepción como una forma de privacidad puede no encontrarse expresamente recogida desde el punto de vista dogmático (como sucede en el caso chileno), su relación viene dada por la susceptibilidad de la afectación de otros intereses (como la igualdad, la libertad o la intimidad) por medio de la vulneración de las normas sobre procesamiento de datos personales. Actualmente, gran parte de las informaciones que circulan, son almacenadas y se procesan en la comunidad, y especialmente en internet, revisten la calidad de datos personales al estar relacionados con personas determinadas. Cualquier sitio o servicio que almacene, procese, indexe o transmita esos datos hace tratamiento de datos personales; debiendo analizarse si esas conductas afectan o no los derechos fundamentales de los titulares de dicha información, y en qué medida lo hacen.

Luego de esta clasificación que vincula a la privacidad con los distintos conceptos que se amparan bajo ella, sólo resta agregar algo acerca del matiz existente entre vida privada e intimidad. Sobre ello podemos señalar que, conforme a la teoría alemana de las esferas, a la intimidad la rodea la esfera de la vida privada "y todo lo que queda fuera de ella constituye la

vida pública".[97] En consecuencia, la intimidad está en el núcleo más íntimo de la persona, y comprende aquello que no se comparte sino con las personas más cercanas.

Finalmente, en cuanto a los bienes jurídicos que resguarda el derecho a la privacidad, la Comisión Interamericana de Derechos Humanos ha señalado que ellos corresponden a: "En primer lugar, el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas. En segundo lugar, el derecho a gobernarse, en ese espacio de soledad, por reglas propias definidas de manera autónoma según el proyecto individual de vida de cada uno. En tercer lugar, el derecho a la vida privada protege el secreto de todos los datos que se produzcan en ese espacio reservado, es decir, prohíbe la divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona. Y, finalmente, la protección de la vida privada protege el derecho a la propia imagen, es decir, el derecho a que la imagen no sea utilizada sin el consentimiento del titular".[98]

3. Problemática y relevancia regional de la privacidad

Como es posible apreciar de los orígenes del concepto de privacidad, nos encontramos frente a un interés que ha ido adquiriendo relevancia desde fines del siglo XIX, y que ha presentado una evolución y expansión cada vez mayores.

En este proceso ha resultado gravitante la vertiginosa evolución de las tecnologías, fenómeno que ha provocado que el derecho a la privacidad haya adquirido una mayor relevancia en los tiempos actuales, en los que se ha visto tal vez más amenazado que nunca antes.

El extenso uso de redes informáticas ha incidido fuertemente en su afectación, ya que Internet es un medio que, técnicamente, facilita la vigilancia de las redes, así como de los datos que por ella transitan, entregando más oportunidades y a muy bajos costos para ello, y de paso también para la vulneración de la privacidad en sus distintas facetas.

Es en este punto donde adquiere relevancia la regulación que se haya de dar a dichas redes, protegiendo las libertades de sus usuarios y buscando un equilibrio con los intereses que asisten a los gobiernos y a las empresas privadas que también operan en ellas.

Además, no se debe olvidar que el resguardo de la privacidad resulta de esencial importancia ya que la afectación de este derecho fundamental incide en otras garantías con las que se encuentra estrechamente vinculado, y que en ocasiones necesitan de él para desarrollarse, tales como la libertad de expresión y la de asociación. Sobre el punto, basta recordar lo sucedido en la denominada "primavera árabe", en que Internet jugó un rol importantísimo para organizar y congregar a los manifestantes; la situación que se vive en China hasta el día de hoy, en que el gobierno intenta controlar fuertemente las redes, mediante un control masivo de los contenidos, a fin de evitar que surjan voces disidentes al gobierno; y, más recientemente, el escándalo por las filtraciones de Edward Snowden que dieron cuenta de la vigilancia masiva efectuada por el

[97] En: http://pendientedemigracion.ucm.es/info/cyberlaw/actual/9/leg04-09-01.htm

[98] Catalina Botero cita al Informe No. 82/10. Caso No. 12.524. Fontevecchia y D'Amico. Argentina. 13 de julio de 2010. Párr. 91 y ss. Cfr: BOTERO, Catalina, *Libertad de Expresión e internet*. Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos, 2013.

gobierno de los Estados Unidos, tanto respecto de otros gobiernos como de individuos particulares.

En este mismo sentido, la Organización de Estados Americanos (OEA) ha reconocido a la privacidad como uno de los principios orientadores de la libertad de expresión en Internet, tal como lo señala en extenso el informe de la relatoría especial para la libertad de expresión de 2013.[99]

Así, en un continente que requiere de medios que contribuyan al fortalecimiento de sus democracias, salvaguardar adecuadamente la privacidad, tanto en el entorno análogo como en el digital, resulta fundamental para dicho fin.

Capítulo II
Marco Normativo

1. Generalidades

Es posible identificar tres grandes áreas que conforman el marco normativo del derecho a la privacidad, a saber: los tratados internacionales, las constituciones, y las leyes particulares de cada país en estudio.

En cuanto al primer punto, es posible encontrar al menos cinco instrumentos internacionales que inciden a nivel latinoamericano, que se refieren a este derecho.

Así, el artículo 11 de la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica)[100], relativo a la Protección de la Honra y de la Dignidad, dispone que:

> "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
>
> 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
>
> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

De este último numeral se desprende que le corresponde al Estado una doble función: por una parte, ha de respetar la privacidad de los individuos; y de otra, velar por que terceras personas no incurran en conductas que pudieran afectarla arbitrariamente.

Por su parte, el artículo 12 de la Declaración Universal de los Derechos del Hombre[101], y 18 del Pacto Internacional de Derechos Civiles y Políticos[102], se refieren a la materia prácticamente en los mismos términos que los numerales 2. y 3. de la Convención antes citada.

[99] Id. anterior.
[100] En: http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

En tanto en los artículos V, IX y X de la Declaración Americana de Derechos y Deberes del Hombre[103], se alude a los derechos a la protección a la honra, la reputación personal y la vida privada y familiar, e inviolabilidad del domicilio y de la circulación de la correspondencia, respectivamente.

Finalmente, se ha de mencionar lo dispuesto por la Convención de los Derechos del Niño, cuyo artículo 16 expresamente señala que "1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o a su reputación. 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".[104]

En el orden nacional, y por tratarse de un derecho fundamental, casi la totalidad de los textos constitucionales latinoamericanos actualmente contiene alguna mención expresa a la privacidad, como tal, o utilizando alguno de los conceptos vinculados con ella, a los que nos referimos previamente.

A modo de ejemplo, en la mayoría de las Constituciones pertenecientes a los países latinoamericanos analizados en este paper, se menciona de alguna forma la protección de los datos personales[105]; mientras que, en los casos en que ello no sucede, como por ejemplo Chile, la Carta Fundamental sí se refiere a conceptos como la "vida privada"[106], y a la "inviolabilidad del hogar y de toda forma de comunicación *privada*"[107], dando nociones de intimidad en un sentido espacial.

Los detalles de cómo cada una de las Constituciones, país por país, aborda el derecho a la privacidad será materia del apartado siguiente de este capítulo, al igual que sucede con la legislación específica.

2. Regulación específica

Argentina[108]

La República Argentina es un estado federal, compuesto por 23 provincias, cada una de las cuales divide su territorio en departamentos, los que a su vez se componen de municipios, más la Ciudad Autónoma de Buenos Aires. En consecuencia, encontramos una gran cantidad de normativa en cada uno de los mencionados niveles, comprendiendo así las reglas nacionales como también las provinciales. En honor a la extensión y fines del presente documento, solo haremos mención de la normativa nacional, así como la provincial de mayor importancia.

---

[101] En: http://www.un.org/es/documents/udhr/
[102] En: http://www2.ohchr.org/spanish/law/ccpr.htm
[103] En: http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp
[104] En: http://www.unicef.cl/unicef/index.php/Texto-Oficial-de-la-Convencion
[105] REMOLINA ANGARITA, Nelson. *Aproximación Constitucional de la Protección de Datos Personales en Latinoamérica.* Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia) Nº 1 Julio - Diciembre de 2012.
[106] Constitución Política de la República de Chile, 1980. El artículo 19 Nº 4 asegura a toda persona "el respeto y la protección a la vida privada" de la persona y de su familia.
[107] Id. Ant. Artículo 19 Nº 5.
[108] Lista de Normas relacionadas a Privacidad y Protección de datos de Argentina obtenida de En: http://www.protecciondedatos.com.ar/ y En: http://www.redipd.org/index-ides-idphp.php

Constitución

En el orden nacional, la Constitución Nacional de Argentina de 1994[109] se refiere en el artículo 18 a la inviolabilidad del domicilio y de la correspondencia, señalando que "El domicilio es inviolable como también la correspondencia epistolar y los papeles privados; y una ley determinara en que casos y con que justificativos podrá procederse a su allanamiento y ocupación".

En tanto el artículo siguiente (19) dispone que "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral publica, ni perjudiquen a un tercero, están solo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ello no prohíbe".

En materia de protección de datos, el inciso 3º del artículo 43 consigna el habeas data, en los siguientes términos: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística".

Las constituciones provinciales más relevantes también se refieren a la acción de Habeas Data, en términos que resultan ser bastante similares. Así sucede en el caso de la Ciudad Autónoma de Buenos Aires[110]; y las Provincias de Buenos Aires[111]; Córdoba[112]; Chaco[113]; Chubut[114]; Entre

[109] En: http://www.constitution.org/cons/argentin.htm

[110] Artículo 16: "Toda persona tiene, mediante una acción de amparo, libre acceso a todo registro, archivo o banco de datos que conste en organismos públicos o en los privados destinados a proveer informes, a fin de conocer cualquier asiento sobre su persona, su fuente, origen, finalidad o uso que del mismo se haga. También puede requerir su actualización, rectificación, confidencialidad o supresión, cuando esa información lesione o restrinja algún derecho. El ejercicio de este derecho no afecta el secreto de la fuente de información periodística". En: http://www.buenosaires.gob.ar/areas/com_social/constitucion/completa.php

[111] Artículo 20 número 3: "A través de la garantía de Habeas Data que se regirá por el procedimiento que la ley determine, toda persona podrá conocer lo que conste de la misma en forma de registro, archivo o banco de datos de organismos públicos, o privados destinados a proveer informes, así como la finalidad a que se destine esa información, y a requerir su rectificación, actualización o cancelación. No podrá afectarse el secreto de las fuentes y el contenido de la información periodística. Ningún dato podrá registrarse con fines discriminatorios ni será proporcionado a terceros, salvo que tengan un interés legítimo. El uso de la informática no podrá vulnerar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos. Todas las garantías precedentes son operativas. En ausencia de reglamentación, los jueces resolverán sobre la procedencia de las acciones que se promuevan, en consideración a la naturaleza de los derechos que se pretendan tutelar". En: http://www.gob.gba.gov.ar/dijl/constitucion.php

[112] Artículo 50: "Toda persona tiene derecho a conocer lo que de él conste en forma de registro, la finalidad a que se destina esa información, y a exigir su rectificación y actualización. Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando tenga un interés legítimo. La ley reglamenta el uso de la informática para que no se vulneren el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos". En: http://www.justiciacordoba.gob.ar/justiciacordoba/files/leyes/ConstitucionCordoba.pdf

[113] Artículo 19: "Todos los derechos y garantías reconocidos, expresa o implícitamente, en esta Constitución, están protegidos en sus ejercicios por las siguientes acciones: (…) Habeas Data: Toda persona tiene derecho a informarse de los datos que sobre sí mismo, o sobre sus bienes, obren en forma de registro o sistemas oficiales o privados de carácter público; la finalidad a que se destine esa información y a exigir su actualización, corrección, supresión o confidencialidad. Tales datos no podrán ser utilizados con fines discriminatorios de ninguna especie. No podrá afectarse el secreto de las fuentes de la información periodística. Responsabilidad: Ningún juez podrá excusar la

Ríos[115]; Neuquén[116]; Salta[117]; San Juan[118]; Santiago del Estero[119]; y Tierra del Fuego, Antártida e Islas del Atlántico Sur[120]

Mención aparte merece la Constitución de la Provincia de Jujuy, que se refiere de manera mucho más extensa y omnicompresiva a los aspectos relacionados con la "Protección de la intimidad, de la honra y de la dignidad" en el artículo 23, en los siguientes términos:

---

denegación de las acciones contempladas en este artículo en el hecho de no haberse sancionado las leyes reglamentarias, en cuyo caso deberá arbitrar las medidas procesales adecuadas. Tampoco podrá negarse a entender en las acciones o resolverlas en violación de los plazos previstos. No podrán los funcionarios o empleados negarse al cumplimiento de la orden judicial respectiva. Si lo hicieren, serán enjuiciados y, en su caso, removidos". En: http://www.biblioteca.jus.gov.ar/const-chaco.html

[114] Artículo 56: "Toda persona puede interponer acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o en los privados destinados a proveer informes y en caso de error, omisión, falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No puede afectarse el secreto de la fuente de información periodística". En: http://www.juschubut.gov.ar/images/constituciones/constitucion_provincial.pdf

[115] Artículo 63: "Toda persona tiene derecho a interponer acción expedita, rápida y gratuita de habeas data para tomar conocimiento de los datos referidas a ella, a sus familiares directos fallecidos, o a sus propios bienes, así como la fuente, finalidad y destino de los mismos, que consten en todo registro, archivo o banco de datos públicos o privados de carácter público, o que estuviesen almacenados en cualquier medio técnico apto para proveer informes. En caso de falsedad o uso discriminatorio de tales datos podrá exigir, sin cargo alguno, la inmediata rectificación o actualización de la información falsa o la supresión o confidencialidad de la sensible. El ejercicio de este derecho no puede afectar las fuentes de información periodística ni el secreto profesional. La acción no procederá cuando la obtención de los datos reclamados estuviese reglamentada". En: http://www.jusentrerios.gov.ar/mediacion/wp-content/themes/mediacion/images/documentos/constitucion_entrerios_2008.pdf

[116] Artículo 61: "Toda persona puede interponer acción de habeas data para tomar conocimiento de los datos a ella referidos, su fuente, origen, finalidad y uso, que consten en registros, archivos o bancos de datos de organismos públicos o privados, en este último caso siempre que ejerzan la función de suministrar informes; y en caso de error, omisión, falsedad, discriminación o de tratarse de datos sensibles de las personas, para exigir la supresión, rectificación, confidencialidad o adecuación de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística". En: http://www.jusneuquen.gov.ar/share/legislacion/leyes/constituciones/constitucion_nqn/cnqn_art58a73.htm

[117] Artículo 89: "HÁBEAS DATA. Toda persona podrá interponer acción expedita de hábeas data para tomar conocimiento de los datos referidos a ella o a sus bienes, y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes. En caso de datos falsos, erróneos, obsoletos o de carácter discriminatorio, podrá exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística". En: http://www.ambiente.gov.ar/archivos/web/biblioteca/File/Contituciones/cp_salta.pdf

[118] Artículo 26: "Todo ciudadano tiene derecho a tomar conocimiento de lo que de él conste en forma de registro y de la finalidad a que se destinan las informaciones, pudiendo exigir la rectificación de datos, así como su actualización. No se puede utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se destine para fines estadísticos no identificables". En: http://www.ambiente.gov.ar/archivos/web/biblioteca/File/Contituciones/cp_sanjuan.pdf

[119] Artículo 60: "Hábeas data. Toda persona puede interponer acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o en los privados destinados a proveer informes y en caso de error, omisión, falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No puede afectarse el secreto de la fuente de información periodística". En: http://www1.hcdn.gov.ar/dependencias/dip/congreso/constitucionesprovinciales/ConsSantEst.pdf

[120] Artículo 45: "Toda persona tiene derecho a conocer lo que de ella conste en forma de registro y la finalidad a que se destine esa información, y a exigir su rectificación y actualización. Esos datos no pueden registrarse con propósitos discriminatorios de ninguna clase, ni ser proporcionados a terceros, excepto cuando éstos tengan un interés legítimo". En: http://www.sup-trib-delsur.gov.ar/sup-trib-delsur/CONSPROVW.htm

"1.- Las acciones privadas de los hombres que de ningún modo ofendan el orden o la moral pública ni perjudiquen a un tercero, están exentas de la autoridad de los magistrados.

2.- Toda persona tiene derecho a que se respete su intimidad y su honra, así como al reconocimiento de su dignidad.

3.- Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada ni de ataques ilegales a su intimidad, honra o reputación.

4.- Cualquier persona afectada en su intimidad, honra o dignidad por informaciones inexactas o agraviantes emitidas a través de los medios de comunicación, tiene derecho a efectuar su rectificación o respuesta gratuitamente, en el mismo lugar y hasta su igual extensión o duración, por el mismo órgano de difusión. Ese cumplimiento se podrá demandar mediante el recurso de amparo ante cualquier juez letrado de la provincia, sin perjuicio de las responsabilidades de otro orden que pudiere corresponder.

5.- Para la efectiva protección de la intimidad, la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio, televisión o cualquier otro medio de comunicación, tendrá una persona responsable que no deberá estar protegida por inmunidades ni dispondrá de un fuero especial.

6.- Todas las personas tienen derecho de tomar conocimiento de lo que constare a su respecto en los registros provinciales de antecedentes personales y del destino de esas informaciones, pudiendo exigir la rectificación de los datos. Queda prohibido el acceso de terceros a esos registros, así como su comunicación o difusión, salvo en los casos expresamente previstos por la ley.

7.- Los registros provinciales de antecedentes personales harán constar en las certificaciones que emitan solamente las causas con condenas efectivas firmes dictadas contra el interesado, con excepción de las que debieran ser remitidas a los jueces.

8.- El procesamiento de datos por cualquier medio o forma nunca puede ser utilizado para su registro y tratamiento con referencia a convicciones filosóficas, ideológicas o políticas, filiación partidaria o sindical, creencias religiosas o respecto de la vida privada, salvo que se tratare de casos no individualmente identificables y para fines estadísticos".[121]

Finalmente encontramos los casos de las provincias de La Rioja[122], Río Negro[123] y San Luis[124], que se centran en el derecho a la privacidad, intimidad, y la libre expresión de las ideas en relación a la vida privada, respectivamente.

[121] En: http://www.jujuy.gov.ar/wp-content/uploads/documentos/constitucion-jujuy.pdf

[122] Artículo 30: "Derecho a la Privacidad: Son inviolables el domicilio, los papeles y registros de datos privados, la correspondencia epistolar y las comunicaciones de cualquier índole. Sólo pueden ser allanados, intervenidos, interceptados o registrados en virtud de orden escrita de juez competente. La ley limitará el uso de la informática para preservar el honor, la intimidad personal y familiar de los habitantes y el pleno ejercicio de sus derechos. El allanamiento de domicilio en horas de la noche es excepcional, debiendo el magistrado que lo dispone fundar la decisión. Las autoridades policiales sólo proporcionarán antecedentes penales de los habitantes en los casos previstos por la ley". En: http://www.biblioteca.jus.gov.ar/const-larioja.html

Normativa

En materia de leyes nacionales, encontramos la Ley Nº 21.173, de 22 de Octubre de 1975, sobre Derecho a la Intimidad, que modifica el Código Civil incorporando el Artículo 1071 bis, que dispone "El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación".[125]

Por su parte, el 2 de noviembre del año 2000, se dictó la Ley Nº 25.326, de Protección de Datos,[126] que fue posteriormente modificada por la Ley Nº 26.343, de 8 de enero de 2008, incorporando a la primera el artículo 47, que regula la eliminación de los datos de obligaciones y calificaciones asociadas de las personas físicas y jurídicas que han incurrido en mora de los bancos de datos destinados a prestar servicios de información crediticia.

Finalmente, se debe mencionar la Ley Nº 26.388, que Reforma del Código Penal en materia de Delitos Informáticos, y también deroga y modifica algunos incisos introducidos por el artículo 32 de la Ley Nº 25.326 al Código Penal, precisamente referido a las sanciones penales.

A nivel de decretos de índole nacional, destacan los siguientes:

---

[123] Artículo 20: "La ley asegura la intimidad de las personas. El uso de la información de toda índole o categoría, almacenada, procesada o distribuida a través de cualquier medio físico o electrónico, debe respetar el honor, la privacidad y el goce completo de los derechos. La ley reglamenta su utilización de acuerdo a los principios de justificación social, limitación de la recolección de datos, calidad, especificación del propósito, confidencialidad, salvaguarda de la seguridad, apertura de registros, limitación en el tiempo y control público. Asegura el acceso de las personas afectadas a la información para su rectificación, actualización o cancelación cuando no fuera razonable su mantenimiento".
En: http://www.legisrn.gov.ar/const_prov.php

[124] Artículo 21: "Es inviolable el derecho que toda persona tiene de expresar libremente sus ideas y opiniones y de difundirlas por cualquier medio, sin censura de ninguna clase. Ninguna ley ni autoridad puede restringir la libre expresión y difusión de las ideas, ni trabar, impedir ni suspender por motivo alguno el funcionamiento de los talleres de impresión, difusoras radiales, televisivas y demás medios idóneos para la emisión y propagación del pensamiento, ni secuestrar maquinarias o enseres, ni clausurar sus locales, salvo por resolución judicial. Aquel que abuse de este derecho es responsable de los delitos comunes en que incurre a su amparo y de la lesión que cause a quiénes resulten afectados. Todos los habitantes de la Provincia gozan del derecho al libre acceso a las fuentes públicas de información. La libertad de expresión comprende también el derecho de las publicaciones a obtener los elementos necesarios a tal fin, y la facultad que tiene toda persona a la réplica o rectificación ante una referencia o información susceptible de afectar su reputación personal, la que debe publicarse gratuitamente, en igual forma y con el mismo medio utilizado. Una ley especial asegura la protección debida a toda persona o entidad contra los ataques a su honra, reputación, vida privada o familiar, cuando ésta es lesionada por cualquiera de los medios de difusión determinados en este artículo. Todos los habitantes de la Provincia tienen derecho a tomar conocimiento de lo que de ellos conste en registro de antecedentes personales e informarse sobre la finalidad a que se destinan dichos registros y la fuente de información en que se obtienen los datos respectivos". En:
http://ministerios.sanluis.gov.ar/res/5088/media/pdf/18992.pdf

[125] En: http://www.codigocivilonline.com.ar/codigo_civil_online_1066_1106.html

[126] En: http://www.jus.gob.ar/media/33481/ley_25326.pdf

- Nº 1.558/2001. Reglamentación de la Ley Nº 25.326, contiene principios generales relativos a la protección de datos, derechos de los titulares de los datos, usuarios y responsables de archivos, registros y bancos de datos, normas sobre control y sanciones.[127]
- Nº 341/2014. Designación del Director Nacional de Protección de Datos.[128]

También se deben mencionar como relevantes en materia de privacidad las disposiciones emanadas de la Dirección Nacional de Protección de Datos Personales, entre las cuales es posible mencionar sólo a modo de ejemplo:

- Nº 10/06- Registro de Bases de Entes Públicos No Estatales.[129]
- Nº 2/08- Repertorio de Jurisprudencia.[130]
- Nº 3/08- Centro de Jurisprudencia, Investigación y Promoción de la Protección de los Datos Personales.[131]
- Nº 7/08– "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público" y el texto modelo de "Convenio de Confidencialidad".[132]
- Nº 9/08- Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados. Prorrógase el plazo establecido por la Disposición Nº 11/2006.[133]
- Nº 10/08- Derecho de Acceso.[134]
- Nº 4/09 - Obligatoriedad de brindar la Opción para el ejercicio del Derecho de Retiro o Bloqueo en toda comunicación que se efectúe con fines publicitarios.[135]
- Nº 7/10- Robo de Identidad.[136]
- Nº 12/10- Confidencialidad de Datos Personales Destinados a Difusión Pública.[137]
- Nº 17/10- Base Informática para la Comunicación Electrónica Interjurisdiccional sobre Datos Personales en Información Crediticia.[138]
- Nº 24/10 - Creación del Registro Nacional de documentos de identidad cuestionados.[139]

En el ámbito provincial, a su vez, encontramos las siguientes normativas sobre privacidad:

- Ciudad Autónoma de Buenos Aires
  - Ley Nº 1.845 de la Ciudad Autónoma de Buenos Aires, sobre Protección de Datos Personales.[140]

[127] En: http://www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf
[128] En: http://www.protecciondedatos.com.ar/dec341.htm
[129] En: http://www.jus.gob.ar/media/33442/disp_2006_10.pdf
[130] En: http://www.jus.gob.ar/media/33451/disp_2008_02.pdf
[131] En: http://www.jus.gob.ar/media/33454/disp_2008_03.pdf
[132] En: http://www.jus.gob.ar/media/33463/disp_2008_07.pdf
[133] En: http://www.jus.gob.ar/media/33466/disp_2008_09.pdf
[134] En: http://www.jus.gob.ar/media/33469/disp_2008_10.pdf
[135] En: http://www.jus.gob.ar/media/33478/DISP_2009_04.pdf
[136] En: http://www.jus.gob.ar/media/86690/disp_2010_07.pdf
[137] En: http://www.jus.gob.ar/media/86693/disp_2010_12.pdf
[138] En: http://www.jus.gob.ar/media/86696/disp_2010_17.pdf
[139] En: http://www.jus.gob.ar/media/118978/disp_2010_24.pdf

- Ley Nº 712, de Garantías del Patrimonio Genético Humano.[141]
- Ley Nº 1.226, sobre Sistema de Identificación al Recién Nacido y de su Madre.[142]
- Ley Nº 2.014, Creación de Registro No Llame.[143]
- Decreto Nº 725/07, que aprueba la reglamentación de la Ley Nº 1.845 de Protección de Datos Personales.[144]
- Disposición Nº 119/07, sobre Creación de Centro de Protección de Datos de la Ciudad Autónoma de Buenos Aires.[145]
- Disposición Nº 143/08, Reglamento de inscripción de Bases de Datos en el Registro de Bancos de Datos del Centro de Protección de Datos Personales de la Ciudad de Buenos Aires.[146]
- Decreto 625/09, Crea el Registro de Empleadores Online.[147]

• Provincia de Buenos Aires
  - Ley Nº 13.074, Registro de Deudores Alimentarios Morosos.[148]
  - Ley Nº 13.120, Privacidad en Juegos de Azar.[149]
  - Disposición Normativa-Serie "B" Nº 20/04 de la Dirección de Rentas. Régimen de información para empresas de servicios: Energía eléctrica, telefonía, gas, televisión por cable y señal satelital.[150]
  - Ley Nº 14.214. Reglamentación del Proceso Constitucional de Hábeas Data de conformidad a lo establecido en el artículo 20, inciso 3º, de la Constitución Provincial.[151]
• Provincia de Chubut
  - Ley Nº 4.244. Ley de Hábeas Data.[152]
• Provincia de Córdoba
  - Ley Nº 9.380. Regulación del Uso de Videocámaras en lugares públicos.[153]
• Provincia de Mendoza
  - Ley Nº 7.261. Creación del Registro de Empresas Privadas de Información de Deudores.[154]
• Provincia de Misiones

---

[140] En: http://www.redipd.org/legislacion/common/legislacion/Argentina/ley_1845_proteccion_datos_personales.pdf
[141] En: http://www.protecciondedatos.com.ar/ley712.htm
[142] En: http://www.protecciondedatos.com.ar/ley1226.htm
[143] En: http://www.protecciondedatos.com.ar/ley2014.htm
[144] En: http://www.protecciondedatos.com.ar/dec72507.htm
[145] En: http://www.protecciondedatos.com.ar/disp11907.htm
[146] En: http://www.protecciondedatos.com.ar/disp14308.htm
[147] En: http://www.protecciondedatos.com.ar/dec62509.htm
[148] En: http://www.protecciondedatos.com.ar/ley13074.htm
[149] En: http://www.protecciondedatos.com.ar/ley13120.htm
[150] En: http://www.protecciondedatos.com.ar/disb20.htm
[151] En: http://www.protecciondedatos.com.ar/ley14214.htm
[152] En: http://www.protecciondedatos.com.ar/ley4244.htm
[153] En: http://www.protecciondedatos.com.ar/ley9380.htm
[154] En: http://www.protecciondedatos.com.ar/ley7261.htm

- Ley Nº 3.794. Protección de Datos Personales. Habeas Data.[155]

- Provincia de Neuquén
  - Ley Nº 2.307. Acción de Habeas Data.[156]
  - Ley Nº 2.399. Adhesión a la Ley Nacional 25.326.[157]
  - Decreto Nº 313/03. Creación del Registro Provincial de Datos Personales (REPRODAP)[158]
- Provincia de Santiago del Estero
  - Ley Nº 6.296. Ley de Amparo.[159]
- Provincia de Tucumán
  - Código Procesal Constitucional, Capítulo IV, artículo 67 sobre Amparo Informativo o Habeas Data.[160]

Bolivia

a) Constitución

Varias disposiciones de la carta boliviana se refieren a la privacidad[161]. Así, el numeral 2º del artículo 21 establece que sus ciudadanos tiene derecho "A la privacidad, intimidad, honra, honor, propia imagen y dignidad".

Por su parte, el artículo 23 de la misma, modificado por la Ley Nº 2631 de 20 de Febrero de 2004, dispone que:

> "I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos, de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Habeas Data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.
>
> II. Si el Tribunal o Juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado.
>
> III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo.

[155] En: http://www.protecciondedatos.com.ar/ley3794.htm
[156] En: http://www.protecciondedatos.com.ar/ley2307.htm
[157] En: http://www.protecciondedatos.com.ar/ley2399.htm
[158] En: http://www.protecciondedatos.com.ar/dec313.htm
[159] En: http://www.protecciondedatos.com.ar/ley6296.htm
[160] En: http://www.protecciondedatos.com.ar/cpctucu.htm
[161] En: http://www.tcpbolivia.bo/tcp/sites/all/modulostcp/leyes/cpe/cpe.pdf

IV. El recurso de Habeas Data no procederá para levantar el secreto en materia de prensa.

V. El recurso de Habeas Data se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el Artículo 19º de esta Constitución".[162]

Mientras tanto el artículo 25 se refiere a la inviolabilidad del domicilio y las comunicaciones, de la siguiente manera:

"I Toda persona tiene derecho a la inviolabilidad de su domicilio y al secreto de las comunicaciones privadas en todas sus formas, salvo autorización judicial.

II. Son inviolables la correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte, éstos no podrán ser incautados salvo en los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente.

III. Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones o comunicaciones privadas mediante instalación que las controle o centralice.

IV. La información y prueba obtenidas con violación de correspondencia y comunicaciones en cualquiera de sus formas no producirán efecto legal".[163]

A su turno, el artículo 130 números I y II, establecen lo siguiente:

"I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa".[164]

Finalmente, el artículo 131 números I, II, III y IV señalan el procedimiento que resulta aplicable a dicha acción.[165]

Normativa

[162] En: http://silep.vicepresidencia.gob.bo/SILEP/masterley/116003
[163] Ibídem
[164] Ibídem
[165] "I. La acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional. II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado. III. La decisión se elevará de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ellos se suspenda la ejecución. IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la Ley". En: Ibídem

El artículo 18 del Código Civil, que data del 6 de Agosto de 1975, establece el derecho a la intimidad: "Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos por la ley"[166].

Además, existe la Ley Nº 1768, de 10 de Marzo de 1997, que modificó el Código Penal incluyendo el Capítulo XI, del Título XII, del Libro Segundo, relativo a los "Delitos Informáticos", los que se encuentran regulados en los artículos 363 bis y 363 ter.[167]

Luego, encontramos la Ley Nº 018, de 16 de Junio de 2010, del Órgano Electoral Plurinacional, que regula en el artículo 72 sus obligaciones; en el 74 el Registro y actualización de datos; en el 76 el Padrón Electoral; en el 77 la Lista de habilitados e inhabilitados, y en el 79 el acceso a información del Padrón Electoral[168]. En tanto la Ley Nº 164 de 8 de Agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación, regula en su artículo 54 los derechos de los usuarios; en el 56 la inviolabilidad y secreto de las comunicaciones; en el 59 las obligaciones de los operadores y proveedores; en el 84 la reglamentación; en el 89 el correo electrónico personal; en el 90 el correo electrónico laboral; y, en el 91 las comunicaciones comerciales publicitarias por correo electrónico o medios electrónicos.[169]

A nivel de Decretos Supremos encontramos los siguientes:

- Nº 28.168, de 18 de Mayo de 2005, sobre Acceso a la Información, cuyo artículo 19 versa sobre la petición de Habeas Data en los siguientes términos:

  "I. Toda persona, en la vía administrativa, podrá solicitar ante la autoridad encargada de los archivos o registros la actualización, complementación, eliminación o rectificación de sus datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a sus derechos fundamentales a la identidad, intimidad, imagen y privacidad. En la misma vía, podrá solicitar a la autoridad superior competente el acceso a la información en caso de negativa injustificada por la autoridad encargada del registro o archivo público.

  II. La petición de Habeas Data se resolverá en el plazo máximo de cinco (5) días hábiles. En caso de negativa injustificada de acceso a la información, la autoridad jerárquica competente, adicionalmente tendrá un plazo de quince (15) días hábiles para proporcionar la información solicitada.

  III. La petición de Habeas Data no reemplaza ni sustituye el Recurso Constitucional establecido en el Artículo 23 de la Constitución Política del Estado. El interesado podrá acudir, alternativamente, a la vía administrativa sin que su ejercicio conlleve renuncia o pérdida de la vía judicial. El acceso a la vía judicial no estará condicionado a la previa utilización ni agotamiento de esta vía administrativa".[170]

[166] En: http://silep.vicepresidencia.gob.bo/SILEP/masterley/118561
[167] En: http://medios.economiayfinanzas.gob.bo/VPSF/documentos/Normas/DGSF/Ley_1768.pdf
[168] En: http://www.redipd.org/legislacion/common/legislacion/Bolivia/Ley_N_018_Organo_Electoral_Plurinacional.pdf
[169] En: http://www.redipd.org/legislacion/common/legislacion/Bolivia/Ley_N_164_Telecomunicaciones.pdf
[170] En: http://comunicacion.gob.bo/sites/default/files/docs/Decreto%20Supremo%20N%C2%BA%2028168%20Acceso%20a%20la%20Informacion_0.pdf

- Nº 1793, de 13 de Noviembre de 2013, Reglamento de la Ley Nº 164 que regula las definiciones (artículo 3º); principios (artículo 4º), funciones de la Agencia de Registro (artículo 40); derechos del titular del certificado (artículo 54); protección de datos personales (artículo 56); y, las comunicaciones comerciales publicitarias (artículo 57).[171]

Brasil

Si bien en este caso también nos encontramos frente a una estado federado, la normativa no resulta ser tan desagregada, como en el caso argentino.

a) Constitución

El artículo 5º de la Constitución de la República Federativa del Brasil de 1988[172], dispone que:

> "Todos son iguales ante la ley, sin distinción de cualquier naturaleza, garantizándose a los brasileños y a los extranjeros residentes en el País la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la prioridad, en los siguientes términos:
>
> LXXII se concederá "habeas data": a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo (...).
>
> LXXVII son gratuitas las acciones de "habeas corpus" y "habeas data" y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía".

Normativa

El Código Penal brasileño establece crímenes contra la Inviolabilidad del Domicilio (artículo 150), contra la Inviolabilidad de la Correspondencia (artículo 151 y 152), contra la Inviolabilidad de los Secretos (artículo 153).[173]

Por su parte, el Código Civil en su artículo 21 dispone que: "La vida privada de la persona natural es inviolable, y el juez, a requerimiento de un interesado, adoptará las providencias necesarias para impedir o hacer cesar acto contrario a esta norma".[174]

Luego, dos leyes generales se vinculan con privacidad, a saber: la Ley Nº 9.507, de 12 de Noviembre de 1997, que Regula el Derecho de Acceso a la información y el Procedimiento del Habeas Data[175]; y la Ley Nº 12.965, de 23 de Abril de 2014, que establece principios, garantías, derechos y deberes para el uso de Internet en Brasil, también llamado "Marco Civil".[176]

En tanto, las siguientes leyes especiales, se vinculan con la materia:

---

[171] En: http://www.redipd.org/legislacion/common/legislacion/Bolivia/DS_1793_Telecomunicaciones.pdf
[172] En: http://www.redipd.org/legislacion/common/legislacion/Brasil/constitucion_brasil_1988.pdf
[173] En: http://www.redipd.org/legislacion/common/legislacion/Brasil/Brasil_codigo_penal.pdf
[174] Traducido al español por Danny Rayman Labrin a partir de el siguiente documento En: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm
[175] En: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm
[176] En: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm

- Ley Nº 9.472, de 16 de Julio de 1997, Dispone la Organización de los Servicios de Telecomunicaciones, la creación y el funcionamiento de un Organismo Regulador y otros aspectos Institucionales, en términos de la enmienda Constitucional Nº 8, 1995. (Artículo 3 IX, Derechos del Usuario del Servicio).[177]
- Ley Complementaria Nº 105, de 10 de Enero de 2001, que entrega Disposiciones sobre Secreto de las Operaciones de Instituciones Financieras.[178]
- Ley Nº 8.078, de 11 de Septiembre de 1990, Disposiciones sobre la Protección de los Consumidores.[179]

Chile

a) Constitución

La protección constitucional sobre intereses vinculados con la privacidad –que, como tal, no se encuentra recogida en el ordenamiento jurídico-, se encuentra en el artículo 19, numerales 4º y 5º de la Carta Fundamental[180], en relación al derecho al "respeto y la protección a la vida privada y a la honra de la persona y de su familia", y a la "inviolabilidad del hogar y de toda forma de comunicación privada (…)", respectivamente.

No hay protección constitucional explícita de los datos personales, no obstante lo cual la jurisprudencia le ha brindado amparo a través de la acción de protección.

Normativa

Existen normas penales de protección a la vida privada y a la inviolabilidad de las comunicaciones (artículos 161 A y B del Código Penal[181]); y una ley especial de protección a la vida privada (Ley Nº 19.628)

Esta última, regula en general la protección de información concerniente a personas naturales, que se consideran titulares de datos. Como contraparte regula al responsable del registro y banco de datos, la persona natural o jurídica a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal, y quien responde frente al titular de los datos. La principal misión de la ley es la regulación del tratamiento de datos personales. A favor de los titulares, se establecen los derechos de acceso o información (sobre qué datos se mantienen, para qué se usan, y quién es responsable), el de modificación o rectificación de datos, el de cancelación o eliminación, y el de oposición o bloqueo. La ley materializa en su articulado principios como el de la finalidad y calidad de la información, y establece una regla general de consentimiento expreso de un titular para el tratamiento de sus datos; no obstante, establece una serie de excepciones que permiten ese tratamiento. No existe en Chile una autoridad pública de control del tratamiento de datos personales, ni sanciones penales para infracciones serias de esta normativa.

[177] En: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm
[178] En: http://www.redipd.org/legislacion/common/legislacion/Brasil/lei_complementaria_105_pt.pdf
[179] En: http://www.redipd.org/legislacion/common/legislacion/Brasil/ley_8078_1990_pt.pdf
[180] En: http://www.leychile.cl/Navegar?idNorma=242302
[181] En: http://www.leychile.cl/Navegar?idNorma=1984#comunicac10

Dicha ley ha sido objeto de varias reformas, así la Ley Nº 19.812, de 13 de Junio de 2002, la modificó para favorecer la reinserción laboral de las personas desempleadas.[182] En tanto, la Ley Nº 20.463, de 25 de Octubre de 2010, la modificó suspendiendo por un plazo determinado la información comercial de las personas cesantes.[183]

Luego, la Ley Nº 20.521, de 23 de Julio de 2011, modificó la Ley Nº 19.628 para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz[184]; mientras que la Ley Nº 20.575, de 17 de Febrero de 2012, estableció el principio de finalidad en el tratamiento de datos personales.[185]

En el ámbito de la acción del Estado encontramos que, como excepción a la transparencia pública, la Ley Nº 20.285 contempla causales de información reservada, que incluyen la seguridad nacional y los derechos de las personas, entre otros. También vinculado a la administración, se encuentra el caso de registros públicos administrados por el Estado. En particular, los padrones electorales previos a cada elección periódica, que conforme a la ley electoral deben hacerse públicos vía web.

En cuanto al funcionamiento de las telecomunicaciones, los operadores en Chile son privados y regidos por la Ley Nº 18.168. Junto con la garantía general de inviolabilidad de las comunicaciones privadas, y la obligación de preservar la privacidad de los usuarios, se sanciona la interceptación o captación maliciosa o grave de cualquier tipo de señal que se emita a través de un servicio público, además de su difusión. Por otra parte, existe un mandato de retención de datos sobre los proveedores de internet, que obliga a guardar información de conexión y números IP por hasta un año para facilitar una eventual investigación criminal.

Luego, en materia de regulaciones específicas, encontramos:

- Decreto 142, de 11 de abril de 2005, sobre Interceptación y Grabación de Comunicaciones Telefónicas y Otras Formas de Telecomunicación, del Ministerio de Transportes y Telecomunicaciones, que establece directrices generales sobre interceptación de telecomunicaciones, tendientes a resguardar la privacidad, y al mismo tiempo a facilitar el trabajo de las policías en la investigación criminal.
- Decreto 779, de 24 de Agosto de 2000, contiene la reglamentación de la Ley Nº 19.629, que regula el Registro de Bancos de Datos Personales a Cargo de los Organismos Públicos.[186]
- Ley Nº 19.223, de 7 junio de 1993. Relativa a Delitos Informáticos (artículos 1º al 4º).
- Ley Nº 19.496, de 4 de marzo de 2012, sobre Protección a los Derechos de los Consumidores.
- Ley Nº 19.628, de 28 de agosto de 1999, cuyo artículo 24 modifica el Código Sanitario a propósito de la reserva en relación a recetas médicas y análisis o exámenes de laboratorios clínicos.

[182] En: http://www.leychile.cl/Navegar?idNorma=199093
[183] En: http://www.leychile.cl/Navegar?idNorma=1018376
[184] En: http://www.leychile.cl/Navegar?idNorma=1028013
[185] En: http://www.leychile.cl/Navegar?idNorma=1037366
[186] En: http://www.leychile.cl/Navegar?idNorma=177681

- Ley Nº 19.759, de 1 de diciembre de 2001, que modifica el Código del Trabajo, incorporando un nuevo inciso 1º al artículo 5º, estableciendo como limitaciones a las facultades del empleador "el respeto a las garantías constitucionales de los trabajadores, en especial cuando pudieran afectar la intimidad, la vida privada o la honra de éstos"[187].

Colombia

a) Constitución

La Constitución Política de Colombia, de 1991[188], dispone en su artículo 15 que: "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 los 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".

Normativa

En este orden, encontramos las Leyes Estatutarias Nº 1.581, de 17 de Octubre de 2012, por la cual se dictan disposiciones generales para la protección de datos personales[189], y Nº 1.266, de 31 de Diciembre de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.[190]

Además, aplican en la especie las Leyes Nº 1.273 de 4 de Enero de 2009, que modificó el Código Penal creando un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-, y preserva integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[191]; y Nº 57 de 5 de Junio de 1985, por la cual se ordena la publicidad de los actos y documentos oficiales.[192]

A un nivel ya más particular, encontramos las siguientes disposiciones relativas a la privacidad:

- Decreto Nº 886 de 13 de Mayo de 2014, por el cual se reglamenta el Artículo 25 de la Ley Nº 1581 de 2012, Relativo al Registro de Bases de Datos.[193]
- Resolución Nº 76.434, de 4 de Diciembre de 2012, emitida por la Superintendencia de Industria y Comercio, por el cual se deroga el contenido del Título V de la Circular Única de la Superintendencia de Industria y Comercio, sobre Acreditación, y se imparten instrucciones relativas a la protección de datos personales, en particular, acerca del cumplimiento de la Ley Nº 1266 de 2008, sobre reportes de información financiera,

[187] En: http://www.leychile.cl/Navegar?idNorma=190282
[188] En: http://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Constitucion_Politica_de_Colombia.htm
[189] En: http://www.sic.gov.co/recursos_user/documentos/normatividad/Leyes/2012/Ley_1581_2012.pdf
[190] En: http://www.elabedul.net/San_Alejo/Leyes/Leyes_2008/ley_1266_2008.php
[191] En: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf
[192] En: http://www.unal.edu.co/secretaria/normas/ex/L0057_85.pdf
[193] En: http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/13/DECRETO%20886%20DEL%2013%20DE%20MAYO%20DE%202014.pdf

crediticia, comercial, de servicios y la proveniente de terceros países, las cuales se incorporan en el citado Título.[194]

- Decreto Nº 2.952 de 6 de Agosto de 2010, por el cual se reglamentan los artículos 12 (sobre requisitos especiales para las fuentes de información) y 13 (aspectos relacionados con la permanencia de la información) de la Ley Nº 1266.[195]
- Decreto Nº 1.727 de 15 de Mayo de 2009, por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.[196]
- Resolución Nº 2.578 de 28 de Septiembre de 2007, emitida por la Ministra de Comunicaciones, por la cual se reglamenta el artículo 11 del Decreto Nº 2870 de 2007 y se dictan otras disposiciones, especial consideración en su Artículo 1º, literal c), que garantiza la inviolabilidad de las comunicaciones.[197]
- Decreto Nº 2.870 de 30 de Julio de 2007, por medio del cual se adoptan medidas para facilitar la convergencia de los Servicios y Redes en materia de Telecomunicaciones. [198]
- Resolución Nº 575 de 1 de Abril de 2002, emitida por el Presidente de la República de Colombia, por el cual se reglamenta la prestación de los servicios de comunicación personal, PCS, y se dictan otras disposiciones.[199]
- Ley Nº 527 de 18 de Agosto de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones, en sus artículos 2 (Definiciones) y 32 (Deberes de las entidades de certificación).[200]
- Ley Estatutaria Nº 270 de 15 de Marzo de 1996, de la Administración de Justicia, en su Artículo 95, sobre Tecnología al Servicio de dicha administración.[201]

Costa Rica

a) Constitución

La Constitución Política de la República de Costa Rica[202], en sus artículos 23 y 24 bis, dispone lo siguiente, respectivamente:

> "El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o

[194] En: http://www.sic.gov.co/documents/10157/353524/Resolucion_76434_2012.pdf/a757d909-3a7e-49a3-a172-71ef0d55d238

[195] En: http://www.sic.gov.co/recursos_user/documentos/normatividad/Decreto_2952_2010.pdf

[196] En: http://www.sic.gov.co/documents/10157/1557222/Decreto_1727_2009.pdf/7ebc2ce2-516d-4d4e-94a2-5a4f8744c022

[197] En: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=27571

[198] En: http://www.mintic.gov.co/portal/604/articles-3593_documento.pdf

[199] En: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6047

[200] En: http://www.supersociedades.gov.co/superintendencia/normatividad/leyes/Documents/Ley%20527%20de%201999.pdf

[201] En: http://www.secretariasenado.gov.co/senado/basedoc/ley_0270_1996.html

[202] En: http://www.costaricaweb.com/general/constitucion.htm

para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley"., y

"Toda persona tiene derecho a tener o no tener personalidad virtual, donde su presencia, contenido y proyección se encuentre regulada por cada una de ellas. No podrá ser utilizada con fines discriminatorios en perjuicio de su titular. El Estado garantizará que la información contenida en la personalidad virtual goce de la adecuada seguridad informática y jurídica, con exclusión de terceros no autorizados que pretendan obtenerla. El Estado podrá hacer uso del contenido de la personalidad virtual de las personas, previa autorización de éstas, siempre que se realice en beneficio y provecho de las mismas".

Normativa

Como normas de general aplicación encontramos la Ley Nº 8.968, de 7 de Julio de 2011, sobre Protección de la Persona frente al tratamiento de sus datos personales[203], y el Código Penal, particularmente en lo dispuesto en sus artículos 196 bis (Violación de datos personales), 217 bis (Fraude informático) y 229 bis (Alteración de datos y sabotaje Informático).[204]

Luego, a nivel más específico, existe el Decreto Ejecutivo Nº 37.554-JP, del 30 de Octubre de 2012, que contiene el Reglamento de la Ley Nº 8968[205]; y la Directriz Nº 046-H-MICITT, de 9 de Abril de 2013, emitida por la Presidenta de la República y los Ministros de Hacienda y el de Ciencia, Tecnología y Telecomunicaciones, sobre computación en la nube en las instituciones públicas.[206]

Ecuador

a) Constitución

El artículo 11 de la Constitución Política de la República de Ecuador[207] , establece que "EI ejercicio de los derechos se regirá por los siguientes principios: Nº 9: El más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución, lo cual implica la obligación estatal de adecuar formal y materialmente, las leyes y normas de inferior jerarquía a la Constitución y los instrumentos internacionales, e implementar las normas que sean necesarias para garantizar la dignidad del ser humano".

En tanto, el artículo 66 reconoce y garantiza a las personas:

"Nº 19: El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Nº 20: El derecho a la intimidad personal y familiar.

[203] En: http://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf
[204] En: http://www.tse.go.cr/pdf/normativa/codigopenal.pdf
[205] En: http://www.tse.go.cr/pdf/normativa/reglamentoleyproteccionpersona.pdf
[206] En: http://www.camtic.org/download/proyectos_de_ley/Directriz_046_H_MICITT.pdf
[207] En: http://cancilleria.gob.ec/wp-content/uploads/2013/06/constitucion_2008.pdf

Nº 21: El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación".

En tanto, el artículo 92, señala que:

"Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados".

Normativa

Aquí encontramos las siguientes leyes generales: Ley Nº 52, de 21 de Septiembre de 2009, Orgánica de Garantías Jurisdiccionales y Control Constitucional la cual establece en su Capítulo VI La Acción de Hábeas Data[208]; y Ley Orgánica de Transparencia y Acceso a la Información Pública, de 18 de mayo de 2004.[209]

En cuanto a regulación particular:

- Ley Nº 162 de 31 de Marzo de 2010, del Sistema Nacional de Registro de Datos Públicos.[210]
- Ley Nº 843 de 28 de Noviembre de 2012, Orgánica Derogatoria a la Ley de Burós de Información Crediticia y Reformatoria a la Ley del Sistema Nacional del Registro de

[208] En: http://www.asambleanacional.gob.ec/system/files/ley_organica_de_garantias_jurisdiccionales_y_control_constitucional.pdf

[209] En: http://www.ecuadorestrategicoep.gob.ec/images/leytransparencia/LOTAIP.pdf

[210] En: http://www.asambleanacional.gob.ec/system/files/ley_del_sistema_nacional_de_datos_publicos_de_los_registros_de_la_propiedad_mercantiles_y_de_prendas_especiales_de_comercio-1.pdf

Datos Públicos, A la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario y a la Ley de Compañías.[211]

- Ley Nº 67 de 17 de abril de 2002, Comercio Electrónico, Firmas y Mensajes de Datos, en su artículo 9.[212]
- Ley Nº 184, de 10 de agosto de 1992, Especial de Telecomunicaciones, en lo relativo a sus artículos 1, 14 y 39.[213]

El Salvador

a) Constitución

Su Carta Fundamental[214] dispone, en el artículo 2º, que "Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

Normativa

En materia de normativa general encontramos la siguiente:

- Decreto Legislativo Nº 618 de 28 de Enero de 2014, que reforma la Ley Especial para la Intervención de las Telecomunicaciones. Su artículo 8º se refiere a la autorización de la intervención telefónica en caso de investigación de delitos cometidos por menores de edad.[215]
- Decreto Legislativo Nº 695 de 29 de Abril de 2012, Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las Personas. Contiene disposiciones tendientes a garantizar los derechos de los consumidores en el tema de la confiabilidad, y buen manejo de datos, relativos a su historial crediticio.[216]
- Decreto Legislativo Nº 534 de 30 de Marzo de 2011, Ley de Acceso a la Información Pública, en cuyo Título III se encuentra regulada la Protección de Datos Personales.[217]
- Decreto Legislativo Nº 285 de 18 de Febrero de 2010, Ley Especial para la Intervención de las Telecomunicaciones. Tiene por objeto garantizar el secreto de las telecomunicaciones y el derecho a la intimidad, no obstante lo cual señala que, de manera excepcional, podrá autorizarse judicialmente, por escrito y motivadamente la intervención temporal de las telecomunicaciones.

[211] En: http://www.asambleanacional.gob.ec/system/files/ley_derogatoria_de_la_ley_de_buros_de_informacion_crediticia_tramite_no.pdf

[212] En: http://www.oas.org/juridico/PDFs/mesicic4_ecu_comer.pdf

[213] En: http://www.cnt.gob.ec/images/Pdfs/lotaip/ley_especial_telecomunicaciones.pdf

[214] En: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/constitucion-de-la-republica

[215] En: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/reformase-el-art.-8-de-la-ley-especial-para-la-intervencion-de-las-telecomunicaciones

[216] En: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-regulacion-de-los-servicios-de-informacion-sobre-el-historial-de-credito-de-las-personas

[217] En: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-acceso-a-la-informacion

- Decreto Legislativo Nº 1.030 de 26 de Abril de 1997, Código Penal, en su Capítulo II se encuentran los delitos relativos a la intimidad.[218]

Las siguientes corresponden a regulaciones de carácter específico:

- Decreto Legislativo Nº 647, de 9 de Abril de 2014, Ley de Desarrollo y Protección Social, en especial sus Artículos 35 literal h) y 50 literal d).[219]
- Decreto Nº 136, de 1 de Septiembre de 2012, Reglamento de la Ley de Acceso a la Información Pública.[220]
- Decreto Legislativo Nº 695 de 27 de Julio de 2011, Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las Personas.
- Decreto Legislativo Nº 166 de 8 de Septiembre de 2005, Ley Protección al Consumidor, artículos 18 literal g), y 21.[221]
- Decreto Legislativo Nº 142 de 6 de Noviembre de 1997, Ley Telecomunicaciones en su artículo 29 literal b).[222]

Guatemala

a) Constitución

El artículo 24 de su Constitución Política[223], establece la inviolabilidad de la correspondencia, documentos y libros, en los siguientes términos:

[218] En: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/codigo-penal

[219] "Art. 35: Las personas beneficiarias de los programas sociales tendrán los siguientes derechos: (…) h) Gozar de la protección y confidencialidad de los datos personales", y "Art. 50: En el marco de la Ley de Acceso a la Información Pública y con el fin de fortalecer la transparencia y la rendición de cuentas de la política de desarrollo, protección e inclusión social, será de acceso público al menos lo siguiente: (…) d) La información agregada de los registros de los beneficiarios de los programas de transferencias monetarias o de bienes materiales, siempre y cuando no contengan información relativa a datos confidenciales; en todo caso, se respetarán las normas del secreto estadístico". En: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-desarrollo-y-protecion-social/archivo_documento_legislativo

[220] En: http://www.mh.gob.sv/portal/page/portal/PMH/LAIP/LAIP/Reglamento_de_la_Ley_de_Acceso_a_la_Informacion_Publica.pdf

[221] "Art. 18.- Queda prohibido a todo proveedor: (…) Compartir información personal y crediticia del consumidor, ya sea entre proveedores o a través de entidades especializadas en la prestación de servicios de información, sin la debida autorización del consumidor" y "Art. 21. - Las entidades especializadas en la prestación de servicios de información estarán obligadas a permitir al consumidor el acceso a la información de sus datos, así como a solicitar la actualización, modificación y eliminación de los mismos, de forma gratuita. Asimismo, tendrán la obligación de corregir la información falsa, no actualizada o inexacta en un plazo máximo de diez días contados a partir de la recepción de la solicitud del interesado. Las entidades especializadas a las que se refiere el presente artículo, no podrán obtener ninguna clase de información personal del consumidor, si no es con la debida autorización de éste, y únicamente en las condiciones en que la misma haya sido conferida". En: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-proteccion-al-consumidor

[222] "Art. 29.- Son derechos de los usuarios: (…) b) AL SECRETO DE SUS COMUNICACIONES Y A LA CONFIDENCIALIDAD DE SUS DATOS PERSONALES NO PÚBLICOS, TENIENDO EN CUENTA LO MENCIONADO EN EL TITULO V-BIS, CAPÍTULO ÚNICO DE LA PRESENTE LEY; (9)" En: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-telecomunicaciones

> "La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.
>
> Los libros, documentos y archivos que se relacionan con el pago de impuestos, tasas, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley.
>
> Los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen prueba en juicio".

Más adelante, el artículo 30 se refiere a la publicidad de los actos administrativos, disponiendo que

> "Todos los actos de la administración son públicos. Los interesados tienen derecho a obtener, en cualquier tiempo, informes, copias, reproducciones y certificaciones que soliciten y la exhibición de los expedientes que deseen consultar, salvo que se trate de asuntos militares o diplomáticos de seguridad nacional, o de datos suministrados por particulares bajo garantía de confidencia".

Por último, el artículo 31, relativo al acceso a archivos y registros estatales señala que

> "Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización.
>
> Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".

Normativa

En el artículo 274, inciso D) del Código Penal (Decreto Nº 17-73 del Congreso de la República), se establece como un delito informático la creación de registros prohibidos, regulando que se impondrá prisión de 6 meses a 4 años y multa de Q.200 a Q.1,000, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Por su parte, el Decreto Nº 57, de 23 de Septiembre de 2008 del Congreso de la República, contiene la Ley de Acceso a la Información Pública, que contempla la protección de los datos personales, y en su Capítulo VI el Hábeas Data.[224]

Finalmente, incide también en materia de privacidad el Decreto Nº 06, de 10 de Marzo de 2003 del Congreso de la República, Ley de Protección al Consumidor y Usuario.[225]

---

[223] En: http://www.cc.gob.gt/index.php?option=com_content&view=article&id=219&Itemid=67

[224] En: http://www.minfin.gob.gt/laip_mfp/docs/decreto_5708b.pdf

Honduras

a) Constitución

La Constitución de la República de Honduras de 1982[226] "garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen", en su artículo 76.

Dicha carta fue modificada, entre otros, por el Decreto Legislativo N° 381 de 20 de Enero de 2006, que reformó el Capítulo I, del Título IV de la misma, reconociendo la garantía del Hábeas Data. Así, el artículo 182 dispone que:

> "El Estado reconoce la garantía de Hábeas Corpus o de exhibición Personal, y de Hábeas Data. En consecuencia en el Hábeas Corpus o exhibición Personal, toda persona agraviada o cualquiera otro en nombre de éste tiene derecho a promoverla; y en el Hábeas Data únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados de la manera siguiente:(...)
>
> 2) El Hábeas Data: Para obtener acceso a la información; impedir su transmisión o divulgación; rectificar datos inexactos o erróneos; actualizar información, exigir confidencialidad y la eliminación de información falsa; respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen. Esta garantía no afectará el secreto de las fuentes de información periodística.
>
> Las acciones de Hábeas Corpus o de Hábeas Data se ejercerán sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles e inhábiles y libres de costas. Únicamente conocerá de la garantía de Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia.
>
> Los titulares de los órganos jurisdiccionales no podrán desechar estas acciones constitucionales y tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad, la seguridad personal, el honor, la intimidad personal, familiar o la propia imagen.
>
> Los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones incurrirán en responsabilidad penal y administrativa.
>
> Las autoridades que ordenaren y los agentes que ejecutaren el ocultamiento del detenido o que en cualquier forma quebranten esta garantía incurrirán en el delito de detención ilegal".

Normativa

[225] En: http://www.wipo.int/wipolex/en/text.jsp?file_id=235835

[226] En: http://www.wipo.int/edocs/lexdocs/laws/es/hn/hn003es.pdf

En esta área encontramos el Decreto Legislativo Nº 170, de 30 de Diciembre de 2006, que contiene la Ley de Transparencia y Acceso a la Información Pública, incidiendo en materia de privacidad, en especial, sus artículos 2 Nº 6, 13 Nº 14, 17 y los contenidos de su Capitulo V, denominado "Datos Personales y Hábeas Data"[227].

México

Hacemos presente que, si bien en este caso también se trata de un Estado federado, sólo nos referiremos a su normativa nacional y leyes federales más representativas.

a) Constitución

El artículo 6º de la Constitución Política de los Estados Unidos Mexicanos[228] señala que:

> "La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.
>
> Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.
>
> El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.
>
> Para efectos de lo dispuesto en el presente artículo se observará lo siguiente:

[227] "ARTICULO 2. OBJETIVOS DE LA LEY. Son objetivos de esta Ley establecer los mecanismos para: (…) 6. Garantizar la protección, clasificación y seguridad de la información pública y el respeto a las restricciones de acceso en los casos de: a) Información clasificada como reservada por las entidades públicas conforme a esta ley, b) información entregada al Estado por particulares, en carácter de confidencialidad, c) los datos personales confidenciales; y, d) la secretividad establecida por ley".; "ARTÍCULO 13. INFORMACIÓN QUE DEBE SER DIFUNDIDA DE OFICIO. Toda Institución Obligada está en el deber de difundir de oficio y actualizar periódicamente a través de medios electrónicos o instrumentos computarizados; a falta de éstos, por los medios escritos disponibles, la información siguiente: (…) 14) El Poder Judicial, publicará además, las sentencias judiciales firmes que hayan causado estado o ejecutoria, sin perjuicio del derecho que tienen las partes para oponerse a la publicación de sus datos personales;"; y "ARTÍCULO 17. CLASIFICACIÓN DE LA INFORMACIÓN COMO RESERVADA. Sin perjuicio de lo dispuesto en la Ley sobre la secretividad de datos y procesos y confidencialidad de datos personales y de información entregada por particulares al Estado bajo reserva; la clasificación de la información pública como reservada procede cuando el daño que puede producirse, es mayor que el interés público de conocer la misma o cuando la divulgación de la información ponga en riesgo o perjudique: 1) La seguridad del Estado; 2) La vida, la seguridad y la salud de cualquier persona, la ayuda humanitaria, los intereses jurídicamente tutelados a favor de la niñez y de otras personas o por la garantía de Habeas Data; 3) El desarrollo de investigaciones reservadas en materia de actividades de prevención, investigación o persecución de los delitos o de la impartición de justicia; 4) El interés protegido por la Constitución y las Leyes; 5) La conducción de las negociaciones y las relaciones internacionales; y, 6) La estabilidad económica, financiera o monetaria del país o la gobernabilidad". En: http://www.ccit.hn/wp-content/uploads/2013/12/LEY-DE-TRANSPARENCIA-Y-ACCESO-A-LA-INFORMACION1.pdf

[228] En: http://www.ordenjuridico.gob.mx/Constitucion/cn16.pdf

A. Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: (…)

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes".

Luego, el artículo 16, incisos 1º, 2º y 12º señalan, respectivamente: "Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (…)

Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley".

Y, por último, el artículo 73 se refiere a la facultad del Congreso "XXIX-O: Para legislar en materia de protección de datos personales en posesión de particulares".

Normativa

En cuanto a normativa de aplicación general encontramos la Ley Federal de 5 de Junio de 2010, de Protección de Datos Personales en Posesión de los Particulares, mediante la cual se reforman los artículos 3º, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.[229] También, ha de hacerse mención al Código Federal Penal, Título IX, Capítulo I, Artículos 210 y siguientes, sobre "Revelación de Secretos".[230]

Ya en un ámbito más específico, es posible identificar la siguiente normativa:

- Reglamento de 21 de Abril de 2014, Interno del Comité de Información del Instituto Federal de Acceso a la Información y Protección de Datos.[231]
- Reglamento de 20 de Febrero de 2014, Interno del Instituto Federal de Acceso a la Información y Protección de Datos.[232]

[229] En: http://inicio.ifai.org.mx/LFPDPPP/LFPDPPP.pdf

[230] En: http://www.wipo.int/edocs/lexdocs/laws/es/mx/mx034es.pdf

[231] En: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/ReglamentoInternodelComit%C3%A9deInformaci%C3%B3ndelIFAI.pdf

[232] En: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Nvo-Reg-Int-2014-20-02-14.pdf

- Reglamento de 21 de Diciembre de 2011, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.[233]
- Reglamento de 11 de Junio de 2003, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.[234]
- Ley Federal de 11 Junio 2002, de Transparencia y Acceso a la Información Pública Gubernamental en especial su Capitulo IV de Protección de Datos Personales de su Título I.[235]
- Ley de 15 de Enero de 2002, Para Regular las Sociedades de Información Crediticia, en especial en sus artículos 1, 2, 18 y 38 a 50.[236]
- Ley Federal de 18 de Enero de 1999, de Protección y Defensa al Usuario de Servicios Financieros, en especial su artículo 8º inciso cuarto.[237]
- Ley Federal de 24 de Diciembre de 1992, de Protección al Consumidor, en especial sus artículos 1 Nº VII y 76 bis.[238]

Nicaragua

a) Constitución

El artículo 26 de la Carta Fundamental[239] señala que

> "Toda persona tiene derecho: 1) A su vida privada y a la de su familia. 2) A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo. 3) Al respeto de su honra y reputación. 4) A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información.
>
> El domicilio sólo puede ser allanado por orden escrita de juez competente, excepto: a) Si los que habitaren en una casa manifestaren que allí se está cometiendo un delito o de ella se pidiera auxilio; b) si por incendio, inundación u otra causa semejante, se hallare amenazada la vida de los habitantes o de la propiedad; c) cuando se denunciare que personas extrañas han sido vistas en una morada, con indicios manifiestos de ir a cometer un delito; d) en caso de persecución actual e inmediata de un delincuente; e) para rescatar a la persona que sufra secuestro.
>
> En todos los casos se procederá de acuerdo a la ley.
>
> La ley fija los casos y procedimientos para el examen de documentos privados, libros contables y sus anexos, cuando sea indispensable para esclarecer asuntos sometidos al conocimiento de los Tribunales de Justicia o por motivos fiscales.

[233] En: http://inicio.ifai.org.mx/PROTECCIONDEDATOSPERSONALES/RLFPDPP.pdf
[234] En: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/ReglamentoLFTAIPG_11062003.pdf
[235] En: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/05LFTAIPG.pdf
[236] En: http://www.diputados.gob.mx/LeyesBiblio/pdf/237.pdf
[237] En: http://www.diputados.gob.mx/LeyesBiblio/pdf/64.pdf
[238] En: http://www.profeco.gob.mx/juridico/pdf/LFPC_actuali_16ene2013.pdf
[239] En: http://www.ineter.gob.ni/Constitucion%20Politica%20de%20Nicargua.pdf

Las cartas, documentos y demás papeles privados sustraídos ilegalmente no producen efecto alguno en juicio o fuera de él".

Normativa

Respecto de la Ley Nº 831, de 14 de Febrero de 2013, de Reforma y Adiciones a la Ley No. 49, "Ley de Amparo"[240], la Asamblea Nacional de Nicaragua señaló que "con esta reforma se pretende la protección de la persona frente al tratamiento de sus datos personales, ya sea que estén almacenados en ficheros de datos públicos o privados, automatizados o no, garantizándoles el respeto a sus derechos constitucionales establecidos en el artículo 26, Inc. 4 párrafo segundo de la Constitución Política de Nicaragua, al mismo tiempo esta ley, regulará y facilitará los procesos legales y administrativos, para que el ciudadano pueda protegerse frente al tratamiento de sus datos"[241].

Luego, encontramos las Leyes Nº 787 de 29 de Marzo de 2012, de Protección de Datos Personales[242]; Nº 192 de 4 de Julio de 1995, de Reforma Parcial a la Constitución Política de la República de Nicaragua, que modifica entre otras disposiciones la del artículo 26[243], y Nº 729 de 30 de Agosto de 2010, de Firma Electrónica, en especial lo dispuesto por su artículo 25, sobre protección de los datos personales.[244]

Panamá

a) Constitución

El artículo 29 de la Carta Fundamental Panameña[245] dispone que

"La correspondencia y demás documentos privados son inviolables y no pueden ser examinados ni retenidos, sino por mandato de autoridad competente y para fines específicos, de acuerdo con las formalidades legales. En todo caso, se guardará absoluta reserva sobre los asuntos ajenos al objeto del examen o de la retención.

El registro de cartas y demás documentos o papeles se practicará siempre en presencia del interesado o de una persona de su familia o, en su defecto, de dos vecinos honorables del mismo lugar.

[240] En: http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/97be104652c1ab2a06257b2c00755fcf?OpenDocument

[241] Fragmento de la Exposición de Motivos durante la segunda sesión ordinaria de la Honorable Asamblea Nacional de Nicaragua, correspondiente el día 17 de abril del 2012. En: http://legislacion.asamblea.gob.ni/Diariodebate.nsf/76ed72912dd57e570625698c00773f5d/a30451f161d003d206257b5c006189f3?OpenDocument

[242] En: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d?OpenDocument

[243] En: http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/927804DC295D0AE5062573080056DA6D?OpenDocument

[244] En: http://www.bcn.gob.ni/sistema_pagos/documentos/Ley_729_Ley_de_firma_electronica.pdf

[245] En: http://www.asamblea.gob.pa/main/LinkClick.aspx?fileticket=fDgmRvYW8cY%3D&tabid=123

Todas las comunicaciones privadas son inviolables y no podrán ser interceptadas o grabadas, sino por mandato de autoridad judicial.

El incumplimiento de esta disposición impedirá la utilización de sus resultados como pruebas, sin perjuicio de las responsabilidades penales en que incurran los autores".

Por su parte, el artículo 42 se refiere al hecho que

"Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley.

Esta información sólo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la Ley".

En tanto la siguiente norma (artículo 43) se refiere a que:

"Toda persona tiene derecho a solicitar información de acceso público o de interés colectivo que repose en bases de datos o registros a cargo de servidores públicos o de personas privadas que presten servicios públicos, siempre que ese acceso no haya sido limitado por disposición escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación".

Luego, el artículo 44 se refiere al habeas data en los siguientes términos:

"Toda persona podrá promover acción de hábeas data con miras a garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información.

Esta acción se podrá interponer, de igual forma, para hacer valer el derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en esta Constitución.

Mediante la acción de hábeas data se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal.

La Ley reglamentará lo referente a los tribunales competentes para conocer del hábeas data, que se sustanciará mediante proceso sumario y sin necesidad de apoderado judicial".

Normativa

En este orden podemos identificar las siguientes leyes:

- Ley Nº 51, de 23 de Septiembre de 2009, que dicta Normas para la Conservación, la Protección y el Suministro de Datos de Usuarios de los Servicios de Telecomunicaciones y adopta otras disposiciones.[246]

[246] En: http://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf

- Ley Nº 6 de 22 de Enero de 2002, que dicta normas para la Transparencia en la gestión pública, establece la acción de Habeas Data y otras disposiciones.[247]
- Ley Nº 24 de 22 de Mayo de 2002, que regula el servicio de información sobre el historial de crédito de los consumidores o clientes, en especial en sus artículos 1, 23, 30, 39 y 40.[248]
- Ley Nº 3 de 5 de Enero de 2000, General sobre las infecciones de transmisión sexual, el virus de la inmunodeficiencia humana y el sida, en especial sus artículo 35 y 37.[249]

Paraguay

a) Constitución

La Carta de 1992[250], se refiere al derecho a la intimidad en el artículo 33, en los siguientes términos:

> "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas".

En tanto, el artículo 36, sobre Derecho a la Inviolabilidad del Patrimonio Documental y la Comunicación Privada, señala

> "El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades. La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios.

Las pruebas documentales obtenidas en violación a lo prescripto anteriormente carecen de valor en juicio.

En todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado".

El Hábeas Data se encuentra regulado en el artículo 135, en los siguientes términos:

> "Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado

[247] En: http://www.css.gob.pa/Ley%206%20de%2022%20de%20enero%20de%202002.pdf
[248] En: https://www.apc.com.pa/wp-content/uploads/2013/11/Ley_24_sobre_historial_de_credito1.07_21_2009_10_16_41_a.m..pdf
[249] En: http://www.legalinfo-panama.com/legislacion/salud/ley032000.pdf
[250] En: http://www.tsje.gov.py/descargar.php?a=pdf/constitucion_de_1992.pdf

competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos".

Normativa

Las Leyes Nº 3.440 de 16 de Julio de 2008 y Nº 4.439 de 3 de Octubre de 2011 modifican varias disposiciones de la Ley Nº 1160 de 26 de Noviembre de 97, Código Penal. La primera de ellas modifica el artículo 143, sobre lesión de la intimidad de la persona[251]; en tanto la segunda combate los Delitos Informáticos, modifica y amplia varias disposiciones del Código Penal.[252]

Finalmente se ha de mencionar la Ley Nº 1.969 de 3 de Septiembre de 2002,[253] que modifica, amplía y deroga varios artículos de la Ley Nº 1.682 de 16 de Enero de 2001, que reglamenta la información de carácter privado, y el acceso a los datos e informaciones personales que se encuentren asentados en los registros públicos.[254]

A nivel más específico, encontramos la siguiente normativa:

- Decreto Nº 1.165 de 27 de Enero de 2014, por el que se aprueba el Reglamento de la Ley Nº 4.868, de Comercio Electrónico, en especial en sus artículos 11, 12 y 13.[255]
- Ley Nº 4.868 de 26 de Febrero de 2013, de Comercio Electrónico, en particular sus artículos 6 literal e), 7 literal b) y 36 Nº 1 literal c)[256]
- Ley Nº 4.610 de 9 de Mayo de 2012, que modifica y amplía la Ley Nº 4017 de 23 de Diciembre de 2010, en especial en su artículo 44 literal d).[257]
- Decreto Nº 7.369 de 23 de Septiembre de 2011, por el que se aprueba el Reglamento de la Ley Nº 4.017 de 23 de Diciembre de 2010.[258]
- Ley Nº 4.017 de 23 de Diciembre de 2010, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico, en especial en su artículo 34.[259]

Perú

a) Constitución[260]

El numeral 5º del artículo 2º señala que toda persona tiene derecho "A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal,

[251] En: http://www.bacn.gov.py/OTM1&ley-n-3440
[252] En: http://www.redipd.org/legislacion/common/legislacion/paraguay/Ley_4439.pdf
[253] En: https://www.informconf.com.py/docs/Ley_1969.pdf
[254] En: http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=1760
[255] En: http://www.redipd.org/legislacion/common/legislacion/paraguay/Decreto_N_1165.pdf
[256] En: http://www.eljurista.com.py/admin/publics/upload/archivos/ea41b40fb8ce27bd7ec64237fd75ef89.pdf
[257] En: http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=216
[258] En: http://www.acraiz.gov.py/index.php/descargas/finish/3-leyes-a-decretos/2-decreto-n-7369-q-por-el-cual-se-aprueba-el-reglamento-general-de-la-ley-n-4017-de-validez-juridica-de-la-firma-electronica-la-firma-digital-los-mensajes-de-datos-y-el-expediente-electronico-/0
[259] En: http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=490
[260] En: http://www.tc.gob.pe/legconperu/constitucion.html

con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado".

Luego, el numeral 6 de la misma disposición señala que también tienen derecho "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". En tanto el Nº 7, se refiere "Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley".

Conforme dispone el artículo 162 de la misma Constitución "Corresponde a la Defensoría del Pueblo defender los derechos constitucionales y fundamentales de la persona y de la comunidad; y supervisar el cumplimiento de los deberes de la administración estatal y la prestación de los servicios públicos a la ciudadanía…"

Finalmente, el artículo 200 señala que: "Son garantías constitucionales:(…) Nº 3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2º, incisos 5) y 6) de la Constitución".

Normativa

En este ámbito encontramos las Leyes Nº 30.096 de 21 de octubre de 2013, de Delitos informáticos, resultando de especial importancia su Capítulo IV de Delitos Informáticos contra la Intimidad y el Secreto de las Comunicaciones[261]; y Nº 30.171 de 9 de Marzo de 2014, por la que se modifican diversas disposiciones de la mencionada Ley de Delitos Informáticos, debiendo prestarse especial atención a la incorporación del Artículo 154-A de Tráfico ilegal de datos personales.[262]

Luego encontramos diversas leyes de aplicación general, tales como: la Ley Nº 29.733 de 3 de Julio de 2011, de Protección de Datos Personales; Ley Nº 28.237 de 31 de Mayo de 2004, Código Procesal Constitucional, en especial en su Título IV de Hábeas de Data[263]; Ley Nº 27.806 de 3 de Agosto de 2002, de Transparencia y Acceso a la Información Pública; Ley Nº 27.309 de 17 de julio de 2000, que incorpora los delitos informáticos al Código Penal[264]; Decreto Legislativo Nº 635 de 8 de Abril de 1991, Código Penal, en especial en su Título IV, Capítulos II, III, IV y V y Título V, Capítulo X265; y Decreto Legislativo Nº 295 de 25 de Julio de 1984, Código Civil, cuyo artículo 14 se refiere al Derecho a la Intimidad Personal y Familiar señalando que "La intimidad

[261] En: http://www.informatica-juridica.com/anexos/Ley_30096_21_octubre_2013_Ley_Delitos_Informaticos.asp
[262] En: http://www.informatica-juridica.com/anexos/Ley_30171_9_marzo_2014_modifica_Ley_30096_Ley_delitos_informaticos.asp
[263] En: http://www.tc.gob.pe/Codigo_Procesal.html
[264] En: http://www.oas.org/juridico/spanish/cyb_per_ley_27309.pdf
[265] En: http://spij.minjus.gob.pe/CLP/contenidos.dll?f=templates&fn=default-codpenal.htm&vid=Ciclope:CLPdemo

de la vida personal y familiar no puede ser puesta de manifiesto sin el asentimiento de la persona o si ésta ha muerto, sin el de su cónyuge, descendientes, ascendientes o hermanos, excluyentemente y en este orden".[266]

En cuanto a regulación de carácter específico, podemos mencionar:

- Resolución Directoral Nº 003-2014-JUS de la Dirección General de Protección de Datos Personales de 20 de Enero de 2014, de la solicitud de Inscripción de Código de Conducta.[267]
- Ley Nº 30.120 de 5 de Diciembre de 2013, Ley de apoyo a la seguridad ciudadana con cámaras de video vigilancia públicas y privadas.[268]
- Resolución Directoral Nº 29-2013-JUS de la Dirección General de Protección de Datos Personales de 18 de Noviembre de 2013, que aprueba el formulario de consulta al contenido del Registro Nacional de Protección de Datos Personales.[269]
- Resolución Directoral de la Dirección General de Protección de Datos Personales de 11 de Octubre de 2013, Nº 019-2013-JUS que aprueba la "Directiva de Seguridad de la Información Administrada por los Bancos de Datos", que orienta sobre las condiciones, los requisitos y las medidas técnicas que se deben tomar en cuenta para el cumplimiento de la Ley Nº 29.733, de Protección de Datos Personales y su Reglamento, aprobado a través del Decreto Supremo Nº 003-2013-JUS, en materia de medidas de seguridad de los bancos de datos[270]; y Directiva de Seguridad de la Información de la misma fecha, emitida por la Autoridad Nacional de Protección de Datos Personales, referida a la misma materia.[271]
- Resoluciones Directorales de la Dirección General de Protección de Datos Personales, todas de 8 de Agosto de 2013: Nº 13-2013-JUS que aprueba el formulario de solicitud de opinión sobre la realización de flujo transfronterizo de datos personales[272]; Nº 12-2013-JUS que aprueba el formulario de modificación de banco de datos personales y el formulario de cancelación de banco de datos personales[273]; Nº 11-2013-JUS que aprueba el formulario de solicitud de procedimiento trilateral de tutela[274]; Nº 10-2013-JUS que aprueba el formulario de absolución de consulta sobre protección de datos personales.[275]
- Decreto Supremo Nº 070-2013-PCM de 13 de Junio de 2013, que modifica el Reglamento de la Ley de Transparencia y Acceso a la Información Pública aprobado por Decreto Supremo Nº 72-2003-PCM.
- Resoluciones Directorales de la Dirección General de Protección de Datos Personales de 31 de Mayo de 2013: Nº 003-2013-JUS que aprueba el formulario de comunicación de realización de flujo transfronterizo de datos personales[276]; Nº 002-2013-JUS que

[266] En: http://www.oas.org/juridico/PDFs/mesicic4_per_cod_civil.pdf
[267] En: http://www.minjus.gob.pe/wp-content/uploads/2014/01/RD-N%C2%B0-003.pdf
[268] En: http://www.congreso.gob.pe/ntley/Imagenes/Leyes/30120.pdf
[269] En: http://www.minjus.gob.pe/wp-content/uploads/2013/12/RD-29-2.pdf
[270] En: http://www.minjus.gob.pe/wp-content/uploads/2013/10/RD-Directiva-de-Seguridad.pdf y su fe de erratas en: http://www.minjus.gob.pe/wp-content/uploads/2013/11/Resoluciones_11.pdf
[271] En: http://sistemas3.minjus.gob.pe/transparencia2/directiva-de-seguridad.pdf
[272] En: http://www.minjus.gob.pe/wp-content/uploads/2013/11/RD-13.pdf
[273] En: http://www.minjus.gob.pe/wp-content/uploads/2013/11/RD-12.pdf
[274] En: http://www.minjus.gob.pe/wp-content/uploads/2013/11/RD-11.pdf
[275] En: http://www.minjus.gob.pe/wp-content/uploads/2013/11/RD-10.pdf
[276] En: http://www.minjus.gob.pe/wp-content/uploads/2013/12/Resolucion-N-3.pdf

aprueba el formulario de denuncia por actos contrarios a la Ley de Protección de Datos Personales y su reglamento, aprobado por Decreto Supremo Nº 003-2013-JUS.[277]

- Ley Nº 30.024 de 22 de Mayo de 2013, por la que se crea el Registro Nacional de Historias Clínicas Electrónicas.[278]
- Decreto Supremo Nº 003-2013-JUS de 21 de Marzo de 2013, por el que se aprueba el Reglamento de la Ley de Protección de Datos Personales.[279]
- Ley Nº 29.499 de 19 de Enero de 2010, que establece la vigilancia electrónica personal.[280]
- Resolución Ministerial 111-2009 MTC/03 de 7 de febrero de 2009, emitida por el Ministerio de Trasportes y Comunicaciones, que salvaguarda derecho a la inviolabilidad y secreto de las telecomunicaciones y Protección Datos Personales y regula las acciones de supervisión y control a cargo del Ministerio de Transportes y Comunicaciones.[281]
- Ley Nº 29.246 de 24 de Junio de 2008, que modifica la Ley Nº 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM).[282]

República Dominicana

a) Constitución

La Constitución del año 2010[283] establece en el artículo 44, sobre Derecho a la intimidad y el honor personal que

> "Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley. Por tanto: (...)
>
> Nº 2: Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos;
>
> Nº 3: Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente,

[277] En: http://www.minjus.gob.pe/wp-content/uploads/2013/12/Resolucion-N-2.pdf
[278] En: http://www.redipd.org/legislacion/common/legislacion/peru/Ley_30024.pdf
[279] En: http://www.minjus.gob.pe/normatividad/DS2013/DS-003-2013-JUS.pdf
[280] En: http://www.congreso.gob.pe/ntley/Imagenes/Leyes/29499.pdf
[281] En:
http://www.mtc.gob.pe/portal/comunicacion/politicas/normaslegales/Aprueban%20la%20Norma%20que%20establece%20medidas%20destinadas%20a%20salvaguardar%20el%20derecho%20a%20la%20inviolavilidad%20y%20el%20secreto%20de%20las%20telecomunicaciones.pdf
[282] En: http://www.ongei.gob.pe/normas/ley_antispam_29246.pdf
[283] En: http://www.ifrc.org/docs/idrl/751ES.pdf

mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente, de conformidad con la ley;

Nº 4: El manejo, uso o tratamiento de datos e informaciones de carácter oficial que recaben las autoridades encargadas de la prevención, persecución y castigo del crimen, sólo podrán ser tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio, de conformidad con la ley".

Más adelante, el artículo 70 incorpora el Hábeas data en los siguientes términos: "Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística".

Normativa

La Ley Nº 172-13, de 13 de Diciembre de 2013, aborda la Orgánica de la Protección de Datos de Carácter Personal de la República Dominicana.[284]

Luego, a un nivel más específico, encontramos la Resolución Nº 7.150 de 18 de Septiembre de 2007, emitida por la Procuraduría General de la República para establecer las políticas para la correcta aplicación del reglamento sobre Registro de Datos de Personas con Antecedentes Delictivos[285]; la Ley Nº 53-07 del 23 de Abril de 2007, contra Crímenes y Delitos de Alta Tecnología, en especial en sus artículos 9 y 19[286]; el Decreto Nº 122-07 8 de Marzo de 2007, Reglamento sobre Registro de Datos de Personas con Antecedentes Delictivos[287]; la Resolución Nº 055-06 de 27 de Junio de 2006, emitida por el Instituto Dominicano de Telecomunicaciones sobre Protección de Datos de Carácter Personal por los Sujetos Regulados.[288]

Además de la Ley Nº 288-05 de 18 de Agosto de 2005, que regula las sociedades de intermediación crediticia y de protección al titular de la información[289]; el Decreto Nº 130-05 de 25 de Febrero de 2005, de Reglamento de la Ley General de Libre Acceso a la Información Pública[290]; la Ley General Nº 200-04 de 28 de Julio de 2004, sobre Libre Acceso a la Información Publica en especial sus Artículos 2, 17 literal k), 18 y 20[291], y la Ley General Nº 153-98 del 27 de Mayo de 1998, de Telecomunicaciones, en especial su Artículo 5.[292]

[284] En: http://www.sep.gob.do/base-legal/leyes/968-ley-172-13/download.html
[285] En: http://transparencia.pgr.gob.do/Repository/Documents/Marco_Legal/PGR/Resolucion_00057.pdf
[286] En: http://www.oas.org/juridico/PDFs/repdom_ley5307.pdf
[287] En: http://www.procuraduria.gov.do/PGR.NET/Transparencia/Documentos/LEY_122-07.pdf
[288] En: http://www.procuraduria.gov.do/PGR.NET/Transparencia/Documentos/7%20OF.00055.pdf
[289] En: http://www.oas.org/es/sla/ddi/docs/RD4%20Ley%20N%20288-05%20de%202005.pdf
[290] En: http://www.infotep.gov.do/pdf_prog_form/decreto_130-05.pdf
[291] En: http://www.hacienda.gov.do/transparencia/02marco_legal_sistema_transparencia/01leyes/Ley%20No.%20200-04%20Libre%20Acceso%20a%20la%20Informaci%C3%B3n%20P%C3%BAblica.pdf
[292] En: http://www.wipo.int/edocs/lexdocs/laws/es/do/do053es.pdf

Uruguay

a) Constitución

La Constitución de la República Oriental de Uruguay[293] contiene varias normas de este rango referidas a privacidad.

Así el artículo 7º señala que "Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad. Nadie puede ser privado de estos derechos sino conforme a las leyes que se establecen por razones de interés general".

Luego el artículo 11 se refiere a la inviolabilidad del hogar "El hogar es un sagrado inviolable. De noche nadie podrá entrar en él sin consentimiento de su jefe, y de día, sólo de orden expresa de Juez competente, por escrito y en los casos determinados por la ley".

A su turno, el artículo 28 trata sobre la inviolabilidad de la correspondencia: "Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general".

Normativa

Tres leyes principales se vinculan con el derecho a la privacidad, a saber: la Ley Nº 19.030 de 7 de Enero de 2013, mediante la cual se aprueba el Convenio Nº 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional[294]; la Ley Nº 18.381 de 17 de Octubre de 2008, de Derecho de Acceso a la Información Pública[295], y la Ley Nº 18.331 de 18 de Agosto de 2008, de Protección de Datos Personales y Acción de "Hábeas Data".[296]

A nivel de regulación específica encontramos:

- Ley Nº 18.812 de 7 de Septiembre de 2011, Regulación de la Central de Riesgos Crediticios del Banco Central por la Ley Nº 18.331 de Protección de Datos Personales.[297]
- Decreto de Protección de Datos Nº 414/2009 de 31 de agosto de 2009, Reglamentario de la Ley Nº 18.331 de Protección de Datos Personales y Acción de Habeas Data.[298]

[293] En: http://www.parlamento.gub.uy/constituciones/const004.htm
[294] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/752242004ea5bb618d38cde117ffa227/Descargar+Ley+N%C2%B0+19030.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=752242004ea5bb618d38cde117ffa227
[295] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/045592004d0aece2882fcafd6066fd91/Descargar+Ley+N%C2%B0+18.381.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=045592004d0aece2882fcafd6066fd91
[296] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/829161004d0a999d861fcefd6066fd91/Descargar+Ley+N%C2%B0+18.331.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=829161004d0a999d861fcefd6066fd91
[297] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/d2d296804d0aa0f4869ecefd6066fd91/Descargar+Ley+N%C2%B0+18.812.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=d2d296804d0aa0f4869ecefd6066fd91

- Ley Nº 18.335 de 26 de Agosto de 2008, Pacientes y Usuarios de los Servicios de Salud, la cual establece sus derechos y obligaciones, en especial en sus Artículos 17 literal E) y 21.[299]
- Ley Nº 18.244 de 27 de Diciembre de 2007, se establecen normas para el tratamiento de datos de los deudores alimentarios morosos.[300]
- Decreto de Protección de Datos Nº 399/006 de 30 de Octubre de 2006, se crea el Registro de Bases de datos, archivos, registros y otros medios similares autorizados, destinados a brindar informes de carácter comercial.[301]
- Decreto de Protección de Datos Nº 246/005 de 8 de Agosto de 2005. Se incorpora la Resolución Nº 21/04 del Grupo Mercado Común, por la cual se regula el derecho a la información del consumidor en las transacciones comerciales efectuadas por Internet.[302]
- Decreto de Protección de Datos Nº 131/005 de 11 de Abril de 2005. Se incorpora la Decisión Nº 13/04 del Consejo Mercado Común, por el cual se regula el intercambio de información a través de sistemas informáticos entre las Administraciones aduaneras del MERCOSUR.[303]
- Decreto de Protección de Datos Nº 37/005 de 27 de Enero de 2005, Regula la destrucción de historias clínicas y la aplicación de tecnología informática. Modifica en los artículos 4 y 11 el Decreto 355/982.[304]
- Ley Nº 17.835 de 23 de Septiembre de 2004, Limitante relativa a la normativa sobre secreto, en su Artículo 1.[305]
- Decreto de Protección de Datos Nº 396/003 de 20 de Septiembre de 2003, Trata acerca de los datos personales relativos a la salud.[306]

---

[298] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/11c874804d1a397b9d83dffd6066fd91/Descargar+Decreto-414-009.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=11c874804d1a397b9d83dffd6066fd91

[299] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/8679cc804d0aef15883ecafd6066fd91/Descargar+Ley+N%C2%B0+18.335.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=8679cc804d0aef15883ecafd6066fd91

[300] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/126052804d0af1bb8854cafd6066fd91/Descargar+Ley+N%C2%B0+18.244.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=126052804d0af1bb8854cafd6066fd91

[301] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/9afb60004d1a4c369e1bdefd6066fd91/Descargar+Decreto+399-006.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=9afb60004d1a4c369e1bdefd6066fd91

[302] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/76ca7c804d1a4d259e2bdefd6066fd91/Descargar+Decreto+246-005.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=76ca7c804d1a4d259e2bdefd6066fd91

[303] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/bb056c004d1a4e4e9e4ddefd6066fd91/Descargar+Decreto+131-005.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=bb056c004d1a4e4e9e4ddefd6066fd91

[304] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/fcf6f5004d1a4fa99e67defd6066fd91/Descargar+Decreto+37-005.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=fcf6f5004d1a4fa99e67defd6066fd91

[305] En:
http://www.datospersonales.gub.uy/wps/wcm/connect/5071b5004d0af4e08873cafd6066fd91/Descargar+Art%C3%ADculo+1+de+la+Ley+N%C2%B0+17.835.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=5071b5004d0af4e08873cafd6066fd91

- Decreto de Protección de Datos Nº 664/008 de 22 de Diciembre de 2008, Regula la inscripción de las Bases de Datos Personales que brindan informes objetivos de carácter comercial.
- Decreto de Protección de Datos Nº 379/008 de 4 de Agosto de 2008, por el cual se regula sobre la investigación con seres humanos, en especial en su artículo 1.[307]
- Decreto de Protección de Datos Nº 250/007 de 9 de Julio de 2007, se regulan aspectos relativos al derecho a la identidad del niño y su identificación desde el nacimiento.[308]
- Decreto de Protección de Datos Nº 249/007 de 9 de Julio de 2007, se regulan aspectos del uso de la tecnología informática en la identificación de personas.[309]

Venezuela

a) Constitución

El artículo 28 de la Constitución de la República Bolivariana de Venezuela[310] dispone que:

> "Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley".

En el artículo 60, se dispone que

> "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación.
>
> La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos".

Finalmente, destaca que el artículo 281, referido a las atribuciones del Defensor o Defensora del Pueblo incluyen "Nº 3: Interponer las acciones de inconstitucionalidad, amparo, hábeas corpus,

---

[306] En: http://www.datospersonales.gub.uy/wps/wcm/connect/fd7ad0004d1a51e39e7bdefd6066fd91/Descargar+Decreto+396-003.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=fd7ad0004d1a51e39e7bdefd6066fd91

[307] En: http://www.datospersonales.gub.uy/wps/wcm/connect/0feda2004d1a42e79daedffd6066fd91/Descargar+Decreto-379-008.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=0feda2004d1a42e79daedffd6066fd91

[308] En: http://www.datospersonales.gub.uy/wps/wcm/connect/c9c069004d1a459a9de9dffd6066fd91/Descargar+Decreto+249-007.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=c9c069004d1a459a9de9dffd6066fd91

[309] En: http://www.datospersonales.gub.uy/wps/wcm/connect/c9c069004d1a459a9de9dffd6066fd91/Descargar+Decreto+249-007.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=c9c069004d1a459a9de9dffd6066fd91

[310] En: http://www.tsj.gov.ve/legislacion/constitucion1999.htm

hábeas data y las demás acciones o recursos necesarios para ejercer las atribuciones señaladas en los numerales anteriores, cuando fuere procedente de conformidad con la ley".

Normativa

En esta área destacan la Ley Nº 34.863 de 16 de Diciembre de 1991, sobre Protección a la Privacidad de las Comunicaciones[311], y la Ley de Reforma de la Ley Orgánica de Telecomunicaciones de 21 de Febrero de 2014.[312]

Además se agregan la Ley de Infogobierno de 17 de Septiembre de 2013, en especial sus artículos 25, 55 Nº 4, 74, 78 y 79[313]; Ley Especial contra Delitos Informáticos del 30 de Octubre de 2001, en especial en sus artículos 20 a 30[314]; y la Ley Orgánica de Telecomunicaciones de 12 de Junio de 2000, en especial en sus artículos 12 Nº 6, 20 Nº 8 y 50 Nº 2.[315]

3. Proyectos de ley

En este apartado sólo haremos mención de aquellos países en estudio que cuentan con información sobre proyectos, o anteproyectos, de ley, omitiéndose aquellos respecto de los cuales no existe información disponible.

Argentina

Los proyectos más recientes en tramitación son:

- Expediente Diputados 1508-D-13 del año 2013, Proyecto de Ley de Responsabilidad de los Proveedores de Servicios de Internet.[316]
- Expediente Diputados 8070-D-12 del año 2012, Proyecto de Ley de Responsabilidad de los Proveedores de Servicios de Intermediación en Internet.[317]
- Expediente Diputados 627-D-09 reproducción de Expediente 623-D-07 del año 2009, Proyecto de Ley de Incorporación del artículo 86 bis de Regulación del Correo Electrónico Laboral a la Ley 20.744 de Contrato de Trabajo.[318]
- Expediente Diputados 3694-D-09 del año 2009, Proyecto de Ley de modificación del artículo 26º de la Ley 25.326 sobre solicitud de datos personales y crediticios por una entidad financiera.[319]

Brasil

[311] En: http://venezuela.justia.com/federales/leyes/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones/gdoc/
[312] En: http://www.asambleanacional.gob.ve/uploads/leyes/2010-12-20/doc_576f11489badcdd456629bcbe165ba5baeddc40e.pdf
[313] En: http://www.asambleanacional.gob.ve/uploads/leyes/2013-09-17/doc_6a1b8e26741ee6208e22f40acf97ce8e161282f2.pdf
[314] En: http://www.tsj.gov.ve/legislacion/ledi.htm
[315] En: http://www.cnti.gob.ve/images/stories/documentos_pdf/ley_telecomunicaciones.pdf
[316] En: http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=1508-D-2013
[317] En: http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=8070-d-2012
[318] En: http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=0623-D-2007
[319] En: http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=3694-D-2009

Existe información de un anteproyecto de Ley de Protección de Datos Personales que data del año 2010, y que aún se encontraría en discusión.[320]

Chile

Encontramos el Boletín Nº 8143-03, que contiene el Proyecto de Ley de modificaciones a Ley N° 19.628, sobre Protección de la Vida Privada y Protección de Datos de Carácter Personal.[321] Éste se encuentra en tramitación desde enero de 2012, y continúa en el primer trámite constitucional en la Cámara de Diputados.

Con fecha 11 de junio de 2014 fueron ingresados dos proyectos, correspondientes a los Boletines Nº 9384-07 y 9388-03. El primero, busca que se reforme la Constitución para consagrar el derecho a la protección de los datos personales[322], en tanto el segundo busca modificar el artículo 13 de la ley N° 19.628, sobre protección de la vida privada, para establecer el "derecho al olvido" de los datos personales almacenados en motores de búsqueda y sitios web.[323]

Honduras

Existe un anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data de Honduras, que data del mes de Mayo del presente año (2014).[324]

Capítulo III
Jurisprudencia

En este capítulo se condensan fallos recientes emanados de las altas cortes de justicia de algunos países latinoamericanos, que resultan representativos a fin de entender la forma en que se abordan y resuelven casos relevantes en materia de privacidad.

Para estos efectos hemos dado preferencia a aquellos casos en que las tecnologías involucradas resultan ser un elemento gravitante en la controversia planteada ante el tribunal, dada la relevancia que ellas tienen en cuanto a la afectación del derecho en estudio.

Argentina

1.1.Derecho a la Intimidad

a) T. I. con Google[325]

[320] En: http://www.acessoainformacao.gov.br/menu-de-apoio/recursos-passo-a-passo/anteprojeto-lei-protecao-dados-pessoais.pdf

[321] Boletín Nº 8143-03. En: http://www.camara.cl/pley/pley_detalle.aspx?prmID=8541

[322] En: http://www.camara.cl/pley/pley_buscador.aspx?prmBUSCAR=9384

[323] En: http://www.camara.cl/pley/pley_detalle.aspx?prmID=9800&prmBL=9388-03

[324] En: http://cei.iaip.gob.hn/doc/Anteproyecto%20de%20Ley%20de%20Proteccion%20de%20Datos%20Personales%20y%20Accion%20de%20Habeas%20Data%20de%20Honduras%20%20Final%2021%2001%2014.pdf

Sentencia 5 de Agosto de 2013, Expediente Nº 732/2013 del Juzgado de Primera Instancia de Distrito en lo Civil y Comercial de Rosario.

En el presente caso la demandante solicita formalmente un requerimiento urgente denominado medida autosatisfactiva en contra de Google, a fin de que éste proceda a eliminar de sus búsquedas su nombre en sitios relacionados con videos de pornografía y/u oferta sexual y/o sitios eróticos, y específicamente respecto de las páginas que menciona la demandante y todo otro sitio de características similares o derivados que ofrezcan videos de pornografía. Todo ello debido a que, tal como menciona la demandante, estudiante con pareja estable, hace años atrás filmó un video casero con su pareja de entonces en donde se puede ver un acto de relación sexual oral, el que estuvo oculto por varios años, sin embargo fue subido a Internet sin su consentimiento, pudiendo ser visto en los links que ella señala.

El Juzgado resolvió, luego de atender a las características, requisitos y procedencia de la medida autosatisfactiva, que "(…) de la publicación mencionada se desprende una afectación al Derecho a la Intimidad comprensivo del derecho de controlar la información relativa a ciertos aspectos de la vida, entre ellos, los datos verídicos pero reservados al conocimiento del sujeto o de un grupo reducido de ellos, cuya divulgación o conocimiento por otros traería aparejado algún daño. En virtud de tal derecho, el sujeto detenta la potestad de oponerse a toda investigación, difusión, o alteración de datos de su vida privada por parte de terceros y a la divulgación de información que, por su naturaleza, esté destinada a ser preservada de la curiosidad pública.- Así, quedan comprendidos en el ámbito del derecho a la intimidad aspectos relacionados con la vida familiar, afectiva o íntima".[326] El Juzgado señala por su parte que estos Derechos se encuentran protegidos por distintas normas del Derecho Internacional de los Derechos Humanos como "la Declaración Americana de los Derechos del Hombre (art. V), Pacto de San José de Costa Rica (art. 11), Pacto Internacional de Derechos Civiles y Políticos (art. 17) entre otros",[327] los cuales, según el Juzgado, tendrían recepción en el Derecho Argentino positivo a través de su incorporación mediante el art. 75 inc. 22 de la Constitución Argentina.

El Juzgado finalmente hace lugar a la Medida Autosatisfactiva ordenando a la empresa Google "la inmediata eliminación de toda referencia a la actora en los sitios individualizados con precisión en la demanda, debiendo asimismo la empresa señalada abstenerse en el futuro de habilitar el uso de enlaces, blogs, foros, grupos, sitios de fans, que injurien, ofendan, agredan, vulneren, menoscaben o afecten la intimidad sexual de la actora, lo que deberá hacer saber a la casa matriz a sus efectos"[328].

1.2. Derecho de Intimidad vs. Libertad de Expresión

a) Rodríguez, María Belén con Google[329]

---

[325] En: http://www.elderechoinformatico.com/index.php?option=com_content&view=article&id=1608:fallo-argentina-derecho-a-la-intimidad-t-i-c-google-s--medida-autosatisfactiva-&catid=88:jurisprudencia&Itemid=87

[326] Ibídem.

[327] Ibídem.

[328] Ibídem.

[329] En: http://oiprodat.com/2014/05/21/audiencia-de-la-corte-suprema-por-el-caso-rodriguez-libertad-de-expresion-vs-derecho-a-la-intimidad/

Causa Expediente Nº 522-2013, actualmente en tramitación en la Corte Suprema de Justicia de Argentina.

El presente caso se refiere a la demanda por daños y perjuicios interpuesta por la modelo argentina María Belén Rodríguez en contra de Google Inc. y Yahoo! Argentina, por el daño material producto del uso indebido de una imagen propia de la modelo que la vincula con sitios de contenido sexual, y daño moral por violación del derecho a la intimidad.

El tribunal de primera instancia mediante sentencia hizo lugar a la demanda, condenando a ambas empresas a abonar a María Belén Rodríguez una cierta cantidad de dinero en proporción al daño que moral que habría sufrido. Además, condenó a las demandadas a eliminar de forma definitiva las vinculaciones del nombre, la imagen y las fotografías de la demandante con sitios y actividades de contenido sexual, erótico y/o pornográfico a través de sus buscadores.

Tanto la modelo María Belén Rodríguez como Google y Yahoo, presentaron recursos de apelación, de esta forma la causa llegó a segundo instancia siendo vista por la Cámara Nacional de Apelaciones en lo Civil, quien para resolver en un primer momento hace un estudio de los medios de prueba rendidos por las partes y los distintos entes a quienes se le solicito informe, extrae así varias conclusiones y señala que: "1) Los buscadores brindan su servicio a través de sistemas informáticos automáticos (sin intervención del ser humano) de actualización constante, que rastrean la información que se agrega a Internet y buscan coincidencias con la o las palabras ingresadas por el usuario; 2) El software utilizado para rastrear la información existente en Internet sigue criterios definidos por seres humanos; 3) Los buscadores no proveen el contenido de los sitios encontrados en la búsqueda, que pertenece a terceros, y, en la mayoría de los casos, no tienen relación contractual con los responsables de los localizadores uniformes de recursos que aparecen en sus listados de resultados (salvo en el caso de los "enlaces patrocinados"); 4) Tampoco modifican los contenidos incluidos en aquellos localizadores uniformes de recursos de terceros (fs. 653 vta., rta. 60); 5) Los listados de resultados son automáticos, pero –como ya lo puntualicé- obedecen a criterios definidos por los seres humanos; 6) Sin la intervención de los buscadores, los contenidos de los sitios de terceros no serían conocidos masivamente, pues para acceder a ellos habría que manejar la dirección web de cada uno, lo que tornaría muy difícil el acceso (fs. 647, rta. 30); 7) Para los buscadores de imágenes se utiliza un software editor de imagen que reduce el original".[330]

Luego de estas conclusiones, la Cámara Nacional hace un estudio de la doctrina y jurisprudencia comparada debido a la falta de regulación especifica respecto a la responsabilidad que podrían tener quienes explotan los motores de búsqueda por parte del legislador, señalando así "que la tendencia ampliamente dominante en el derecho comparado no pasa por imponer una responsabilidad objetiva a quienes explotan motores de búsqueda, sino que se exige, en general, que tengan un conocimiento efectivo de los datos lesivos originados en páginas de terceros para que pueda endilgárseles el deber de responder. Una cuestión distinta pasa por establecer desde cuándo puede considerarse que existe ese conocimiento efectivo, pues como se ha visto, en muchos casos se exige que medie

[330] Punto V, Sentencia Expediente Nº 99613-2006 pronunciada por la Cámara Nacional de Apelaciones en lo Civil con fecha 13 de Mayo de 2013.

una comunicación de una autoridad competente para que aquel se concrete".[331] Luego de hecho este análisis señala que, en Argentina, la doctrina y la jurisprudencia entienden en general que la responsabilidad de los motores de búsqueda debe enmarcarse en la órbita extracontractual. Sin embargo, se discute cuál es el factor de atribución aplicable y nos dice que hay quienes se inclinan por un factor objetivo, mientras que otros lo hacen por la responsabilidad subjetiva.

La Cámara Nacional de Apelaciones en lo Civil manifiesta así "que quienes sostienen que la responsabilidad de los buscadores de Internet tiene carácter objetivo –con lo cual, para que pueda condenárselos a reparar, bastaría con constatar que por su intermedio se puede acceder a las páginas que alojan los contenidos dañosos- se apoyan, obviamente, en el art. 1113, segundo párrafo, segundo supuesto, del Código Civil. Esto implica sostener dos cosas, a saber: a) que, más allá de la mención que esa norma efectúa al "riesgo o vicio de la cosa", también se encuentran comprendidas en su ámbito las actividades riesgosas, ya sea que se empleen o no cosas para llevarlas a cabo, y b) que, además, la actividad de quienes explotan motores de búsqueda en Internet puede calificarse de "riesgosa"".[332]

Señalado esto la Cámara Nacional sostiene que, en un primer análisis, podría pensarse que los motores de búsqueda en Internet reúnen esta calificación, no sólo por el gran volumen de contenidos de terceros que manejan, sino fundamentalmente porque de no ser por la existencia de aquellos motores, los contenidos lesivos que eventualmente alojen los millones de páginas web existentes no podrían prácticamente ser conocidos por nadie que no busque acceder directamente a la página en cuestión, de modo que para acceder a dichas páginas necesitarían conocer e ingresar la dirección exacta. De esta manera los motores de búsqueda facilitan la divulgación de los contenidos, potencia sus efectos nocivos, y desde este punto de vista bien podría ser considerada riesgosa.

Pese a lo señalado por la Cámara Nacional de Apelaciones en lo Civil, ésta cree que corresponde aplicar otra postura, y señala que la Constitución, como fuente principalísima en el derecho privado, impediría, a su juicio, que ciertos casos en los que están en juego derechos fundamentales puedan resolverse simplemente con la alusión de uno u otra norma del Código Civil. Para el Tribunal es necesario que se investigue previamente, si la aplicación de ese texto legal respeta efectivamente los principios constitucionales en juego, o si, por el contrario, es preciso aplicar otro estándar que efectivamente dé adecuada respuesta a aquella tensión de derechos fundamentales.

A modo ejemplar, la Cámara Nacional señala la tensión que ha existido entre la responsabilidad civil de la prensa y la libertad de expresión, y razona entorno a ella "[a] partir de la década de 1980, la Corte Suprema de Justicia de la Nación fue dejando de lado la aplicación directa de los textos del Código Civil para generar una serie de standards de cuño pretoriano, que se derivan directamente de un juicio de ponderación de los principios constitucionales en juego: la libertad de expresión por un lado, y los derechos personalísimos (a la intimidad, la imagen, el honor, etc.) de la víctima, por el otro. Nacen así, primero, la doctrina "Campillay" (CSJN, Fallos, 308:789; 319:2965; 326:4123, etc.), luego la de la "real

[331] Punto VII, Sentencia Expediente Nº 99613-2006 pronunciada por la Cámara Nacional de Apelaciones en lo Civil con fecha 13 de Mayo de 2013.
[332] Ibídem.

malicia" (CSJN, Fallos, 319:3428; 320:1227; 327:943; 331:1530; 327:943, etc.) y, finalmente, un standard particular para las opiniones (CSJN, Fallos, 321:2558; 331:1530, etc.), cuyo fundamento no se encuentra, obviamente, en el Código Civil (vid. sobre estas cuestiones: Tobías, José W., "Derechos personalísimos y libertad de información", LL, 17/12/2007, p. 1 y ss.; Ibarlucía, Emilio A., "Nuevas precisiones sobre las reglas de las doctrinas 'Campillay' y de la real malicia", LL, 30/8/2008, p. 3; Badeni, Gregorio, "Publicación de opiniones y la doctrina de la real malicia", LL, 8/9/2008, p. 6; Gulco, Hernán, "La ratificación de la doctrina del caso 'Patitó' (con algunas modificaciones muy encomiables)", LL, 8/6/2010, p. 3). Como es sabido, de este modo se consagra en cabeza de los medios de prensa una responsabilidad subjetiva que, en ocasiones –cuando la información inexacta versa acerca de un funcionario público o figura pública- se traduce en un factor de atribución agravado (la "real malicia"), cercano, cuanto menos, al dolo eventual (conocimiento de la falsedad, o notoria despreocupación acerca de la verdad o falsedad de lo informado). Y a veces, como ocurre en el caso de las opiniones relacionadas con cuestiones de interés público, se consagra una cuasi irresponsabilidad del medio de prensa, cuyo único límite estaría dado por el empleo de expresiones insultantes para transmitirlas (CSJN, 30/10/2012, "Quantín, Julio c/ Benedetti, Jorge Enrique y otros"; ídem, 26/3/2013, "Moslares, José Luis c/ Diario La Arena y otros").

Entiendo que la ratio de esta línea jurisprudencial, que finca en tutelar especialmente la libertad de expresión –en tanto uno de los pilares fundamentales de la democracia- e impedir que, por la vía oblicua de establecer reglas demasiado rigurosas en materia de responsabilidad, se llegue a consagrar una suerte de censura, es igualmente aplicable a la materia que ahora toca abordar al tribunal".[333]

Hecho mención de lo anterior, la Cámara Nacional de Apelaciones afirma que en el conflicto en cuestión se encuentra en juego los derechos fundamentales al honor, la imagen y la intimidad vs. el derecho a la libertad de expresión y el derecho colectivo al acceso a la información, señala al respecto que esté último derecho se encontraría comprendido en la misma libertad de expresión lo cual plasma de la siguiente forma "[s]í que la búsqueda, recepción y difusión de ideas e informaciones de toda índole por Internet se encuentra amparada por la garantía constitucional de libertad de expresión, y las aquí demandadas cumplen un rol importante al posibilitar el acceso de los usuarios de la red a los contenidos de los millones de sitios web existentes, solo cabe concluir que su actividad se encuentra amparada por aquella garantía constitucional".[334] Siguiendo con su razonamiento la Cámara Nacional señaló, que a la hora de evaluar la responsabilidad civil estos elementos era importantes, ya que a juicio del Tribunal "la aplicación de una responsabilidad objetiva a quienes explotan motores de búsqueda en Internet significaría en la práctica que todo perjuicio que sufra un individuo por algún contenido presente en la red derivaría en la responsabilidad del motor de búsqueda, lo cual o bien llevaría a estos últimos a una desmedida autorrestricción o bien, directamente, tornaría inviable su actividad, lo que perjudicaría seriamente la libre circulación de ideas e informaciones en la red, con lesión, en cualquier caso, de la libertad de expresión.

[333] Punto VIII, Sentencia Expediente Nº 99613-2006 pronunciada por la Cámara Nacional de Apelaciones en lo Civil con fecha 13 de Mayo de 2013.
[334] Ibídem.

Por no mencionar que una tan estricta regla de responsabilidad podría, incluso, alcanzar a otros intermediarios de Internet que facilitan el acceso a la red y, por consiguiente a los localizadores uniformes de recursos de terceros, como los proveedores de acceso a Internet".[335]

Es por estas razones que la Cámara señala que a su criterio la responsabilidad debiera encuadrarse sobre la base de aplicar un factor subjetivo de atribución, por lo que a su juicio la cuestión debería resolverse por aplicación de los arts. 512[336] y 1109[337] del Código Civil. A lo que se añade que, dado el grado de especialización que en la materia poseen estos empresarios profesionales, les sería también aplicable el estándar agravado que surge del art. 902[338] del Código Civil. Para arribar a esta conclusión la Cámara Nacional de Apelaciones en lo Civil toma en cuenta lo señalado por el derecho comparado, en particular por el autor español Ricardo Lorenzetti, manifestando que comparte sus conceptos, entendiendo así que "el deber de diligencia que –en los términos de los ya citados arts. 1109 y 902 del Código Civil- compete a las demandadas, les impone una pauta de conducta tendiente a impedir, en la medida de lo posible, la difusión de páginas y contenidos que ilícita y ostensiblemente dañen a terceros. Ahora bien, considera que de ninguna manera puede exigírseles, como regla general, un control ex ante, en ausencia de toda notificación o reclamo por parte de los eventuales afectados. Más allá del cuantiosísimo volumen de información que procesan diariamente los motores de búsqueda, se entiende que el fundamento principal para esta conclusión radica en el hecho de que, en infinidad de casos, no es posible saber de antemano si un determinado contenido resulta ser efectivamente dañoso o no. Lo que para ciertas personas, o incluso la mayoría de la población, es intolerable (como la vinculación de sus datos con páginas de contenido erótico, o la difusión de fotos íntimas), puede para otras ser aceptable y hasta deseable y consentido (para quien trabaje como modelo en revistas de esa clase, por ejemplo, o quien defienda al nudismo como estilo de vida y asuma una actitud militante al respecto), y no es posible pretender que los motores de búsqueda se conviertan en una suerte de censores que determinen por sí mismos, y en ausencia de todo pedido de los afectados, qué contenidos son admisibles y cuáles no lo son (lo cual, una vez más, nos acercaría a una peligrosa forma de censura)".[339] Luego en este mismo orden de ideas señala que "[e]n definitiva, pienso, con Gautier, que no puede pedirse a los operadores de Internet que conozcan todos los contenidos ilícitos alojados en las páginas, dado que la manipulación de los datos a la que proceden reviste una magnitud y una escala considerables. Pero como también lo señala ese autor, "no se trata

[335] Ibídem.

[336] Art. 512 del Código Civil Argentino señala: La culpa del deudor en el cumplimiento de la obligación consiste en la omisión de aquellas diligencias que exigiere la naturaleza de la obligación, y que correspondiesen a las circunstancias de las personas, del tiempo y del lugar.

[337] Art. 1.109 del Código Civil Argentino. Todo el que ejecuta un hecho, que por su culpa o negligencia ocasiona un daño a otro, está obligado a la reparación del perjuicio. Esta obligación es regida por las mismas disposiciones relativas a los delitos del derecho civil.
Cuando por efecto de la solidaridad derivada del hecho uno de los coautores hubiere indemnizado una parte mayor que la que le corresponde, podrá ejercer la acción de reintegro.

[338] Art. 902 del Código Civil Argentino que señala: Cuando mayor sea el deber de obrar con prudencia y pleno conocimiento de las cosas, mayor será la obligación que resulte de las consecuencias posibles de los hechos.

[339] Punto VIII, Sentencia Expediente Nº 99613-2006 pronunciada por la Cámara Nacional de Apelaciones en lo Civil con fecha 13 de Mayo de 2013.

tampoco de cerrar los ojos cuando, por las circunstancias o por las quejas de los terceros víctimas, han sido alertados" (Gautier, Pierre-Yves, "De l'éventuel 'rôle actif' des opérateurs Internet Dans la réalisation du dommage (qualifications de responsabilité civile)", Dalloz, 2011.2054)".

Esta cuestión se relaciona con la discusión acerca de si basta con un pedido genérico (de retiro de todos los contenidos, cualquiera sea el sitio en el que se encuentren, que resulten perjudiciales para el peticionante), o si debe señalarse cada sitio web en particular. La pericia practicada en autos deja bien en claro que los eventuales filtros que puedan emplearse trabajan sobre palabras; lo que puede "bloquearse", entonces, es la asociación de ciertos términos con otros. En ese sentido, se lee a fs. 636: "Es posible realizar una búsqueda en los dos buscadores mencionados, que evite que en los resultados de la búsqueda aparezca determinada palabra. Quién gobierna la información es el buscador, de cualquier otra manera sería imposible administrar las relaciones de búsqueda a partir de conectores lógicos y/o otros operadores brindados en el afán de permitir satisfacer las necesidades del usuario" (sic).

Un poco más adelante, el experto insiste en que "las demandadas están en condiciones técnicas de realizar este tipo de filtrados (fs. 636 vta.)".[340] En este sentido, la Cámara señala que cuando los buscadores se limitan a facilitar el acceso a contenidos que se encuentran en sitios web de terceras personas, estos no tendrían forma, de saber con anticipación que contenidos serían ilegales o agraviantes, por lo que por regla debiera el interesado poner en conocimiento de esa circunstancia para que se proceda, rápidamente, a filtrar, bloquear o extraer de sus listados de resultados aquellos contenidos. Por otra parte, señala que no cree que este deber del explotador del motor de búsqueda de bloquear contenidos ilícitos requiera una previa orden judicial, como lo sostendría parte de la doctrina. Ya que a su juicio de el ordenamiento jurídico de Argentina ese requisito no surgiría y no resultaría compatible con su deber de diligencia. Señaló si que a su criterio, bastaría "con que hayan tomado conocimiento –en principio, mediante comunicación del usuario- de la existencia del contenido nocivo para que se encuentren obligados a bloquearlo con prontitud, pues esa es la conducta esperable de un empresario diligente de la clase de las aquí demandadas".[341] Por lo que comunicado a el buscador este a su juicio debiera bloquear o filtrar el contenido con celeridad cuando fuere avisado de que aquel es ilícito o que daña derechos de terceros.

Por lo mencionado anteriormente, la Cámara Nacional determina que la demandante no acreditó haber cursado ningún tipo de notificación previa a las demandadas a fin de advertirles acerca de estos enlaces de páginas, ni que se hayan negado a bloquear los contenidos que le vulneraban su derechos fundamentales, razón por la que dejó sin efecto la condena respecto a este punto hecha en el tribunal de primera instancia en contra de Google y Yahoo!.

La Cámara Nacional, sin embargo considero que Google utilizó y reprodujo imágenes de la demandante –reduciéndolas, almacenándolas, y publicándolas en su buscador de imágenes- sin su consentimiento, lo cual, en ausencia de un régimen especial que establezca una excepción para estos casos, resultaba violatorio de lo prescrito por su ley de propiedad

[340] Ibídem.
[341] Ibídem.

intelectual. La Cámara encuentra pertinente destacar "sobre este punto, que el supuesto que ahora se examina es distinto de los que he considerado anteriormente, porque no se trata aquí de la difusión de ideas, informaciones, juicios de valor, etc., contenidos en páginas web –aspectos que, como ya lo señalé, se encuentran en general abarcados por la garantía de libertad de expresión- sino de imágenes de terceros, cuya difusión no puede considerarse igualmente protegida por aquella garantía. Nótese que incluso en lo que hace a la responsabilidad civil de la prensa –campo este donde, como también lo puntualicé, la libertad de expresión alcanza su más alto nivel de protección constitucional- se ha señalado que la doctrina de la real malicia es inaplicable en los casos en los que se denuncia la publicación indebida de la imagen de una persona (CCiv. Com. Azul, Sala II, 4/10/2011, "Dumerauf, Hugo c/ Diario El Popular", LL, 7/3/2012, p. 5, y nota aprobatoria de José Fernando Márquez: "La doctrina de la real malicia y la violación del derecho a la imagen")".[342] Razón por la cual descarta lo señalado por Google y confirma la condena a reparar en la sentencia de primera instancia pero sólo respecto a este punto.

Para el caso de Yahoo consideró que, al no existir pruebas de que hubiera realizado la conducta reprochada a Google, la sentencia se modificaba a su respecto, por lo que sólo se condenó a Google al pago de una indemnización por concepto de daño material por la violación del derecho a la imagen de la actora, en tanto editó y reprodujo fotografías de su persona sin autorización, reduciendo así el monto anterior dado por la sentencia de primera instancia dejándolo en $30.000.-(pesos Argentinos), y se condenó al pago por concepto de daño moral a la luz de las características del hecho generador, su repercusión espiritual en la víctima, y las demás circunstancias del caso a un monto también reducido respecto al que se le había señalado anteriormente, así pasó de ser $100.000.- a $20.000.-(pesos Argentinos).

Finalmente respecto de los agravios relativos, la condena a hacer que impuso la sentencia a las demandadas, consiste en eliminar toda vinculación del nombre, la imagen y las fotografías de la actora con sitios y actividades de contenido sexual, erótico y/o pornográfico a través de los buscadores "www.google.com.ar" y "www.yahoo.com.ar". Se señaló que sin bien Google y Yahoo desarrollaron una herramienta para recibir denuncias por violación de derechos, ella es de difícil acceso, y que para una persona común y corriente es prácticamente imposible ponerla en marcha. Por lo que a juicio de la Cámara Nacional de Apelaciones en lo Civil, esta falencia implicaría una clara negligencia de Google y Yahoo!, sin embargo, señaló que en este caso no era posible atribuirles consecuencias por responsabilidad debido a la falta de relación causal con los daños que la demandante reclamaba, toda vez que en ningún momento se habría alegado que la demandante habría pretendido notificar la existencia de contenidos puntuales por medio de aquella herramienta y había encontrado dificultades para hacerlo.

Tal como mencionamos en un principio, la causa sigue en tramitación encontrándose actualmente en la Corte Suprema de Justicia Argentina. Las implicancias que puedan resultar del presente juicio son diversas e importantes para los derechos fundamentales de las personas en Internet, por lo que resulta conveniente seguir de cerca la resolución a la que pueda llegar el Supremo Tribunal Argentino.

[342] Punto XII, Sentencia Expediente Nº 99613-2006 pronunciada por la Cámara Nacional de Apelaciones en lo Civil con fecha 13 de Mayo de 2013.

1.3. Habeas Data y Privacidad

a) ONG Asociación por los Derechos Civiles con Cámara Nacional Electoral[343]

A la fecha de emisión del presente informe, se encuentra en tramitación ante el Juzgado Contencioso Administrativo Federal Nº 4 de la Ciudad de Buenos Aires, una causa contra la Cámara Nacional Electoral, la entidad pública encargada de la administración de los procesos eleccionarios a nivel nacional.

Con fecha 22 de octubre de 2013, con motivo de las elecciones de agosto del mismo año, la Cámara Nacional Electoral lanzó un versión en línea del padrón electoral para que los ciudadanos argentinos pudieran consultar su lugar de votación y la mesa en la cual deberían hacerlo. El problema está en que, más allá de esta información, se encontraba también la fotografía de alguno de los electores que previamente a las elecciones habían renovados sus documentos de identidad.

En conformidad con lo señalado por ADC si bien finalizadas las primarias, el sitio de consulta fue suspendido, en septiembre se habilitó nuevamente con el padrón electoral definitivo para las elecciones del 27 de Octubre del año 2013. Ante esto ADC presentó una acción de habeas data colectiva solicitando la eliminación del Registro Nacional de Electores la totalidad de las imágenes fotográficas de los ciudadanos y ciudadanas contenidas y exhibidas en el sitio de consulta oficial www.padron.gob.ar solicitando a su vez como medida cautelar el retiro inmediato de las fotografías del sitio de Internet aludido.

ADC sostuvo en su presentación que la publicación, exhibición y disponibilidad sin autorización de estas fotos viola el derecho a la privacidad de estas personas. En este sentido ADC señalo "que la publicación de las fotografías en un sistema de acceso abierto pone en riesgo la autonomía de las personas en tanto les impide tener un control adecuado sobre un dato personalísimo y sensible como es la imagen de sus respectivos rostros. Además, señalaron que la publicación en Internet de las fotografías de más del 30 por ciento de los electores del padrón electoral implica, entre otras cuestiones, una cesión de hecho de esa información a terceros, quienes la podrían compilar e integrar a bases de datos con fines comerciales e ilícitos".[344]

ADC además afirmo que "el derecho a la privacidad es un derecho fundamental en una comunidad democrática garantizado en el artículo 19 de la Constitución Nacional, en diversos instrumentos internacionales de Derechos Humanos con jerarquía constitucional y en la Ley 25.326 de Protección de Datos Personales. Como lo ha sostenido la Relatoría Especial para la Libertad de Opinión e Información de la ONU, la protección de los datos personales es una forma especial de protección del derecho a la privacidad".[345]

Chile

1.4. Vida Privada e Inviolabilidad de las Comunicaciones

[343] En: http://www.adc.org.ar/1045_la-adc-pidio-a-la-justicia-que-se-retiren-las-fotos-de-los-votantes-del-padron-electoral-online/
[344] Ibídem.
[345] Ibídem.

a) Figueroa Silva Omar contra Prefecto de la Prefectura Cautín

Sentencia de la Corte de Apelaciones de Temuco, de fecha 28 de Junio de 2012 recaída en el Rol Nº 684-2012, confirmada por la Corte Suprema en sentencia de fecha 30 de Agosto de 2012, recaída en Rol Nº 5.322-2012.

El presente caso trata sobre un funcionario de Carabineros, quien recurre de protección en contra de la resolución dictada por el prefecto Coronel de su prefectura, mediante la cual se dispuso la eliminación de las filas de la institución del funcionario de Carabineros recurrente en la causa. El hecho que motivó la eliminación fue un comentario en su cuenta privada de Facebook en contra de su jefe en el cual señalaba textualmente "la noticia que me dieron en la mañana fue la gota que me *hechó* (sic) a perder el combinado, ahora si te odio jefe, descargaré toda mi venganza en ti, espérate hijo de …".

En consecuencia, el prefecto Coronel de su prefectura le aplicó la medida del Artículo 127 Nº 4 inciso 5º del Reglamento Nº 8 de Carabineros de Chile, consistente en la baja con efectos inmediatos, estimando que el recurrente infringió las faltas tipificadas en el artículo 22 Nº 1 letra d), Nº 5 letra e) del Reglamento Nº 11 sobre Disciplina de Carabineros de Chile, resolución que tiene el carácter de provisoría mientras este pendiente el sumario respectivo.

La Corte de Apelaciones de Temuco señala en su considerando 4º que "…,se debe dejar en claro que en los alegatos en estrados, el recurrente ante la pregunta de la Corte manifestó que lo expuesto en la red social Facebook se había obtenido por comentarios de terceras personas hacia los superiores y no por el hecho de que la Institución o el recurrido hubiera obtenido alguna clave para ingresar al Facebook del actor; en definitiva que se hubiera violado su privacidad. De la misma forma en el numeral doce de la acción de protección, el recurrido en audiencia de 26 de abril recibido por el Oficial mayor de Secretaría José Hernández Hernández señaló que había escrito lo consignado y que da cuenta el recurso. En consecuencia, respecto de este capítulo alegado por el recurrente debe ser desechado, puesto que como se ha señalado, el actor a través de su red social expone a un número determinado de personas sus comentarios sin que exista prohibición de que aquellos terceros que lo reciben puedan comentarlo con otras personas".[346]

Posteriormente la Corte de Apelaciones señala que no se ha incurrido en ninguna irregularidad ya que aún se encuentra pendiente la investigación, por que se encuentra en una etapa en curso, ciñéndose el recurrido al estatuto que lo rige. Señala a su vez que en cuanto a la arbitrariedad de la conducta del recurrido "no es caprichosa, se ha ajustado a la razón y tiene los fundamentos de hecho y de derecho"[347], señalado esto la Corte de Apelaciones de Temuco rechazó el recurso de protección interpuesto por el funcionario de Carabineros.

Por su parte la Corte Suprema de Chile confirmó la sentencia apelada, sin embargo, existieron dos votos disidentes, uno de los cuales nos parece relevante para el presente estudio, correspondiente al del Ministro Sergio Muñoz quien cita el Artículo 19 Nº 5 de la

[346] Considerando 4º Sentencia Corte de Apelaciones de Temuco fecha 28 de Junio de 2012 recaída en Rol 684-2012

[347] Considerando 6º Sentencia Corte de Apelaciones de Temuco fecha 28 de Junio de 2012 recaída en Rol 684-2012

Constitución Política de la República de Chile, que establece la inviolabilidad de las comunicaciones, y que se vincula estrechamente "con el inciso primero del artículo 1° de la Constitución Política de la República de Chile, que declara que las personas nacen libres e iguales en dignidad y derechos; dignidad que comprende el derecho a la intimidad, que en la esfera material está radicado en el hogar y de igual modo en las comunicaciones, ámbitos de privacidad de las personas y que reconoce sus orígenes en la Declaración de Derechos de Virginia de 12 de junio de 1776, que inspira la IV enmienda de la Constitución estadounidense de 17 de septiembre de 1787. Así se vincula dignidad, privacidad, intimidad, hogar y comunicaciones privadas, que es el contenido material que se resguarda con este derecho fundamental. Incluso en el derecho comparado se protege la disposición que se hace de las comunicaciones privadas, las que incluso en tales condiciones no puede tomar conocimiento de ellas la autoridad".

Posteriormente señala el Ministro Muñoz que "Esta misma normativa, sin embargo, nos proporciona las disposiciones que hacen procedente, sobre la base de intereses sociales superiores, establecer limitaciones a esta garantía. Es así como, según se ha dicho, sólo la ley puede indicar los casos y la forma en que las comunicaciones pueden interceptarse, abrirse o registrarse. El principio de legalidad impone que ninguna norma de rango inferior puede limitar tales garantías. Este antecedente resulta suficiente para acoger el recurso".

Luego señala: "3º.- Que cabe precisar que "Facebook" es un sitio web que permite a sus usuarios el poder comunicarse e intercambiar opiniones entre ellos, para lo cual el interesado debe solicitar autorización expresa a un tercero para incorporarlos en sus contactos y dicho tercero sólo se integrará a los mismos luego de consentir expresamente en ello, de lo que se desprende que sólo entre quienes así han consentido la información y sus comunicaciones es pública, no existiendo habilitación para que dicha información sea utilizada por otras personas. 4°.- Que entendiendo que la garantía constitucional puede ser afectada, previa habilitación legal, por la autoridad competente y siguiendo el procedimiento pertinente, todo sin alterar su esencia, es pertinente resolver si en la situación de autos que antes se ha descrito, se encuentra justificada legalmente alguna autorización a la Institución de Carabineros para tal proceder, circunstancia que corresponde descartar, de modo que ante la inexistencia de tales habilitaciones que le permitan desarrollar la acción llevada adelante, en orden a acceder a las publicaciones realizadas por el actor, ésta resulta ilegítima y en consecuencia la autoridad de Carabineros no podía acceder a ella ni menos utilizarla como fundamento de una sanción disciplinaria, más aún cuando no se señala en el informe, emitido en su oportunidad, de quien se obtuvo dicha información, constituyéndose en consecuencia en prueba ilícita y por ende no susceptible de ser utilizada".

Señalando finalmente el Ministro Muñoz que conforme a lo relatado el funcionario de Carabinero habría sido afectado en su garantía a mantener en reserva toda forma de comunicación privada por el proceder de Carabineros, por lo que el no habría rechazado el recurso sino que por el contrario lo habría acogido.

Inaplicabilidad por inconstitucionalidad del inciso segundo del artículo 5º de la Ley N' 20.285, sobre Acceso a la Información Pública[348]

Sentencia del Tribunal Constitucional de Chile, Rol Nº 2153-11-INA.

Con fecha 26 de diciembre de 2011, el Subsecretario del Interior, Rodrigo Ubilla Mackenney, solicita la declaración de inaplicabilidad por inconstitucionalidad del inciso segundo del artículo 5º de la Ley N' 20.285, sobre Acceso a la Información Pública, en la parte que dispone que es pública "toda otra información que obre en poder de los órganos de la Administración, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento".

La gestión pendiente invocada es un reclamo de ilegalidad deducido por la Subsecretaria de Interior en contra del Consejo para la Transparencia, seguido ante la Corte de Apelaciones de Santiago, mediante el cual se impugna la decisión del Consejo para la Transparencia, que ordenó entregar el contenido de correos electrónicos institucionales entre el Subsecretario y el Gobernador Provincial de Melipilla.

En el fallo del Tribunal Constitucional destaca el reconocimiento expreso que se hace a los derechos fundamentales que la Constitución garantiza a toda persona, incluidos los funcionarios públicos.

En primer lugar se analiza la naturaleza del correo electrónico, señalando que éste es "una forma de comunicación, pues a través de este medio se transmiten mensajes de un emisor a uno o varios receptores. Esta comunicación exige un soporte técnico, pues requiere la intervención de aparatos, de redes o infraestructuras, de operadores de éstas, de programas informáticos, de protocolos de transferencia en la internet. Hay de por medio un proceso de transmisión del mensaje o contenido. [...] el correo electrónico se transmite por un canal cerrado, en el sentido de que a él no pueden acceder terceros".[349]

Luego, al examinar el fondo del requerimiento que sostiene que "los correos son comunicaciones y documentos privados, en el lenguaje del artículo 19 Nº 5º de la Constitución, se concluye que por lo mismo, están protegidos por este derecho".[350] Señala el Tribunal que "el hecho de que la Constitución garantice la comunicación y los documentos que se emplean en ella, tiene enorme importancia. En efecto, mientras la comunicación propiamente tal tiene un inicio y un término, los documentos exceden ese margen de temporalidad, porque subsisten aún después de terminada la comunicación. Ello no implica que se encuentren desprotegidos por la Constitución, dado el tenor y el sentido del artículo 19 Nº 5º. La Constitución garantiza la inviolabilidad de la comunicación y de los documentos que la desarrollan.

Que, a continuación, hay que señalar que las comunicaciones que protege el artículo 19, Nº 5º, tienen que ser, en primer lugar, directas, en el sentido de que tengan un origen y un destino definidos, sean presenciales o a distancia. sean presenciales o a distancia. La norma protege la comunicación entre ausentes como entre personas que estén reunidas. Es decir,

[348] En: http://www.tribunalconstitucional.cl/wp/ver.php?id=2537
[349] Ibídem. Considerando Decimoquinto.
[350] Ibídem. Considerando Vigesimonoveno.

protege las conversaciones que se lleven a efecto en forma material o virtual [...]El carácter inviolable de la comunicación no tiene que ver tampoco con el contenido de la misma. Se protege el mensaje, sea que tenga que ver con aspectos públicos o privados, sea que se refieran a aspectos trascendentes o intrascendentes, afecten o no la vida privada.

Que, por otra parte, la Constitución establece que la inviolabilidad impide interceptar, abrir o registrar comunicaciones y documentos privados.

Que la Constitución latina establece que la inviolabilidad puede romperse "en los casos determinados por la ley" [...] la ley debe definir "los casos" en que la autorización es posible [...], toda resolución que levante total o parcialmente la inviolabilidad, requiere ser motivada [...] es necesario que la ley defina "las formas" en que la autorización se puede dar [...]los casos y las formas deben estar "determinados". Es decir, deben estar establecidos o fijados de modo preciso, no genéricamente".[351]

Luego concluye que "de este modo, el acceso a comunicaciones privadas solo puede permitirlo el legislador cuando sea indispensable para una finalidad de relevancia mayor; cuando no haya otra alternativa disponible, bajo premisas estrictas; con una mínima intervención y nunca de manera constante y continua, sino que de forma limitada en el tiempo y siempre de modo específico, señalándose situaciones, personas, hechos".[352]

En consecuencia, estima vulnerado el artículo 19 Nº 5º de la Constitución al considerar que los correos electrónicos se enmarcan perfectamente dentro de la expresión "comunicaciones y documentos privados" que utiliza el articulo 19 Nº 5º de la Constitución, y que la regla general es que, salvo prohibición expresa, las casillas institucionales pueden usarse para comunicaciones personales o privadas.

Añade "Que la segunda razón para considerar que se vulnera el artículo 19 Nº 5º de la Constitución es que no compartimos lo afirmado por el Consejo para la Transparencia, al sostener que la Ley Nº 20.285 es uno de los casos y formas determinados por la ley que permiten interceptar, abrir o registrar comunicaciones y documentos privados asociados a ellas.[...] nada apunta a que la intención del legislador con la Ley Nº 20.285 fuera levantar la inviolabilidad de las comunicaciones.[...] no tendría sentido que el legislador se hubiera preocupado de establecer estrictas condiciones para acceder a comunicaciones y documentos privados cuando investiga un delito o una conducta antimonopólica, que contempla incluso la autorización judicial, si cualquier ciudadano, sin invocar inter6s alguno, pudiera acceder a esos mismos antecedentes si estuvieran en manos de un funcionario, por la vía de la Ley Nº 20.285.[...] el legislador, de manera paciente, coherente y consistentemente, ha ido diseñando un sistema para levantar la inviolabilidad a que se refiere el articulo 19 Nº 5 de la Constitución".[353]

Agrega el Tribunal que carece de sentido "que una persona, sin invocar ningún interés o derecho, pudiera acceder a más documentación que el propio interesado en un

[351] Ibídem. Considerando Trigésimo cuarto a Trigésimo octavo.
[352] Ibídem. Considerando Cuadragésimo primero.
[353] Ibídem. Considerando Cuadragésimo sexto.

procedimiento. [...] Ahora, si los correos fueran actos administrativos, debieron emitirse bajo firma electrónica, simple o avanzada".[354]

Finalmente, el Tribunal arriba a la conclusión de que el inciso segundo del artículo 5º, impugnado, excede, en su aplicación a la gestión pendiente de autos, lo dispuesto en la Carta Fundamental, razón por la cual se le declara inaplicable.

1.5. Vida Privada y Protección de Datos

a) Control de Constitucionalidad respecto del Artículo 4º del proyecto de ley que sanciona el acoso sexual de menores, la pornografía infantil y la posesión de material pornográfico. (Boletín 5837). Ley Nº 20.526 (D. Oficial: 13/08/11)[355]

Sentencia del Tribunal Constitucional de Chile, Rol Nº 1894-2011

La presente sentencia trata sobre el control constitucional ejercido por el Tribunal Constitucional Chileno en conformidad al artículo 93 Nº 1 de la Constitución Política de la República de Chile, esto es "[e]jercer el control de constitucionalidad de las leyes que interpreten algún precepto de la Constitución, de las leyes orgánicas constitucionales y de las normas de un tratado que versen sobre materias propias de estas últimas, antes de su promulgación;"[356], respecto del Artículo 4º del entonces Proyecto de Ley Boletín 5837, que sanciona el acoso sexual de menores, la pornografía infantil y la posesión de material pornográfico, dicho artículo señalaba lo siguiente:

"Artículo 4º. Los establecimientos comerciales, cuya actividad principal sea ofrecer al público servicios de acceso a Internet, a través de computadores propios o administrados por ellos, deberán mantener un registro actualizado de los usuarios, durante un plazo no inferior a un año, en el que se consignará su nombre, cédula de identidad o número de pasaporte, o con los datos que se consignan en la licencia de conducir o en el pase escolar, fecha y hora inicial de cada acceso e individualización del equipo en el cual se utilizó el servicio.

El responsable del establecimiento deberá exigir a los usuarios la exhibición de alguno de los documentos antes indicados en el acto de su registro y siempre que fuesen a hacer uso de un computador para los efectos señalados en el inciso precedente.

Los establecimientos a que se refiere el presente artículo, no permitirán el uso de sus computadores a las personas que no proporcionen los datos previstos en el inciso primero o que lo hicieren en forma incompleta y a las personas que no portaren alguno de los documentos anteriormente señalados, o se negaren a exhibirlos.

Los registros a que se refiere el presente artículo tienen el carácter de reservado y su examen sólo podrá ordenarse por el juez de garantía, a petición del Ministerio Público, sin perjuicio del ejercicio de las atribuciones establecidas en el inciso séptimo. El incumplimiento del deber de reserva establecido en el presente inciso, por parte del responsable del establecimiento o alguno de sus dependientes, será sancionado con multa de 2 a 10 unidades tributarias mensuales y clausura temporal del establecimiento por un período no superior a

[354] Ibídem. Considerando Cuadragésimo noveno.
[355] En: http://www.tribunalconstitucional.cl/wp/descargar_expediente.php?id=32083
[356] Artículo 93 Nº 1 Constitución Política de la República de Chile

tres meses. La reincidencia en la comisión de dicha infracción, se castigará con multa de 4 a 20 unidades tributarias mensuales y la clausura definitiva.

El incumplimiento de las obligaciones establecidas en los incisos primero a tercero del presente artículo será sancionado con multa de 2 a 10 unidades tributarias mensuales. En el caso de una segunda condena por dicho incumplimiento, se podrá aplicar, adicionalmente, la clausura temporal del establecimiento por un período no superior a tres meses. De existir una tercera condena por tal incumplimiento, se aplicará el doble de la multa y la clausura definitiva.

De las infracciones contempladas en las disposiciones que preceden, conocerán los juzgados de policía local, conforme a las normas del procedimiento ordinario, contemplado en la Ley N° 18.287, que Establece Procedimiento ante los Juzgados de Policía Local.

Para efectos de la aplicación de lo dispuesto en el presente artículo, todos los establecimientos a que se refiere el inciso primero estarán sujetos a la vigilancia e inspección de Carabineros de Chile y de los inspectores municipales, resultando aplicable lo dispuesto en el artículo 2° de la ley N° 19.925, sobre Expendio y Consumo de Bebidas Alcohólicas.

Un reglamento, dictado por el Ministerio de Justicia, determinará las características especificas del Registro que deberán llevar los establecimientos a que se refiere el inciso primero, las medidas de seguridad que deberán adoptarse y toda otra norma que resulte necesaria para su implementación.

Lo dispuesto en el presente artículo entrará a regir noventa días después de la publicación en el Diario Oficial del reglamento a que se refiere el inciso precedente".[357]

Tal como se puede leer en el citado artículo, la ley establecía la obligación por parte de los establecimientos conocidos en chile como cibercafés a llevar un registro y solicitar a cada uno de sus usuarios que se identificara, señalando a su vez la hora y día en el que tuvo acceso a Internet. El Tribunal Constitucional en su análisis, específicamente en el punto II de Vida Privada o Intimidad, critica la disposición señalando que han hecho falta los resguardos establecidos por el artículo 19 en su número 4 de la Constitución Política de la República, el cual asegura a todas las personas el respeto y protección de la vida privada, que se encontraría en armonía con el Pacto Internacional de Derechos Civiles y Políticas en su artículo 17 números 1 y 2, los cuales prevén que "1.- Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada y que 2.- Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".. En este mismo sentido el Tribunal Constitucional en su considerando Vigesimoprimero afirma que "en efecto, sin pretender extenderse ahora a todos los contornos que presenta el referido derecho, ni querer agotar todas las situaciones que podrían lesionarlo, es lo cierto que éste comprende un ámbito de no intromisión en un aspecto reservado de la vida personal, que cierra el paso a las indagaciones de otros, sean agentes estatales o privados. Esto, a menos que medie el consentimiento espontáneo de la misma persona, a modo de mantener cierto gobierno sobre los datos que le conciernen, o la ley autorice una controlada intrusión para el caso -por ejemplo- de una específica investigación en curso, que haga suponer la comisión de un ilícito

[357] Artículo 4º de Proyecto de Ley Boletín 5837, reproducido en Considerando 5º de Sentencia 1894-2011 de Tribunal Constitucional.

concreto y donde no sea posible obtener la información faltante por otros medios en fuentes abiertas"..[358]

Luego, siguiendo con esta idea, el Tribunal Constitucional chileno señala en su considerando Vigesimosegundo "que, naturalmente, cualquiera entiende -aun sin ser jurisperito- que está a salvo en su legítima discreción para circular anónima e indistinguiblemente de los demás, sin chequeos o registros, a menos que a juicio de una autoridad competente, hubiera causas probables que inciten a pensar que se están perpetrando ilícitos concretos u verosímiles. De suerte que, esto sentado, dicha intimidad resultaría usurpada en caso de seguimientos o monitoreos sistemáticos, constantes y focalizados para husmear a qué lugares asiste alguien, por pertenecer a una categoría a priori sospechable de ciudadanos; por dónde -vías, caminos o canales- se desplaza en particular; cuál es el número de los sitios que visita y de las direcciones contactadas, precisamente; con quién, o con cuánta duración y frecuencia se producen las conexiones realizadas. Más todavía cuando, a partir de estos datos, hoy es factible ir de hurones e inferir historiales o perfiles individuales, que incluyen hábitos y patrones de conducta humana, hasta poder revelar las preferencias políticas, opciones comerciales e inclinaciones sociales de las personas".

De esta forma el Tribunal Constitucional determina la importancia del derecho a la intimidad, señalando por su parte que si bien no es un derecho absoluto, éste no puede ser usurpado sólo por pertenecer a un determinado grupo de individuos, y menos por la importancia que tienen hoy en día ciertos datos que son parte de la vida privada de las personas. Posteriormente, el Tribunal Constitucional repara la extensión que tiene el derecho a la intimidad y lo vincula al caso en concreto diciendo así que "la intimidad no sólo puede darse en los lugares más recónditos, sino que también se extiende, en algunas circunstancias, a determinados espacios públicos donde se ejecutan específicos actos con la inequívoca voluntad de sustraerlos a la observación ajena (Eduardo Novoa Monreal, Derecho a la vida privada y libertad de información, Veintiuno Editores, 1981, páginas 51 y 202-204. Asimismo, Enrique Barros Bourie, Honra, Privacidad e Información: Un Crucial Conflicto de Bienes Jurídicos, Revista de Derecho, 1998, Universidad Católica del Norte, página 47).

Así, no obstante que los cibercafés constituyen locales accesibles en general al público, en cuanto no se puede inadmitir a ningún cliente o usuario, a diferencia de otros lugares de afluencia masiva, suelen organizarse internamente en cámaras o cabinas individuales y reservadas, justamente en consideración a los servicios de interconexión que facilitan y a modo de cautelar que dentro de ellos tenga cobijo un cierto ámbito de privacidad. Igualmente Internet, puesto que si bien esta red informática mundial configura un espacio abierto a todos, los sitios visitados en un recorrido, así como los correos electrónicos y la mensajería instantánea allí producidos, revisten carácter confidencial;"[359]

El Tribunal Constitucional concluyó que, ni aún con los fines superiores que procuraba alcanzar el proyecto, esto es la prevención y el combate delitos de acoso sexual de menores, la pornografía infantil y la posesión de material pornográfico, eran suficientes para justificar

[359] Sentencia Tribunal Constitucional de Chile Rol 1894-2011

la implementación de un medio como el "registro" al resultar su implementación lesiva para el ejercicio los derechos constitucionales.

Colombia

1.6. Habeas Data y Lista Negras

a) Julia con Empresa de Masajes

Sentencia Expediente Nº T-634 de 2013, pronunciada por la Corte Constitucional de Colombia el 13 de Septiembre de 2013. En la causa, la peticionaria, quien trabajaba como masajista en la empresa demandada, suscribió una autorización para que ésta publicara su imagen en la página web, medios de publicidad y en artículos impresos, con fines publicitarios. Las fotografías, en conformidad a lo señalado por la actora, mostrarían situaciones comprometedoras. Las imágenes fueron publicadas en la página que la empresa demandada tenía en la red social Facebook, lo que significó perjuicios graves para la vida íntima y social de la demandante, y también le habría ocasionado controversias e inconvenientes familiares y personales, incluyendo comentarios ofensivos y denigrantes contra su persona. La empresa demandada se negó a retirar las imágenes cuando le fue solicitado por la demandante, aludiendo que ya habían sido publicadas vía web y otros medios de publicidad (volantes), y que la campaña publicitaria le había significado costos.

Cabe mencionar que la Corte Constitucional hace un examen de las imágenes de la demandante, junto a otras de las publicadas por la empresa, ya que considera que el contexto y conjunto de las fotos son un elemento pertinente para el análisis de la posible vulneración de los derechos fundamentales de doña Julia. Por medio de este examen el Tribunal señala que las fotos hacen parte de una secuencia en la que aparecen otras masajistas y otras imágenes. Así, una secuencia inicial de fotos muestra imágenes de la peticionaria primero con su mano sobre la espalda de un hombre tendido en el piso, luego con su rodilla sobre la espalda del mismo y luego con uno de sus pies sobre la parte superior de su espalda, la imagen que le sigue a éstas fotografías muestra a otra de las masajistas en una tina con un hombre quien aparece bebiendo de una copa. Esta última fotografía permite inferir que la empresa también ofrece interacciones más íntimas entre los clientes y las masajistas diferentes a las de masajista-cliente en las habitaciones para el servicio de masaje. De manera similar, una segunda secuencia de fotos incluye una imagen que muestra a mujer rodeando con su mano el mentón de un hombre y dándole un beso en la parte posterior de su cuello en la misma habitación en la que aparece la accionante en otra fotografía.

Luego señala que respecto a las imágenes de doña Julia en particular, en su mayoría, muestran a la actora usando una bata corta y descalza en una habitación con un hombre desnudo con su cadera parcialmente cubierta por una toalla. En otra de las fotos, la accionante aparece rodeando con sus brazos y una de sus piernas a un hombre que se encuentra sentado sobre el piso. De modo que luego de examinar las fotografías en su conjunto, la Corte señala que, tanto las de la accionante como las demás que aparecen en la página de Facebook de la empresa demandada, permiten razonablemente pensar que la publicidad en la red social Facebook es por lo menos ambigua ya que no muestra de manera

exclusiva servicios de masajes, por lo que en definitiva sería dudoso que los servicios ofrecidos fueran exclusivamente los indicados masajes.

A continuación, la Corte hace un análisis de los derechos fundamentales afectados y a su vez determina la importancia de la autorización que la peticionaria había dado para el uso de las fotografías. En este punto resulta importante señalar que la jurisprudencia de la Corte Constitucional de Colombia ha considerado que el derecho fundamental a la propia imagen es vulnerado cuando una imagen es publicada sin autorización de su titular, de modo que en caso contrario, habiendo autorización no podría haber vulneración de garantías fundamentales. Sin embargo, la Corte señaló que la autorización para el uso de la propia imagen involucra además de la aceptación de los lugares donde se publicará, aspectos teleológicos, relacionados con el consentimiento sobre la finalidad del uso de la imagen. La Corte sostuvo además que, aún cuando la autorización constituye un requisito para el uso legítimo de la imagen por terceros, lógicamente y bajo el criterio interpretativo de conformidad con la Constitución, la satisfacción de este requisito no puede entenderse como que tiene la potencialidad y el carácter general y suficiente para excluir e impedir de manera absoluta la posibilidad de invocar y obtener el amparo constitucional.

En este mismo sentido la Corte concluye que la autorización no puede interpretarse como una renuncia indefinida, total e ilimitada a disponer de la propia imagen o al desconocimiento de otros derechos fundamentales como la honra, el buen nombre o la intimidad. Así, a modo ejemplar, señaló que el uso de la propia imagen no podía ser utilizada para denigrar a una persona, para someterla al escarnio público o, como ocurría en este caso, a generar ambigüedades acerca del trabajo para el que fue contratada[360].

Posterior a este análisis, la Corte se refirió a los demás derechos fundamentales lesionados, mencionando que en el caso del derecho a la intimidad el actuar de la demandada vulneró este derecho, ya que, "aunque las imágenes no daban a conocer aspectos de su vida íntima, su publicación y el acceso que ésta brinda a multiplicidad de públicos en la red social Facebook afectan su intimidad personal y social. En este sentido, la publicación de sus imágenes en el contexto y condiciones reseñadas, incluyendo el libre acceso de terceros a su imagen en la red, afecta las relaciones de la accionante con su familia y su núcleo social porque las imágenes publicadas no corresponden a lo que ella, como lo señaló en su acción de tutela, representa "como ser humano", a lo cual debe agregarse que, como también lo manifestó la accionante, el contenido de las imágenes "le ha causado un gran perjuicio" a su "vida social y familiar, acarreándome innumerables comentarios ofensivos y denigrantes".

Como lo señaló la sala en las consideraciones, el derecho a la intimidad garantiza una esfera de privacidad libre de intervenciones arbitrarias de terceros, al tiempo que es un derecho que sólo puede ser limitado por razones justificadas constitucionalmente. En el caso bajo estudio, la ausencia de razones constitucionales que justifiquen la negativa de la demandada para retirar las imágenes de la actora y por tanto facilitar y permitir el libre acceso de terceros a las mismas, evidencia la vulneración a su esfera íntima, que se tradujo en una perturbación grave de su entorno personal, familiar y social".[361]

[360] Punto 9.3 Sentencia Expediente Nº T-634 de 2013 pronunciada por la Corte Constitucional de Colombia.
[361] Punto 9.6 Sentencia Expediente Nº T-634 de 2013 pronunciada por la Corte Constitucional de Colombia.

Es así como la Corte Constitucional decide conceder la tutela a los derechos fundamentales, ordenado que la empresa retirara de la red social Facebook, y de cualquier otro medio de publicidad, las imágenes de doña Julia, y que se abstuviera de publicarlas y divulgarlas en el futuro.

Costa Rica

1.7. Derecho a Intimidad y Cámara de Vigilancia

a) Anónimo con Ministerio de la Presidencia

Sentencia Expediente Nº 3575 del año 2014, pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica con fecha 14 de Marzo de 2014.

La causa se refiere a un recurso de amparo interpuesto en contra del Ministerio de la Presidencia de Costa Rica, en el que la recurrente relató haberse percatado de que, en un poste contiguo a la Casa Presidencial y a su propiedad, se había instalado un poste metálico con unas varillas pegadas a la tapia del patio de su casa. Posteriormente su hija habría procedido a conversar con los funcionarios con el fin de solicitarles removieran las varillas de su tapia. Su hija señaló que, tal como se le indicó, en el poste principal habría sido colocada una varilla para instalar una cámara de seguridad por orden de la Casa Presidencial. Luego de corroborada la información, habría llamado al Jefe de Seguridad de Casa Presidencial, solicitando así que se retiraran las varillas y la cámara de seguridad de su propiedad. Si bien las varillas fueron removidas, la cámara se habría instalado en el poste metálico, siendo que ella rota sobre sí misma y las grabaciones en video alcanzan su propiedad, situación por la que consideró violentados sus derechos al honor, a la intimidad y a la imagen.

La Sala Constitucional, previo a entrar al fondo del asunto, hace referencia al derecho a la intimidad y señala que "este Tribunal en la sentencia 2013003835 de las 09:05 horas del 22 de marzo de 2013 señaló:

"El recurrente alega que el accionado ha colocado una cámara de seguridad con la cual enfoca a su vivienda, por lo que siente que se está vulnerando su derecho a la intimidad. La Sala, en la sentencia número 6776-94 de las catorce horas cincuenta y siete minutos del 22 de noviembre de 1994, indicó lo siguiente:

"El derecho a la intimidad tiene un contenido positivo que se manifiesta de múltiples formas, como por ejemplo: el derecho a la imagen, al domicilio y a la correspondencia. Para la Sala el derecho a la vida privada se puede definir como la esfera en la cual nadie puede inmiscuirse. La libertad de la vida privada es el reconocimiento de una zona de actividad que es propia de cada uno y el derecho a la intimidad limita la intervención de otras personas o de los poderes públicos en la vida privada de la persona; esta limitación puede manifestarse tanto en la observación y captación de la imagen y documentos en general, como en las escuchas o

grabaciones de las conversaciones privadas y en la difusión o divulgación posterior de lo captado u obtenido sin el consentimiento de la persona afectada".[362]

Luego de señalado esto entra al fondo del asunto y señala que efectivamente existió una violación al derecho a la intimidad de la peticionaria, pues durante el 26 de diciembre de 2013, al estar girando la cámara de seguridad en 360º y enfocando su propiedad, esta tuvo que soportar una injerencia en su ámbito privado que devino en una lesión a ese derecho fundamental. La Corte así falla a favor de la peticionaria, pero sólo para efectos indemnizatorios, toda vez que la actuación lesiva de los derechos fundamentales de la accionante ya había sido solucionada.

1.8. Derecho a Intimidad e Información en Internet

b) A.P.F. con Poder Judicial de Costa Rica

Sentencia Expediente Nº 3712 del año 2012, pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica con fecha 16 de Marzo de 2012. En la causa, la recurrente presentó un recurso de amparo debido a que, al ingresar su nombre en el buscador de Google, aparecía el enlace directo a la página de Internet del Sistema Costarricense de Información Jurídica, en el que se encuentra una sentencia de la Sala Segunda de la Corte Suprema de Justicia, relacionada con una demanda de impugnación de paternidad interpuesta por su padre, en la que se ventilan cuestiones muy íntimas de su familia. En este sentido la demandante señala que se vulnera su derecho a la intimidad ya que la sentencia mantiene datos que permiten su identificación y la de sus progenitores, ventilando un conflicto familiar del que cualquier persona podría tener conocimiento al acceder a Google.

La Sala Constitucional señaló que, en anteriores oportunidades, se ha establecido un criterio jurisprudencial que ha decantado por la reserva de los datos personales en las sentencias en materia penal, precisamente, atendiendo a la naturaleza sensible de esa rama del derecho, excluyendo otras disciplinas jurídicas. Así, por ejemplo, señala que en Sentencia Nº 6431, de 20 de Mayo de 2011, se señaló que "debe la información que corresponde a las partes en el proceso penal cuyas causas penales se encuentren ya sea con una solicitud de sobreseimiento o con una sentencia de sobreseimiento en poder del Ministerio Público o en el Sistema Integral de Gestión de Despachos Judiciales del Poder Judicial, mantenerse en reserva y compartirse únicamente en los casos y para los fines claramente definidos, entre los que está mantener la certeza del estado actualizado de los procesos penales que se ventilan a su cargo, para lo cual deberán implementar las medidas tecnológicas que permitan garantizar el secreto de la información. Asimismo deberá el Poder Judicial implementar medidas tecnológicas de prevención que permitan garantizar frente a terceros usuarios, el derecho a la intimidad de la información que permita identificar a las distintas partes en los distintos

[362] Punto III Sentencia Expediente Nº 3575 del año 2014 pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica.

procesos de las ramas jurídicas cuya información está a disposición de terceros, incluso por Internet o a través de la red"[363].

Sin embargo, la Sala Constitucional, analizando los antecedentes y las particularidades del caso concreto reconsidera esa tesis y estima que la recurrente está en lo correcto debido a que, la materia de familia, pertenece a la esfera íntima de cada individuo, de modo que todos aquellos conflictos que se puedan dar en el seno no tienen por qué ser del conocimiento inmediato de terceros ajenos a éste. Es así que la Corte señala que, si bien las sentencias son documentos públicos y por ello su acceso sería irrestricto, "resulta razonable la protección de los datos contenidos en ellas que permitan identificar a las partes involucradas y vincularlas con el conflicto específico. Es claro que la difusión de las sentencias, en este caso, vía Internet, constituye un instrumento necesario para garantizar la transparencia de la Administración de Justicia amén de que es un medio idóneo para que la población tenga conocimiento de los criterios jurídicos que resultan aplicables en las distintas ramas del derecho. No obstante, para lograr esos propósitos, en materia de familia podría resultar innecesaria la publicación de todos aquellos datos que permitan identificar a las partes involucradas en el conflicto, sobre todo, considerando que en muchos de los asuntos que se ventilan en esa jurisdicción, hay menores de edad de por medio".[364]

En consideración a lo señalado anteriormente la Sala Constitucional de la Corte Suprema estimó que se produjo la violación del derecho a la intimidad de la recurrente, por lo que se dispuso la eliminación de los datos personales, condenando a su vez al Estado al pago de las costas, daños y perjuicios causados.

1.9. Derecho de Intimidad y Datos Personales

a) Y.A.S. con Empresa Cero Riesgo Información Crediticia Digitalizada S.A. y Protectora de Crédito Comercial S.A.

Sentencia Expediente Nº 3998 del año 2012, pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica con fecha 23 de Marzo de 2012. En la causa, el recurrente interpone recurso de amparo en contra de las empresas Cero Riesgo Información Crediticia Digitalizada Sociedad Anónima y Protectora de Crédito Comercial Sociedad Anónima fundado en que, pese a la aprobación de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, ambas empresas inobservaban la legislación, toda vez que mantenían en sus bases de datos el historial de toda su información personal, la cual incluso se encontraba desactualizada o era falsa, publicitándola a terceros sin su consentimiento o autorización, lo que podría dar lugar a que se afectara eventualmente su seguridad, privacidad e intimidad.

La Sala Constitucional, previo a entrar al caso concreto, hace mención a la ampliación del ámbito protector del derecho a la intimidad, para ello señala que se reconoce el "derecho fundamental de toda persona física o jurídica a conocer lo que conste sobre ella, sus bienes

[363] Punto VI de Sentencia Expediente Nº 6431 del año 2011 pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica con fecha 20 de Mayo de 2011.

[364] Punto IV Sentencia Expediente Nº 3712 del año 2012 pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica.

o derechos en cualquier registro o archivo, de toda naturaleza, incluso mecánica, electrónica o informatizada, sea pública o privada; así como la finalidad a que esa información se destine y a que sea empleada únicamente para dicho fin, el cual dependerá de la naturaleza del registro en cuestión. Da derecho también a que la información sea rectificada, actualizada, complementada o suprimida, cuando la misma sea incorrecta o inexacta, o esté siendo empleada para fin distinto del que legítimamente puede cumplir. Es la llamada protección a la autodeterminación informativa de las personas, la cual rebasa su simple ámbito de intimidad. Se concede al ciudadano el derecho a estar informado del procesamiento de los datos y de los fines que con él se pretende alcanzar, junto con el derecho de acceso, corrección o eliminación en caso el que se le cause un perjuicio ilegítimo".[365]

Jurisprudencia anterior, de la misma Sala Constitucional, señala que los datos y documentos tales como la dirección del domicilio, el número del teléfono celular y la fotografía, forman parte de las datos privados que han sido establecidos como sensibles y, como tales no son de dominio público.

La Corte Suprema hizo alusión a su vez a los señalado por la Ley Nº 8.968, de Protección de la Persona frente al tratamiento de sus datos personales, señalando así que luego de la aprobación de ésta se delimitó de forma clara cuáles son los datos personales que pueden ser susceptibles de publicación y/o divulgación por terceras personas o empresas que se dediquen a esta actividad, y cuáles no. De esta forma el Tribunal destaca lo señalado en el artículo 9 Nº 3 de esta ley, en donde se indica de manera expresa que la dirección exacta de la residencia de una persona, su fotografía, así como los números de teléfono privados y otros de igual naturaleza, no pueden ser considerados como datos personales de acceso irrestricto, es decir, que su divulgación por terceros no es permitida sin el consentimiento expreso y libre del titular de esa información.

En el análisis del caso en concreto ,la Sala Constitucional señaló que se acreditó que la empresa Cero Riesgo Información Crediticia Digitalizada Sociedad Anónima tenía información considerada sensible. Por su parte, la Corte Suprema señala que en ambos estudios consta que el recurrente no tiene demandas, remates, transacciones comerciales, gravámenes, propiedades, vehículos ni morosidad patronal con la Caja Costarricense de Seguro Social, por lo que la información en estas casillas aparece en blanco. La Corte Suprema en este punto aclara que "si bien en las bases de datos de las empresas recurridas, existen datos suyos referentes a su edad, fecha de nacimiento, estado civil, nombres de sus padres, profesión, propiedades, participación en sociedades, deudas con la Caja Costarricense de Seguro Social y procesos judiciales civiles, esa información de ninguna manera puede considerarse de carácter meramente privado, tal y como pretende el amparado, toda vez que esta se encuentra en fuentes públicas como el Registro Civil y el Registro Público, o se refiere al comportamiento crediticio del tutelado, el cual puede ser

[365] Punto V Sentencia Expediente Nº 3998 del año 2012 pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica.

conocido por razones de seguridad del sistema financiero nacional, tal y como lo ha sostenido en reiterada jurisprudencia esta Sala"[366]

Dicho esto, la Corte señala que la empresa poseía en sus registros la fotografía, dirección del domicilio, y números celulares propios, entre otros datos sensibles pertenecientes al peticionario los cuales consideraba como privados, y que por ese motivo no podía ser dada a conocer en las bases de datos de las empresas que se dedican a esta actividad, de esta forma la Sala Constitucional concede el recurso de amparo reconociendo la lesión al derecho a la intimidad del recurrente, así como a su derecho a la autodeterminación informativa por lo que ordenó la eliminación de dicha información.

1.10. Derecho a la Intimidad y Computadores de Funcionarios Públicos

a) U.D.R. con Municipalidad de Atenas

Sentencia Expediente Nº 7573 del año 2012, pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica de fecha 8 de Junio de 2012. En la causa, se interpone recurso de amparo en contra de la Municipalidad de Atenas, fundado en que el recurrente, funcionario de la recurrida con el cargo de contador, fuera separado de su cargo por un plazo de 2 meses, por acuerdo del Consejo Municipal tomado por sesión extraordinaria de 19 de Enero de 2012. El recurrente señaló en su oportunidad que esta decisión no tuvo un sustento fáctico ni jurídico. Luego, fue comunicado de la decisión con fecha 20 de Enero de 2012, y además en forma verbal se le indicó que se le prohibía ingresar a la oficina en donde trabajaba, negándosele así el acceso a su computadora y demás objetos personales que utilizaba para desarrollar sus labores. Con posterioridad, el día 8 de Marzo de 2012 se le notificó la apertura de un procedimiento administrativo en su contra, el cual se tramitaba bajo un expediente, con el fin de determinar su eventual responsabilidad civil y disciplinaria por una supuesta inobservancia a su deber de cumplir con la prohibición de ejercer libremente su profesión, ya que se consideró que los documentos privados que él almacenaba en su computador correspondían a trabajos de contabilidad privados, ajenos al trabajo municipal.

El recurrente señaló que se le solicitó a un notario que confeccionara un acta notarial, a efecto de consignar la existencia de documentos privados en la computadora que solía utilizar, lo cual fue llevado a cabo en la presencia de los recurridos. Por su parte, el recurrente aclaró que los trabajos de contabilidad que se encontraron fueron elaborados por otro contador para varias empresas, quien se los facilitó para ser utilizados como referencia en una exposición sobre prácticas contables que él iba a dar en un curso. Alega así que la información personal extraída de su computadora fue obtenida sin la orden de un juez, sin su consentimiento y conocimiento. De esta forma, a través de la prueba fundamental del procedimiento seguido en su contra, a saber, el acta notarial, se tuvo acceso a información de terceros cubierta por el secreto tributario, lo cual lesiona los derechos de esos terceros, además de estimar vulnerados sus derechos a la intimidad y al secreto de las comunicaciones.

[366] Punto VII Sentencia Expediente Nº 3998 del año 2012 pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica.

La Sala Constitucional, previo a entrar al caso concreto, analiza el derecho a la intimidad y señala que "[e]l artículo 24 de la Constitución Política y el artículo 11 de la Convención Americana sobre Derechos Humanas consagran el derecho a la intimidad que, entre otras cosas, pretende garantizarle a todo individuo un sector personal, una esfera privada de su vida inaccesible al público salvo expresa voluntad del interesado. En este sentido, la Sala en sentencia número 6776-94 de las 14:57 horas del 22 de noviembre de 1994, indicó lo siguiente: "El derecho a la intimidad tiene un contenido positivo que se manifiesta de múltiples formas, como por ejemplo: el derecho a la imagen, al domicilio y a la correspondencia. Para la Sala el derecho a la vida privada se puede definir como la esfera en la cual nadie puede inmiscuirse. La libertad de la vida privada es el reconocimiento de una zona de actividad que es propia de cada uno y el derecho a la intimidad limita la intervención de otras personas o de los poderes públicos en la vida privada de la persona; esta limitación puede manifestarse tanto en la observación y captación de la imagen y documentos en general, como en las escuchas o grabaciones de las conversaciones privadas y en la difusión o divulgación posterior de lo captado u obtenido sin el consentimiento de la persona afectada."

Entonces, es claro que se trata de un fuero de protección a la vida privada de los ciudadanos pues la intimidad está formada por aquellos fenómenos, comportamientos, datos y situaciones de una persona que normalmente están sustraídos al conocimiento de extraños y cuyo conocimiento por éstos puede turbarla moralmente, a menos que esa misma persona asienta a ese conocimiento. Si bien, no puede menos que reputarse que lo que suceda dentro del hogar del ciudadano es vida privada, también puede ser que lo que suceda en oficinas, hogares de amigos y otros recintos privados, esté en ese ámbito (ver sentencia número 2006-005607 de las 15:22 horas del 26 de abril de 2006)"[367]

De esta forma, la Sala Constitucional reconoce un derecho a la vida privada más extenso, que incluso se puede dar más allá del seno del hogar. Luego de señalado esto la Corte Suprema se preocupa de analizar las potestades legitimas de control y fiscalización del empleador y para ello hace mención a lo señalado por la Organización Internacional del Trabajo (OIT) y su Repertorio de Recomendaciones prácticas respecto a la protección de los Datos Personales de los Trabajadores, de esta forma señala que "los empleadores puedan ejercer cierto tipo de actos de control o vigilancia, sin aviso previo, cuando existan sospechas que los empleados están incurriendo en infracciones graves que le puedan traer un perjuicio a la empresa. En ese sentido, la OIT afirma que: 1) Cuando los trabajadores sean objeto de medidas de vigilancia, éstos deberían ser informados de antemano de las razones que las motivan, de las horas en que se aplican, de los métodos y técnicas utilizados y de los datos que serán acopiados, y el empleador deberá reducir al mínimo su injerencia en la vida privada de aquéllos. 2) El secreto en materia de vigilancia sólo debería permitirse cuando a) se realice de conformidad con la legislación nacional; o b) existan sospechas suficientes de actividad delictiva u otras infracciones graves. 3) La vigilancia continua debería permitirse solamente si lo requieren la salud, la seguridad y la protección de los bienes (véase la página web: http://www.ilo.org). Por otra parte, la doctrina ha dicho que para que el patrono pueda controlar legítimamente a sus trabajadores, debe existir una necesaria concurrencia de un

[367] Punto III Sentencia Expediente Nº 7573 del año 2012 pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica

interés empresarial constitucionalmente relevante, lo cual se conoce como el principio de finalidad legítima. De acuerdo con los especialistas, los datos de carácter personal únicamente pueden recogerse para un motivo determinado, explícito y legítimo («) Debe haber un fin determinado, explícito y legítimo que justifique la restricción que experimentan los trabajadores en sus derechos fundamentales («) En cualquier caso, el fin ha de ser lícito, y no contrario a normas imperativas («) No basta cualquier finalidad, tiene que haber una motivación fuerte, que esté como mínimo- en consonancia o a la altura del sacrificio que se reclama a la otra parte por el juego de equilibrios que debe existir entre el interés de la empresa y los derechos fundamentales del trabajador (véase, Goñi Sein, José Luis. La videovigilancia empresarial y la protección de datos personales. Editorial Thomson Civitas, España, 2007)"[368]

Hecho este análisis, la Sala Constitucional hace el ejercicio de aplicar esta doctrina al caso concreto y señala así que "se puede afirmar que el patrono tiene la potestad, dentro de sus poderes de dirección, de fiscalizar los documentos y archivos que sus empleados tengan almacenados en las herramientas de trabajo que se les pone a su disposición, siempre y cuando se tenga una sospecha lo suficientemente fundada como para establecer que el trabajador (o en este caso, el funcionario público) está ejerciendo una actividad delictiva u otra infracción grave que perjudique de manera directa el funcionamiento de la empresa (o en este caso, de la contabilidad de la Administración Pública). Este sería un caso claro en el que el derecho a la intimidad personal cedería frente a la potestad que tiene la Administración de proteger sus finanzas y resguardar la forma en que se lleva a cabo su contabilidad, además de su potestad de dirigir y controlar la actividad laboral de sus trabajadores cuando, en apariencia, esta actividad está perjudicando gravemente el funcionamiento de la Administración".[369]

Dicho esto la Corte se detiene en el requisito del "perjuicio", y señala que sin este elemento podrían existir situaciones en los cuales un empleado podría tener almacenados archivos o documentos meramente personales en su computadora y, no por ello, el empleador se encuentra facultado sin más para accesar a esos archivos. De esta forma, a juicio de la Sala Constitucional, sólo cuando el empleador tiene una duda bastante fundada de que la información que pueda tener el empleador le podrían estar ocasionando perjuicios en el funcionamiento de su empresa u oficina pública, sólo en ese caso el empleador se encontraría facultado a intervenir sin previo aviso. Sin perjuicio, de esta potestad que tendría el empleador, la Corte Suprema señaló que es necesario que exista una proporcionalidad entre el fin perseguido por el empleador y el derecho a la intimidad y privacidad de los documentos o archivos digitales que mantenga el trabajador en la computadora asignada, a fin de que sea en casos especialísimos donde el empleador proceda a ejercer estas potestades, ya que los trabajadores no dejan su derecho a la vida privada y la protección de sus datos cada vez que ingresan a su lugar de trabajo, sino que, por el contrario, esperarían legítimamente encontrar en ese lugar un cierto grado de privacidad, el

[368] Punto IV Sentencia 7573 del año 2012 pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica.
[369] Ibídem.

cual debe conciliarse con otros derechos e intereses legítimos como los que tiene el empleador, ya sea este una empresa privada o un órgano público.[370]

Luego de esto la Corte Suprema entra a analizar el caso en concreto en particular, de esta forma reconoce el interés legitimo que tenía la Municipalidad señalando que "existen ciertos escenarios en los que el derecho a la intimidad que le asiste al trabajador, debe, excepcionalmente, conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con eficacia y eficiencia, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones irregulares de los trabajadores o funcionarios. En la especie, aprecia la Sala que el levantamiento de la información electrónica en cuestión fue debido a información manejada por la Alcaldesa de Atenas, en el sentido que se habían detectado irregularidades en el Departamento de Contabilidad de ese Municipio, específicamente en cuanto a las conciliaciones bancarias, y fue por ello que se decidió tomar medidas, entre ellas la separación temporal del recurrente de su cargo (en su condición de encargado de dicho Departamento), y la orden de iniciar una investigación en su contra. Bajo esa perspectiva, considera la Sala que en el caso expuesto por el tutelado se cumplen los supuestos en los que, excepcionalmente, puede el empleador acceder a este tipo de datos privados, pues lo que en apariencia almacenaba el funcionario en su computadora eran trabajos privados de contabilidad que podían poner en peligro el prestigio de la Municipalidad (lo cual será dilucidado en el procedimiento administrativo) y que, a su vez, iban en contra del plus salarial por prohibición que se le reconoce en esa Corporación. En opinión de este Tribunal, la Municipalidad recurrida ha demostrado su interés legítimo y, por ende, ha cumplido el principio de finalidad legítima explicado en esta sentencia, en la medida en que ella también debe hacer prevalecer su derecho de administrar con eficiencia, eficacia, y transparencia la función pública que le fue encomendada, y su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones irregulares que -se sospecha- fueron cometidas por el recurrente. Así las cosas, la Sala encuentra que la Municipalidad de Atenas sí tenía un interés legítimo y constitucionalmente válido para recabar esta prueba e incorporarla a la investigación que está realizando, con las necesarias medidas de seguridad que ha tomado la autoridad recurrida".[371]

De esta forma, la Corte Suprema en su voto de mayoría, considera que el derecho a la intimidad no habría sido vulnerado, no así respecto al derecho al debido proceso, sobre el cual señala que "este Tribunal estima que el levantamiento de la información en cuestión sin la presencia del recurrente, constituye una vulneración al debido proceso, ya que se le privó de la posibilidad de estar presente durante una diligencia que lo podría afectar, sin poder fiscalizar el procedimiento y sin haber podido eliminar o almacenar en algún dispositivo de su propiedad aquella información de carácter estrictamente privado y que no causara perjuicio directo a la Municipalidad (ver en similar sentido, sentencia número 2005-015063 de las 15:59 horas del 01 de noviembre de 2005)".[372] Razón por la cual la Corte

[370] Ibídem.
[371] Punto V Sentencia Expediente Nº 7573 del año 2012 pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica.
[372] Ibídem.

Constitucional sólo acoge el amparo respecto a esta vulneración del debido proceso y no en cuanto al derecho a intimidad.

Es interesante hacer mención a la nota separada de la magistrada Calzada y los magistrados Castillo y Piza, quienes señalan que concurrieron con el voto de mayoría porque consideraban que en esta causa se vulneraron los derechos del recurrente en cuanto al levantamiento de la información sin su presencia, pero ellos consideraron además que si se había vulnerado el derecho a la intimidad del recurrente, ya que la actuación de la Municipalidad de Atenas de incursionar en su computador, sin previa advertencia sobre el uso y el control de los medios electrónicos por parte de la Municipalidad, suponía una lesión a su derecho a intimidad y vida privada. Para llegar a esta conclusión los magistrados señalan que, tal como se mencionó en el análisis del derecho a intimidad hecho en el punto IV de la sentencia, la celebración de un contrato de trabajo no implica en modo alguno la privación para el trabajador de los derechos que la Constitución le reconoce, tal como también ha mencionado el Tribunal Constitucional Español. Los magistrados citan así lo señalado por éste: "Es necesario preservar el equilibrio entre las obligaciones dimanantes del contrato para el trabajador y el ámbito de su libertad constitucional, pues dada la posición preeminente de los derechos fundamentales, la modulación derivada del contrato de trabajo sólo se producirá en la medida estrictamente imprescindible para el logro del legítimo interés empresarial (Sentencias 99/1994, 204/1997)".[373]

Luego de esta afirmación señalan que en el caso en concreto lo que buscan es encontrar el equilibrio entre los derechos del funcionario de la Municipalidad, específicamente su derecho a la intimidad personal, y el logro de los intereses legítimos de dicho organismo, al cumplimiento de las obligaciones de sus empleados públicos y al buen uso de los instrumentos de trabajo, como en este caso el computador que puso a su disposición la misma Municipalidad de Atenas. Así, los magistrados señalan que "los llamados derechos laborales inespecíficos o derechos fundamentales de orden general- adquieren una significación especial en el marco de las relaciones de trabajo o de empleo público, las que modulan su ejercicio para hacerlo compatible con el poder de dirección del empleador público o privado-. Es verdad, por ello, que el ejercicio de esos derechos en el seno de una entidad o de una unidad de trabajo, queda limitado por los derechos de los demás trabajadores y de los propios empleadores, puesto que la libertad de reunión, de libertad de expresión o el derecho a la intimidad, por ejemplo, no pueden afectar la operación de la empresa o entidad donde trabajan, ni pueden impedir el uso de controles preventivos razonables; pero es verdad también, que una persona por el hecho de trabajar y cruzar el umbral de una entidad para la que trabaja, no se despoja ni renuncia a esos derechos, sino que sólo los hace compatibles con sus deberes y los derechos de los demás (otros trabajadores, los empleadores y las normas aplicables a su actividad o función). Y como esto es así, compete también a las autoridades administrativas, judiciales y constitucionales, velar por su vigencia, proteger a sus titulares, resolver controversias y garantizar el ejercicio de esos derechos fundamentales".

[373] Punto IX Sentencia Expediente Nº 7573 del año 2012 pronunciada por la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica.

Dicho esto los Magistrados hacen alusión al criterio jurisprudencial que se ha ido creando, y señalan que "[y]a esta Sala Constitucional, en Sentencia # 2005-15063, del primero de noviembre del dos mil cinco, había establecido: En primer término, es preciso señalar que el correo electrónico y los documentos electrónicos almacenados en la computadora que utilizaba la recurrente, aunque sea un bien público, están protegidos por el derecho fundamental al secreto de las comunicaciones y nunca podría realizarse un control de los mismos con garantías inferiores a las establecidas por el mencionado precepto. Asimismo, el hecho que la computadora sea propiedad del Ministerio de Comercio Exterior, no significa que la amparada haya renunciado completamente a la garantía de inviolabilidad de las comunicaciones privadas, por cuanto, como se indicó anteriormente, la garantía del derecho fundamental no depende de la titularidad del medio sino que es independiente de la titularidad del soporte (En este sentido, puede verse la sentencia del Tribunal Europeo de Derechos Humanos de 24 de agosto de 1998 No. 872/1997, caso Lambert c. Francia). Los trabajadores no renuncian a la esfera de privacidad y a la protección de datos por ejercer una función pública, sino que, por el contrario, esperan legítimamente encontrar allí un grado de privacidad, ya que en él desarrollan una parte importante de sus relaciones con los demás. En otros términos, la circunstancia que al funcionario o empleado se le suministre un equipo para el cumplimiento y ejercicio de sus funciones de propiedad de la Administración o empleador-, no excluye que el mismo sea soporte de información confidencial o personal cubierta por el secreto o reserva de las comunicaciones y, en general, por el derecho a la intimidad« La apertura por el empleador de los mensajes electrónicos de la cuenta del funcionario o trabajador sólo es justificable en circunstancias muy limitadas ya que el acceso a este tipo de datos no es necesario para satisfacer un interés legítimo del empleador, debiendo prevalecer por el contrario el derecho fundamental al secreto de las comunicaciones. Por otra parte, la celebración de un contrato entre la Administración y la amparada en relación con la operación del equipo de cómputo, no implica la privación de los derechos que la Constitución le reconoce como ciudadana« En este sentido, el Ministro de Comercio Exterior ordenó el respaldo de toda la información que contenía el disco duro del ordenador, sin haber permitido que la recurrente eliminara la información de carácter privado que había almacenado. Con ello, resultaba sumamente fácil que cualquier persona ajena se impusiera en conocimiento de los mensajes y documentos privados sin el consentimiento de la agraviada, lo que supone una violación al artículo 24 de la Constitución Política« En el mismo sentido, merecen citarse las Sentencias #2006-005607,#2006-017380, #2007-011054, 2008-15332 (frente a una empresa privada) y #2010-010713. Aunque cada una con matizaciones diferentes, todas ellas recalcan, que a pesar de que una computadora sea de una empresa privada o institución pública, los datos privados que los -trabajadores y- funcionarios públicos allí tengan, deben ser respetados (la expresión es de la Sentencia #2007-011054). Por eso, la jurisprudencia de esta Sala Constitucional ha afirmado, que la apertura por el empleador de los mensajes electrónicos de la cuenta del trabajador sólo es justificable en circunstancias muy limitadas ya que el acceso a este tipo de datos no es necesario para satisfacer un interés legítimo del empleador, debiendo prevalecer por el contrario el derecho fundamental al secreto de las comunicaciones« (Sentencia # 2006-005607); y que si lo que se pretende demostrar es que supuestamente la recurrente le facilitaba información de máxima confidencialidad a quien no correspondía mediante correos electrónicos…(Sentencia #2006-005607); imponerse del conocimiento de esa

información, aun y cuando se utilice la computadora institucional o del patrono, es contrario al derecho a la intimidad personal. En el presente recurso, no se trata de valorar la conducta del recurrente a efectos disciplinarios, sino de resolver un problema previo sobre el alcance y la forma del control institucional sobre el uso, por un funcionario público, de la computadora que se le ha facilitado por la corporación municipal como instrumento de trabajo. Se trata, pues, del enjuiciamiento de una conducta a efectos disciplinarios desde la perspectiva del alcance de la protección de un derecho fundamental, y de la determinación de los límites del control institucional sobre un ámbito que aunque vinculado a las funciones públicas, puede afectar a la intimidad del recurrente".[374]

Luego los magistrados reconocen que cuando existe una expectativa razonable de intimidad esta no puede ser desconocida, es así como señalan que "[e]l hecho que la computadora sea propiedad de la Municipalidad, no significa que el amparado haya renunciado a la garantía de inviolabilidad de su intimidad ni al secreto de sus documentos privados, por cuanto, como ha dicho la jurisprudencia de esta Sala Constitucional, Es verdad, que la computadora asignada por la Municipalidad al señor U.D.R es un instrumento de trabajo, no un efecto personal del funcionario y que el uso de la computadora, por tanto, está sujeto a las facultades de control que la legislación laboral y administrativa concede a los empleadores y autoridades competentes; pero la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos facilitados por las entidades públicas o privadas a los trabajadores y funcionarios, crea una expectativa de confidencialidad que no puede ser desconocida (lo que está entre comillas es del Tribunal Supremo español, Sentencia STS 6128/2007 de 26 de septiembre sobre despido disciplinario por uso incorrecto de ordenador). Por ello, la entidad, de acuerdo con las exigencias de buena fe, antes de afectar la intimidad y el secreto de los documentos de sus trabajadores, debe establecer previamente las reglas de uso de esos medios e informar a los trabajadores y funcionarios que el uso de esos instrumentos se va a controlar, de manera que si la computadora se utiliza para usos privados en contra de esas prohibiciones y con conocimiento de los controles, no podría entenderse que al realizarse el control se vulnere lo que el Tribunal Europeo de Derechos Humanos ha llamado correctamente una expectativa razonable de intimidad".[375]

Finalmente, la magistrada Calzada y los magistrados Castillo y Piza, señalan que "[e]n el presente caso, aunque se haya dado un uso distinto al bien o instrumento suministrado por el patrono (la Municipalidad) al recurrente; la buena fe (principio constitucional y general del derecho laboral artículo 19 del Código de Trabajo); habría exigido no solo respetar el ámbito de intimidad conforme a lo dicho; sino apercibir previamente sobre el uso inadecuado del instrumento puesto a su disposición; antes de proceder a imponerse del contenido de los documentos incorporados en la computadora asignada por la Municipalidad al funcionario. Sin embargo, ese apercibimiento no se dio, ni tampoco se han establecido reglas de uso de los instrumentos informáticos previamente detalladas, ni se han dado a conocer específicamente a cada uno de los funcionarios a quienes se les asignan; ni mucho menos se ha informado previamente sobre la existencia de controles específicos y de

[374] Ibídem.
[375] Ibídem.

medidas que se aplicarían en relación con el uso inadecuado de las computadoras institucionales, por lo que era esperable que el recurrente considerara que los archivos personales incorporados en la computadora facilitada por la institución, estaban cubiertos por una expectativa razonable de intimidad".[376] Así los Magistrados concluyen que el actuar de la Municipalidad no sólo vulneró el debido proceso sino que también su derecho a intimidad.

México

1.11. Derecho a la Privacidad y Geolocalización de Teléfono Móvil

a) Acción de Inconstitucionalidad en contra del Decreto por el cual "se reforman, adicionan y derogan diversas disposiciones del Código Federal de Procedimientos Penales, del Código Penal Federal, de la Ley Federal de Telecomunicaciones, de la Ley que establece las Normas Mínimas sobre Readaptación Social de Sentenciados y de la Ley General del Sistema Nacional de Seguridad Pública", publicado en el Diario Oficial de la Federación el 17 de Abril de 2012.

Sentencia Expediente Nº 32-2012, pronunciada por la Suprema Corte de Justicia de México con fecha 16 de Enero de 2014. En la causa, don Raúl Plascencia Villanueva, en su carácter de Presidente de la Comisión Nacional de los Derechos Humanos interpone acción de inconstitucionalidad en contra de los artículos 133 Quáter, del Código Federal de Procedimientos Penales y 16, fracción I, apartado D y, 40 Bis de la Ley Federal de Telecomunicaciones, contenidos en el Decreto por el cual "se reforman, adicionan y derogan diversas disposiciones del Código Federal de Procedimientos Penales, del Código Penal Federal, de la Ley Federal de Telecomunicaciones, de la Ley que establece las Normas Mínimas sobre Readaptación Social de Sentenciados y de la Ley General del Sistema Nacional de Seguridad Pública" (en adelante el Decreto), toda vez que se les otorga a las Procuradurías General de la Republica y Locales la facultad de solicitar a los concesionarios del servicio de telecomunicaciones la localización geográfica, en tiempo real, de los equipos de comunicación móvil asociados a una línea, relacionados con la investigación de delitos de delincuencia organizada, contra la salud, secuestro, extorsión o amenazas y adiciona "algún delito grave" y con ello se vulneraría los artículos 14 y 16 de la Constitución Política de los Estados Unidos Mexicanos, 11 de la Convención Americana sobre Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos, 12 de la Declaración Universal de Derechos Humanos y 16 de la Convención sobre los Derechos del Niño, relativos a los derechos humanos a la privacidad o a la vida privada.

El recurrente señaló que, en el caso del artículo 133 Q, sería inconstitucional en conformidad al derecho humano a la privacidad o a la vida privada, ya que permitir que la Procuraduría General de la República y las demás entidades federativas, sin fundar y motivar la causa legal, se encuentran facultadas, sin límites, para ordenar la localización geográfica de una persona, en tiempo real, implicaría un ilimitado acceso a información privada, al constituir un registro exhaustivo y preciso de los movimientos públicos y la localización de la persona, lo que refleja detalles importantes sobre su vida personal, familiar, política, religiosa y

[376] Ibídem.

social.[377] Luego señala el recurrente que, en opinión de la Comisión Nacional de los Derechos Humanos de México (en adelante Comisión Nacional), la norma impugnada carecía de tres principios fundamentales que la convertían en una disposición arbitraria, al no acatar las garantías de legalidad y seguridad jurídica, así como el derecho humano a la privacidad o a la vida privada, los cuales eran los siguientes:

(i) Falta de participación de la autoridad judicial en la autorización, supervisión y revocación de la solicitud de localización geográfica de un equipo de comunicación móvil, ya que de acuerdo con la Constitución Federal de México, una persona no puede ser privada de sus derechos si no es mediante juicio seguido ante Tribunales competentes, ni ser molestada en su persona sin mandamiento escrito fundado y motivado, por parte de la autoridad competente, como se aprecia de tales preceptos. De modo que dichas disposiciones constitucionales contrastarían con la reforma impugnada en la presente acción de inconstitucionalidad, puesto que los numerales citados, permitirían que el derecho a la privacidad de una persona sea disminuido, sin que para tales efectos medie orden de una autoridad judicial, fundada y motivada que no sólo autorice la medida, sino además, supervise su debida aplicación y pueda revocarla en un tiempo determinado. Señala además la Comisión Nacional que en México existirían en su ordenamiento jurídico otras herramientas de persecución del delito de naturaleza invasiva de la privacidad de las personas, que para su procedencia, se requiere de autorización y supervisión judicial. A modo ejemplar señalar sería el caso de la intervención de comunicaciones o el cateo.[378]

(ii) Falta de precisión en el alcance de la medida, en cuanto a los sujetos que pueden ser destinatarios de la localización geográfica de un equipo de comunicación móvil. Respecto a esto, señalan que la norma debe ser clara y detallada en cuanto a sus alcances y limitaciones, lo que implica que deban precisarse de manera exacta, todas y cada una de las circunstancias y condiciones que deben concurrir para que proceda, ya que esta medida lesionaría derechos humanos, lo que incluiría a su vez un señalamiento sobre los particulares que podrían ser sujetos de la medida. Por lo que, en opinión de la Comisión Nacional, lo dispuesto por la invocada norma no satisface los requisitos de legalidad, certeza y seguridad jurídica que exige la Constitución Federal de México, pues la noción de "estar relacionados con investigaciones" es sumamente escueta, pues, podría comprender un amplísimo rango de personas.[379]

(iii) Falta de precisión en el alcance de la medida, en cuanto al límite temporal de duración. Respecto a esto el recurrente señala que la ausencia de un límite temporal sobre la facultad para monitorear la localización geográfica de una o varias personas, sumada a que la medida deba no sería otorgada por un juez, la convertiría en una atribución arbitraria y susceptible de abuso por parte de quien la tuviera a su cargo. Agrega que, toda disposición lesiva de los derechos humanos, tiene que contar con el elemento de proporcionalidad entre el fin perseguido y la medida.[380]

[377] Punto Tercero, Concepto de invalidez: Primero, Sentencia Expediente Nº 32-2012 pronunciada por la Suprema Corte de Justicia de México.
[378] Ibídem.
[379] Ibídem.
[380] Ibídem.

Además, el recurrente señala que el artículo 16, fracción I, apartado D, de la Ley Federal de Telecomunicaciones, violaría las garantía de legalidad, certeza y seguridad jurídica, además del derecho a la privacidad o a la vida privada, consagrados en los artículos 16 de la Constitución Federal, 11 de la Convención Americana sobre Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos, 12 de la Declaración Universal de Derechos Humanos, y 16 de la Convención sobre los Derechos del Niño.[381]

El recurrente a su vez menciona el caso "Escher y otros vs. Brasil", en el cual se condenó a Brasil por la intercepción y monitoreo ilegal de líneas telefónicas, la divulgación de comunicaciones y denegación de justicia, fundado entre otros por la vulneración al derecho a intimidad, lo cual en el presente caso significaría la vulneración del Artículo 11 de la Convención Americana de Derechos Humanos.

Señala además el recurrente que el artículo 16 de la Ley Federal de Telecomunicaciones, regularía las bases sobre las cuales habría de llevarse a cabo una licitación pública para concesiones sobre bandas de frecuencia del espectro para usos determinados y, en virtud de ello, establecería, entre otros aspectos, los requisitos que deberían cumplir los interesados en participar en la licitación. Entre otros, el interesado debería incluir una propuesta de las acciones coordinadas con la autoridad correspondiente, que permitiera combatir los delitos de extorsión, amenazas, secuestro en cualquiera de sus modalidades o algún delito grave o relacionados con la delincuencia organizada. De modo que en opinión de la Comisión Nacional daría pauta a diversas interpretaciones, la más grave a su parecer correspondía a que adicionaría supuestos de procedencia no previstos por el Código Federal de Procedimientos Penales, ya que incluiría, además de los delitos de delincuencia organizada, extorsión, amenazas y secuestro, a "algún delito grave" lo que no se previene en la ley adjetiva reformada, lo que por sí sólo es ilegal. Señala que como consecuencia de esta incongruencia se generaría un entorno de incertidumbre e inseguridad sobre los alcances de esta facultad, en concreto, si procede únicamente respecto de los delitos que enuncia el Código Federal de Procedimientos Penales, o también respecto de otros delitos graves. Además, señala que producto de esto se podría tener como premisa que el código adjetivo en materia penal establece un listado enunciativo de los delitos respecto de los cuales procede la facultad de solicitar la localización geográfica de equipos de telefonía móvil y, en una interpretación sistemática, concluir que los supuestos de procedencia se amplían por la disposición del artículo 16 que se impugna. Siendo así la Comisión Nacional considera que la facultad prevista por esta disposición legal podría llegar a ejercerse en investigaciones relacionadas con cualquier delito grave, lo que resultaría desafortunado desde la perspectiva del derecho a la privacidad o a la vida privada.

La Suprema Corte de México, previo a estudiar la constitucionalidad de las normas impugnadas hace las siguientes consideraciones respecto al Derecho a la privacidad o Intimidad, el cual señala se encuentra en el Artículo 16 primer párrafo de la Constitución Política de los Estados Unidos Mexicanos "dicha norma establece –en general- la garantía de seguridad jurídica de todo gobernado de no ser molestado en la privacidad de su persona, de su intimidad familiar, o de sus papeles o posesiones, sino cuando medie mandato de

[381] Punto Tercero, Concepto de invalidez: Segundo, Sentencia Expediente Nº 32-2012 pronunciada por la Suprema Corte de Justicia de México.

autoridad competente debidamente fundado y motivado, cuya finalidad principal es el respeto a un ámbito de vida privada personal y familiar que, por regla general, debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, con la limitante que la propia Ley Fundamental establece para las autoridades.

Asimismo, que la referida garantía –en un sentido muy amplio- puede extenderse a una protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad.

De aquí es posible derivar el reconocimiento de un derecho a la intimidad o a la vida privada que abarque las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de vida, con la salvedad anotada por la Carta Magna.

Así, el derecho a la intimidad o a la vida privada protege a la persona en la posibilidad de gozar de un ámbito (sea que éste se concrete en hechos o informaciones, en decisiones, o incluso un espacio físico) reservado frente a la acción y el conocimiento de los demás, ámbito que relaciona a la persona con su círculo cercano.

Ahora bien, conforme lo ha sostenido reiteradamente por este Alto Tribunal, los derechos fundamentales, entre ellos el derecho a la privacidad, no son absolutos, ni ilimitados en sí mismos; encuentran sus límites, bien en la misma Ley Fundamental de modo directo, o de manera indirecta o mediata en la legislación ordinaria, por la necesidad de preservar otros derechos o bienes protegidos constitucionalmente.

Así se desprende del primer párrafo del artículo 1º constitucional, al señalar que los derechos humanos reconocidos en la propia Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, pueden restringirse o suspenderse válidamente en los casos y con las condiciones que la misma Ley Fundamental establece.

De igual forma este principio encuentra reconocimiento en el ámbito internacional, en tanto el artículo 30 de la Convención Americana sobre Derechos Humanos (Alcance de Restricciones) dispone que las restricciones permitidas, de acuerdo con la Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas, lo que se confirma con la propia interpretación de la Corte Interamericana de Derechos Humanos.

De ahí que el legislador válidamente pueda regular y limitar su ejercicio, aunque siempre acotado a ciertas condiciones, en tanto los límites que establezca han de estar justificados por la necesidad de proteger a su vez otros derechos e intereses constitucionalmente tutelados, no deben ser arbitrarios o desproporcionales.

En este sentido es necesario tener en cuenta que las restricciones a todos los derechos fundamentales se engloban en el concepto de orden público, en tanto constituye el orden social que permite la vigencia efectiva de los mismos.

Así, en el ejercicio de un derecho fundamental se debe conciliar que éste no impida o llegue a bloquear la efectividad de otros derechos, esto es, conseguir la funcionalidad del sistema”.[382]

[382] Ibídem.

Señalado lo anterior la Suprema Corte analiza en primer lugar los artículos 133 Quáter del Código Federal de Procedimientos Penales y 40 bis de la Ley Federal de Telecomunicaciones, procediendo a determinar su alcance y contenido. Así, señala que esta norma otorga al Procurador General de la República la facultad de solicitar a los concesionarios o permisionarios del servicio de telecomunicaciones, la localización geográfica, en tiempo real, de los equipos de comunicación móvil asociados a una línea, que se encuentren relacionados con investigaciones de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas. Lo que permitiría establecer que la solicitud que dirige el Procurador General de la República, o las personas en quienes delegue esta facultad, a concesionarios o permisionarios del servicio de telecomunicaciones, tiene por objeto conocer la localización de un equipo terminal móvil asociado a una línea telefónica determinada en el momento en que se procesa la búsqueda, y no así de la intervención de las comunicaciones que se realicen a través de tales equipos, ni siquiera del registro de las llamadas.

En este sentido es una medida que no tiene otro propósito que dotarlo de una herramienta efectiva en el curso de una investigación. Señala además, que esta facultad, conforme lo dispone la norma cuestionada, es delegable en los servidores públicos que determine el Procurador y la ejerce mediante solicitud que puede emitir por simple oficio o por medios electrónicos, quienes por lo demás tienen una obligación de sigilo sujeta a sanciones en caso de que la autoridad investigadora utilice los datos e información obtenidos, para fines distintos a los señalados en la disposición, remitiendo este incumplimiento a una norma del Código Penal Federal, que establece una de las hipótesis en que se configura el delito de ejercicio indebido de servicio público.

Por lo demás, existiría de manera correlativa una obligación a concesionarios y permisionarios de telecomunicaciones la obligación de atender las solicitudes que les formule la autoridad, previendo a su vez una sanción respectiva en caso de incumplimiento, obligación que el artículo 40 bis de la Ley Federal de Telecomunicaciones en cuestión reiteraría expresamente, como un deber de colaboración a cargo de los concesionarios y permisionarios del servicio de telecomunicaciones, el que se extiende respecto de las solicitudes que emitan de los procuradores de las entidades federativas o de los servidores públicos en quienes deleguen esta facultad, de conformidad con las leyes correspondientes.

La Suprema Corte por lo demás analiza las facultades que la Constitución Federal y las leyes confieren al Ministerio Público, y concluye que la localización de un equipo de comunicación móvil asociado a una línea se inserta dentro de las actividades y diligencias propias de la investigación de los delitos, que la ley le confiere al Ministerio Público, mediante tecnologías disponibles en materia de telecomunicaciones, con las que deben contar los concesionarios o permisionarios del servicio, que tienden a facilitar y hacer más eficaz la persecución de delitos que lastiman de manera singular a la sociedad, como consta del proceso legislativo del que emanaron las normas generales que se cuestionan. Señala además la Suprema Corte que la intención del legislador al aprobar este paquete de reformas fue fortalecer las herramientas de la autoridad ministerial en el combate de delitos en materia de delincuencia organizada, secuestro, extorsión o amenazas. Y, en lo particular, por cuanto a la geolocalización, busca consolidar un marco legal que permita al Estado Mexicano investigar

con mayor eficacia, en tiempo real, delitos que se consuman en materia de delincuencia organizada, secuestro, extorsión o amenazas, con el fin de establecer la posibilidad de fijar geográficamente la ubicación aproximada del lugar de donde se está realizando la llamada que provenga de sus autores o copartícipes, con la intención de proceder a su aprehensión y, lo que es más importante, localizar y rescatar con vida a la víctima del secuestro, cuando se trate de este delito. Razón por la que la posible restricción a la vida privada de una persona, que pudiera tener lugar de solicitarse la localización de un equipo de comunicación móvil, debe ceder en interés de preservar el orden público y la paz social, garantizar la protección de los mencionados derechos, y la eficaz investigación de los delitos. Cabe señalar que la Corte señala que la medida que se cuestiona, se acota a la ubicación del lugar del que proviene una llamada realizada a través de un equipo móvil asociado a una línea y no comprende la intervención de comunicaciones ni el registro de llamadas, medidas para las cual existiría una diversa reglamentación, por lo que no cabría estimar que se vulnera el derecho a la privacidad.

Siguiendo con su argumentación la Corte señala que siguiendo la recta lectura de las disposiciones cuestionadas, estas otorgarían esta facultad a la autoridad ministerial solo de forma excepcional, no procediendo indiscriminadamente, sino solo en los casos señalados taxativamente. La Corte, en su razonamiento, se hace cargo respecto de los tres principios fundamentales que carecerían las normas impugnadas del siguiente modo:

(i) Falta de participación de la autoridad judicial en la autorización, supervisión y revocación de la solicitud de localización geográfica de un equipo de comunicación móvil: respecto a esto la Suprema Corte señala que la medida de que se trata tiene por objeto la localización geográfica de un equipo de comunicación móvil, en modo alguno constituye un acto de privación, pues no tiene como efecto disminuir o suprimir en forma definitiva un derecho del particular que en su caso lo detente o se encuentre en posesión del mismo, señala además que el ejercicio de esta facultad que confiere la disposición al Procurador General de la República y a quienes éste la delegue, como todo acto de autoridad, deberá ajustarse a lo que dispone el primer párrafo del artículo 16 de la Constitución Federal, sin que sea necesaria la intervención judicial por lo que deberá constar por escrito de la autoridad competente, que funde y motive la causa legal del procedimiento, requerimientos que contrario a lo que aduciría la recurrente devienen de la propia norma, pues además de que faculta al Procurador General de la República o a las personas que éste determine, para solicitar la localización de un equipo móvil, le impone la obligación de formular tal solicitud en forma escrita o por medios electrónicos y sólo la podrá requerir en los supuestos que acota la disposición, extremos que en todos los casos deben cumplirse.

Señala además la Suprema Corte que la comparación que propone el recurrente con el cateo o la intervención de comunicaciones, respecto de las cuales, afirma, el legislador acató las normas constitucionales en su regulación, no resulta ser un parámetro para demostrar la inconstitucionalidad de las disposiciones impugnadas, ya que estas por su objeto mismo son invasivas de la privacidad de las personas, lo que hace necesaria la intervención y ponderación por parte de la autoridad judicial para su práctica, lo que no acontecería respecto de la localización de aparatos móviles desde los cuales se origina una llamada, cuyos alcances solo serían para localización.

(ii) Falta de precisión en el alcance de la medida, en cuanto a los sujetos que pueden ser destinatarios de la localización geográfica de un equipo de comunicación móvil: respecto a esto la Corte señalo que el alcance de la medida, por cuanto los sujetos que pueden ser destinatarios de la localización de un equipo de comunicación, atento al objeto de la misma, la ausencia de la precisión que se apunta deviene innecesaria, pues será en todo caso los elementos que aporte a la investigación que produzca como resultado el conocimiento de quien o quienes hacen uso del equipo de comunicación móvil o lo detentan, o demás indicios sobre la comisión de un delito, en cuyo supuesto no se exime a la autoridad investigadora de cumplir con las formalidades que la ley prevé de resultar procedentes otras medidas en la indagatoria a su cargo, una vez identificados los probables responsables de los delitos que se investigan.

(iii) Falta de precisión en el alcance de la medida, en cuanto al límite temporal de duración: respecto a esto señala que la disposición tiene por objeto la ubicación geográfica de un equipo de comunicación móvil en tiempo real, se agota en el momento en que se determine la posible localización del equipo. Señala además que no debe perderse de vista que la norma cuestionada autoriza al Procurador General de la República o a los servidores públicos en quienes delegue la facultad, para solicitar la localización geográfica de equipos de comunicación móvil, asociados a una línea, que se encuentren relacionados en la investigación de ciertos delitos, en una relación de medio a fin, de modo que debe entenderse que esta facultad subsiste y se justifica mientras subsista el hecho que la originó, y colmado éste, tal facultad se extingue, por lo cual no puede afirmarse que no esté acotada a un límite temporal, supeditado a la propia investigación y a los elementos que vaya arrojando. La Corte señala un ejemplo de un caso de secuestro y señala que si la localización geográfica del equipo móvil desde el cual se están realizando llamadas, no arroja datos sobre el lugar en que se encuentra retenida la víctima y la investigación continúa, la posibilidad de que la autoridad ministerial ejerza la facultad que le confiere la norma subsiste, en tanto precisamente la averiguación previa consiste en aquellas diligencias que realiza la autoridad investigadora en ejercicio de sus funciones de orden público y en cumplimiento de un imperativo constitucional, con objeto de indagar si hay elementos para determinar la existencia o no de un delito y, en su caso, a conducir a sus probables responsables.

La Suprema Corte posteriormente toma en consideración lo señalado por la Comisión Nacional respecto del caso “Escher y otros vs. Brasil”, resuelto por la Corte Interamericana de Derechos Humanos, y considera que “el caso que se invoca versó sobre conductas diversas a las que autorizan las normas cuestionadas. Y si bien la Corte Interamericana se pronuncia en el sentido que el artículo 11 de la Convención Americana sobre Derechos Humanos se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones, es necesario insistir que la medida que autoriza la norma no está dirigida a una persona en lo particular, ni tiende tampoco a obtener información sobre el contenido de sus comunicaciones, sino que constituye un instrumento que acotado a

la investigación de ciertos delitos, pretende evitar se sigan perpetrando en perjuicio de las víctimas".[383]

Por lo demás, la Corte consideró que las normas cuestionadas cumplían con el artículo 11.2 de la Convención Americana de Derechos Humanos ya que la medida de geolocalización perseguía un fin legitimo, ya que, tendía a facilitar la investigación y persecución de ciertos delitos mediante el uso de tecnologías de vanguardia en materia de telecomunicaciones, delitos enunciados taxativamente en los que los bienes jurídicamente tutelados son la vida, la seguridad, la libertad e integridad física y sicológica de las personas y la salud pública, todo lo cual justifica se confiera su acceso a la autoridad ministerial, precisamente en atención a la particular protección que merecen, tanto como en aras de mantener el orden público y la paz social, y evitar que tales delitos se sigan perpetrando. Era idonea, porque se constituye en un medio apto para alcanzar el fin perseguido, ya que consideró que la delincuencia organizada por lo general utiliza estos aparatos para perpretar los hechos delictivos, considerados en la norma. Además señaló que era necesaria, en la medida que se constituye en una herramienta eficaz en la investigación y persecución de los delitos taxativamente previstos, que de otra forma pudiera verse menoscabada o limitada, al privarse a la autoridad de instrumentos suficientes y adecuados, más aún si se toma en cuenta que es un hecho notorio que la geolocalización es un servicio que ofrecen proveedores particulares para recuperar bienes o conocer su ubicación precisa. Y por último que era proporcional en sentido estricto, toda vez que la posible restricción que supone se ve compensada por la importancia de los bienes jurídicamente protegidos, y en aras de mantener el orden público y la paz social que se presuponen como base para la consolidación de un estado democrático de derecho, ante lo cual debe ceder el interés particular.

De esta forma la Corte Consideró que el Artículo 133 Quater del Código Federal de Procedimientos Penales y 40 bis de la Ley de Telecomunicaciones no resulta violatorio del derecho de privacidad. Sin perjuicio de lo cual, la Suprema Corte señala que "conviene puntualizar que aun reconociendo que pudieran constituir una intromisión al ámbito privado de los individuos, de cualquier forma satisfacen los parámetros de razonabilidad y proporcionalidad que este Alto Tribunal ha determinado en el ejercicio del control de constitucionalidad, por lo que cabe todavía una precisión más.

Si bien es cierto que, por regla general, toda invasión al derecho a la privacidad requiere una orden judicial. Conforme a los criterios de este Alto Tribunal y del sistema interamericano de derechos humanos, sólo puede prescindirse de tal orden en los casos de urgencia, esto es, (i) cuando se pongan en riesgo la vida o integridad física de las víctimas del delito, o bien, (ii) cuando exista riesgo de que se oculte o desaparezca el objeto del delito.

Así, las normas impugnadas son constitucionales si y sólo si, se interpreta que las mismas tienen aplicación únicamente en estos supuestos de excepción, lo cual deberá estar suficientemente motivado por la autoridad competente.

[383] Considerando Quinto, Sentencia Expediente Nº 32-2012 pronunciada por la Suprema Corte de Justicia de México.

Conviene señalar que la explicable necesidad de que en algunos casos la geolocalización deba dictarse con la premura requerida para proteger a las víctimas o preservar la identificación del lugar en que se origina una llamada, tampoco releva a la autoridad ministerial de su obligación constitucional de fundar y motivar sus actos, concretamente mediante: 1. La instrucción al personal técnico que corresponda, que mínimamente razone la excepcionalidad del caso, dado el tipo de delitos que se investiga; 2. La averiguación previa en la que se provee la medida, y 3. Las condiciones fácticas que revelen la eventualidad de daño a las personas o del ocultamiento de datos para esclarecer los hechos de la investigación; de todo lo cual habrá de dejarse constancia en el expediente cuya información deberá de mantenerse en sigilo hasta el momento procesal oportuno, de modo que ni aún el concesionario o permisionario del servicio puedan acceder a ella".[384].

De esta forma, la Suprema Corte no descarta que podría llegar a restringir el derecho a intimidad, pero considera que, incluso ocurriendo tal caso, se cumpliría con los estándares que habilitan esta limitación.

Luego de analizado la disposición del 133 Quater del Código Federal de Procedimientos Penales y 40 bis de la Ley de Telecomunicaciones, la Suprema Corte analiza la norma del artículo 16, fracción I, apartado D, de la Ley Federal de Telecomunicaciones, la cual violaría las garantía de legalidad, certeza y seguridad jurídica, además del derecho a la privacidad o a la vida privada, puesto que su redacción admite diversas interpretaciones, así la Corte señala que en un primer escenario de interpretación, partiendo de que la finalidad del Código Federal de Procedimientos Penales fue establecer de manera limitativa los supuestos de procedencia de la facultad para solicitar la localización geográfica de equipos de comunicación móvil, al disponer en la norma que se tilda de inconstitucional, que los interesados en participar en una concesión de bandas de frecuencia del espectro, incluirán las acciones coordinadas con la autoridad para combatir los delitos de extorsión, amenazas, secuestro en cualquiera de sus modalidades o algún delito grave o relacionado con la delincuencia organizada, se extralimita, por lo que como consecuencia, esta falta de congruencia, crearía un entorno de incertidumbre e inseguridad sobre los alcances de esta facultad, en concreto, si procedería únicamente respecto de los delitos que enuncia el Código Federal de Procedimientos Penales, o también respecto de otros delitos graves.

El segundo escenario, se refiere a que se podría tener como premisa que el código adjetivo en materia penal establece un listado enunciativo de los delitos respecto de los cuales procede la facultad de solicitar la localización geográfica de equipos de telefonía móvil y, en una interpretación sistemática, concluir que los supuestos de procedencia se amplían por la disposición del artículo 16 que se impugna, y así bajo esta interpretación, se llegaría al extremo de considerar que tal facultad se puede ejercer también en investigaciones relacionadas con cualquier delito grave, lo que resultaría desafortunado desde la perspectiva del derecho a la privacidad o a la vida privada.

La Suprema Corte cita el numeral impugnado el cual dispone:

"Artículo 16. Para llevar a cabo el procedimiento de licitación pública a que se refiere el artículo 14 de esta Ley, la Secretaría publicará en el Diario Oficial de la Federación y en un

[384] Ibídem.

periódico de la entidad o entidades federativas cuya zona geográfica sea cubierta por las bandas de frecuencia objeto de concesión, convocatoria para que cualquier interesado obtenga las bases correspondientes.

Las bases de licitación pública incluirán como mínimo:

I. Los requisitos que deberán cumplir los interesados para participar en la licitación, entre los que se incluirán:

[…]

D. En el caso de los servicios de telecomunicaciones, las acciones coordinadas con la autoridad correspondiente, que permitan combatir los delitos de extorsión, amenazas, el secuestro en cualquiera de sus modalidades o algún delito grave o relacionado con la delincuencia organizada.

[…]".[385]

Y señala que esta disposición no tiene su origen, ni una vinculación directa, con la adición del artículo 133 Quáter al Código Federal de Procedimientos Penales, que permitiría establecer otro alcance, que no sea un deber de colaboración con la autoridad ministerial por parte de empresas concesionarias o permisionarias de los servicios de telecomunicaciones. Razón por la que considera que es válido el artículo.

De esta forma la Suprema Corte estima que la acción de inconstitucionalidad es infundada razón por la cual reconoce la calidez de los artículos 133 Quáter del Código Federal de Procedimientos Penales, 16, fracción I, apartado D y 40 Bis de la Ley Federal de Telecomunicaciones, en los términos de los considerandos quinto y sexto de este fallo.

Cabe hacer presente los votos de los ministros que estuvieron por conceder la acción de inconstitucionalidad o que hubieran adoptado otra línea argumentativa respecto del artículo 133 Quáter del Código Federal de Procedimientos Penales, los artículos 16, fracción I, apartado D y 40 Bis de la Ley Federal de Telecomunicaciones :

- Ministro José Ramón Cossío Díaz quien señalo que "el punto de partida del análisis debe ser el derecho humano que protege la Constitución y no la facultad de la autoridad. En abstracto, este derecho nos tiene que llevar hacia la consideración de que toda medida legislativa es inconstitucional siempre que potencialmente vulnere este derecho y no exista una justificación de su necesidad constitucional, razonabilidad y proporcionalidad, no en un conjunto de casos, supuestos o delitos, sino razonado para cada uno de ellos, permitiendo a este Tribunal un control particular con el que se permita su examen pormenorizado y se evite una justificación de un supuesto por otro.

  Aún siendo sensible a las condiciones sociales y políticas, y en particular, de seguridad del Estado mexicano como condición fáctica, éstas no pueden llevarme a constituir una razón de justificación general de la medida impugnada, menos aún como una facultad del legislador ordinario. En un momento dado, esta situación podría explicar una eventual modificación de la propia norma constitucional, o la declaración de suspensión de garantías o derechos humanos ahora, pero nunca la justificación de la norma ordinaria que va más allá del propio sistema de derechos y facultades que la Constitución reconoce y pretende hacer operativas y

[385] Considerando Sexto, Sentencia Expediente Nº 32-2012 pronunciada por la Suprema Corte de Justicia de México.

eficaces".[386] Razón por la cual considera que el artículo 133 Quáter del Código Federal de procedimientos penales y 40 bis de Telecomunicaciones debieron haber sido declarados inconstitucionales.

- Ministra Olga Sánchez Cordero de García Villegas: ella consideró que si bien, la medida cumplía con los requisitos de perseguir un fin legítimo y ser idónea para alcanzar dicho objetivo carecía de garantías suficientes para ser una medida absolutamente necesaria, pues existen otros medios que alcanzan el propósito buscado por la norma, de manera menos intrusiva o con mayores garantías para el respeto al derecho a la vida privada. La ministra consideró necesario que, dada la imposibilidad de que el individuo utilice medios de defensa y de control ex ante en contra de un potencial uso arbitrario de herramientas como la geolocalización, es necesaria la existencia de salvaguardas. Estas podrían ser, entre otras la autorización judicial, de un aviso simplemente en casos de extrema urgencia o necesidad debidamente justificada, o de cualquier otro mecanismo que garantice un control y regulación de la medida. De otro modo, las personas carecerían de la seguridad de que su información personal contará con un mínimo de confidencialidad; y que solo será utilizada en los casos expresamente establecidos en la ley, cuando se ha acreditado, prima facie, la razonabilidad de su empleo.

  Señala la ministra que, en un sentido parecido, las Naciones Unidas lo han mencionado al interpretar el Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos el cual se refiere a la prohibición de injerencias arbitrarias o ilegales en la vida privada, familia, domicilio o correspondencia, es así que señala que "el Relator de Naciones Unidas sobre Promoción y Protección de los Derechos Humanos en el Combate al Terrorismo ha señalado que los Estados pueden hacer uso de las medidas de vigilancia, siempre que se trate de casos específicos de interferencia, sobre la base de un aviso o una orden emitida por un juez en mostrar una causa o motivos razonables probables, pero adicionalmente debe entenderse que la lucha contra la inseguridad ciudadana no es una opción que "…automáticamente legitime cualquier interferencia con el Derecho a la Privacidad. [Y] cada instancia de injerencia necesita ser sujeta a una evaluación crítica" a través de una garantía, en cuyo caso la mejor opción es la autoridad judicial". De esta forma ella señala que, en la legislación mexicana sería indudable cumplir con los extremos de los artículos 16 de la Constitución Federal; los numerales 8 y 11 de la Convención Americana y 17 del Pacto Internacional de Derechos Civiles y Políticos; y, al no satisfacerse estos requisitos en las normas deviene su inconstitucionalidad. Por lo que, si bien, a su juicio, no se trataría propiamente del supuesto previsto textualmente en el artículo 16, le parece que las razones que imperan en ambos casos son las mismas. Idea que cree se refuerza si se considera que la información debe ser protegida en todos sus aspectos, dado que es un requisito indispensable que cualquier restricción a un derecho fundamental que ésta se encuentre debidamente justificada, entre otros, a la luz del principio de proporcionalidad.[387] Conforme a este razonamiento la ministra concluye que debió haber sido declara la inconstitucionalidad de las normas cuestionadas.

[386] Voto Particular Ministro José Ramón Cossío Díaz, Sentencia Expediente Nº 32-2012 pronunciada por la Suprema Corte de Justicia de México.

[387] Voto Particular Ministra José Olga María del Carmen Sánchez Cordero, Sentencia Expediente Nº 32-2012 pronunciada por la Suprema Corte de Justicia de México.

- Ministro Arturo Záldivar Lelo de Larrea, quien señala si bien considera que los preceptos impugnados eran válidos, la línea argumentativa que se adopto debió haber sido otra, es así como señala que "la norma debía ser leída de modo que permita armonizar las necesidades del Estado en el combate al crimen con el respeto a los derechos humanos, integrando en su interpretación los requerimientos de proporcionalidad que señala la jurisprudencia de la Corte Interamericana de Derechos Humanos. En este sentido, coincido con el sentido de la resolución respecto a que la norma es constitucional pero siempre y cuando tal disposición sea interpretada de acuerdo a los requisitos establecidos por la Corte Interamericana de Derechos Humanos y a los exigidos por el derecho penal mexicano tratándose de intromisiones al derecho a la privacidad".[388]

  De esta forma el ministro consideró que sólo si las normas impugnadas tenían aplicación en los supuestos de excepción contemplados, además de estar suficientemente fundadas por la autoridad competente, lo cual debería haber quedado más claro en la sentencia, consideraba que sólo así las normas impugnadas serían constitucionales.

- Ministro Alfredo Gutiérrez Ortiz Mena, en su voto concurrente señaló que él coincide con la decisión pero considera importante hacer algunas consideraciones que lo llevan a separarse de algunos de los razonamientos de la mayoría. De esta forma señala que coincide con la decisión mayoritaria que concluye (i) que la medida de localización geográfica de equipos móviles no tiene el efecto principal ni incidental de acceder a los contenidos de las conversaciones, (ii) ni proceder a la identificación específica de una persona, sino a la identificación limitada de un equipo que puede estar relacionado con la comisión de un delito, el cual puede llevar a cualquier persona relacionada con el mismo. El Ministro señala que la pregunta relevante era otra, a saber, ¿Si existe una expectativa de privacidad legítima sobre la señal generada por un equipo de comunicación móvil para su ubicación en un momento preciso y efímero, señal que no se obtiene mediante el acceso a un lugar protegido constitucionalmente, sino que se obtiene mediante el registro de un dato generado en la infraestructura de telecomunicaciones? Respecto a esta interrogante en su opinión la respuesta es negativa por tres razones:

  "1) Las señales de ubicación que envía un equipo móvil forman parte de un ámbito de información disponible para los permisionarios o concesionarios de telecomunicaciones para muy distintos propósitos comerciales, por tanto, a diferencia de los contenidos de las conversaciones, no cabe esperar que esas señales de ubicación no sean conocidos por nadie; más bien lo contrario se presupone. Esta identificación es importante para contabilizar en alguna forma las llamadas locales y de larga distancia y distintos servicios. Esta razón, sin embargo, no es suficiente por sí misma para justificar la conclusión, pero ayuda a ilustrar que el espacio de intimidad del que se trata no es uno que pertenezca a una intimidad en sentido fuerte de las personas.

  2) Las señales de ubicación de los equipos móviles de comunicación forman parte de un ámbito disponible de información no sólo para propósitos comerciales, sino también para una potencial regulación del Estado, por tanto, no puede esperarse razonablemente que esa señal de identificación sea de conocimiento privado de quien lo usa. Incluso el artículo 27 constitucional otorga facultades al nuevo Instituto Federal de Telecomunicaciones para "la regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de radiofusión y telecomunicaciones".

[388] Voto Concurrente Ministro Arturo Zaldívar Lelo de Larrea, Sentencia Expediente Nº 32-2012 pronunciada por la Suprema Corte de Justicia de México.

3) Sobre la base de lo anterior, cabe afirmar que las redes de telecomunicaciones sobre las cuales se generan las señales de identificación de los equipos móviles son las autopistas del siglo XXI, por lo que si en otras circunstancias no se ha considerado que la identificación de las placas de los automóviles o demás rasgos de identificación de una unidad por parte de un agente policiaco sea equivalente a entrometerse en un espacio en el que exista una expectativa de privacidad legítima —a diferencia de la intromisión en las comunicaciones que tienen lugar en el interior de los automóviles— no veo razón para afirmar lo contrario en este caso. Esta analogía es inevitable, pues como lo estableció este Tribunal Pleno en la jurisprudencia 65/2007, el espectro radioeléctrico forma parte del espacio aéreo que constituye un bien nacional de uso común sujeto al régimen de dominio público de la federación".[389]

En definitiva, señala que al no existir una expectativa de privacidad legítima, debe concluirse que la identificación del equipo de comunicación móvil no exige autorización judicial. Por lo que el artículo 16 de la Constitución Nacional de los Estados Unidos de Mexicanos sólo exigiría que la utilización del instrumento de investigación no sea arbitraria y, por tanto, basta con que se funde y motive la causa legal y sea emitido por autoridad competente.

Es importante señalar que luego de señalado esto el Ministro se refiere al cuidado que se debe tener en casos futuros en relación con el uso del almacenamiento de datos y señala que "[e]n casos futuros que involucren tecnología equivalente, estimo, que los jueces constitucionales deberán analizar con igual visión integral la preocupación constitucional de proteger la intimidad de las personas y habrá de analizarse nuevas posibilidades de abuso en el almacenamiento de datos que revelen aspectos de la identidad de las personas sobre los cuales podría existir una expectativa de privacidad legítima.

Si este llegara a ser el caso, la expectativa de privacidad legítima habría, a diferencia de este caso, de ameritar una protección constitucional mayor y, por tanto, la aplicación de un escrutinio estricto, que no sólo amerite verificar los pasos de la necesidad, idoneidad y proporcionalidad, sino también requiera de la participación de una autoridad judicial para su utilización".[390]

De esta forma el Ministro reconoce la importancia de la afectación que podría ocasionarse al derecho a intimidad cuando se abusa del almacenamiento de datos y se violenta la expectativa de privacidad legítima, señala finalmente que este no sería el caso en cuestión y que este último punto al que se refiere sería parte de una discusión aún abierta.

- Ministro Sergio A. Valls Hernández. En su opinión la acción era fundada, pues si bien la medida perseguía un fin legítimo, ésta encuadraba en la vigilancia de comunicaciones, toda vez que en un principio, un equipo móvil estaría relacionado a una persona, y la ubicación geográfica de tal equipo sería, sin duda, una forma en que podría obtenerse información del individuo, siendo que el derecho a la intimidad y a la vida privada están protegidos por el artículo 16 constitucional. En su razonamiento el ministro señala que este precepto no sólo resguardaría el contenido de las comunicaciones, sino que protegería en amplio sentido la inviolabilidad de éstas, siendo la ubicación o dirección de donde se emite una comunicación,

[389] Voto Concurrente Ministro Alfredo Gutiérrez Ortiz Mena, Sentencia Expediente Nº 32-2012 pronunciada por la Suprema Corte de Justicia de México.
[390] Ibídem.

un dato de la misma y, por ende, no debería ser de fácil acceso, sino en casos excepcionales y mediante escrutinio judicial. Señala además el Ministro que "[e]s un hecho que una actividad privada de las personas, son las comunicaciones, por lo que, la información relacionada con éstas, como es el lugar en donde se originan, debe estar protegido del acceso arbitrario de terceros, al pertenecer a un espacio privado de éstas".[391] De esta forma el ministro concluye que respecto del artículo 133 Quater del Código Federal de Procedimientos Penales no puede coincidir con la afirmación de que ante el interés público de combatir los delitos, el derecho humano a la intimidad o privacidad de una persona deba ceder y, por ende, la normatividad impugnada sea constitucional, como sostuvo la mayoría de la Suprema Corte.

Luego señala que, respecto de los artículos 40 bis de la Ley Federal de Telecomunicaciones, tampoco coincidía con lo señalado por la mayoría, en cuanto reconoce la validez del artículo que, para garantizar la operatividad del referido artículo 133 Quater, obliga a los concesionarios y permisionarios de servicios de telecomunicaciones a colaborar con las autoridades, es decir, a atender las solicitudes que les hagan los procuradores o servidores públicos autorizados por éstos, para realizar tal ubicación geográfica, pues, insiste que, bajo el orden jurídico constitucional y convencional de México, ello debe ser autorizado vía judicial y no dejarse al arbitrio de las procuradurías.

Por su parte, respecto del artículo 16, fracción I, apartado d, impugnado, si bien comparte que el sentido de la mayoría, al estimar constitucional dicho precepto, no comparte las consideraciones en que la mayoría basó su dicho, pues, señala que si se atendía al contenido del referido artículo 16, fracción I, apartado d, en relación con lo dispuesto en el diverso numeral 14 de la misma Ley Federal de Telecomunicaciones, lo que regulaba "son las bases para la licitación pública para concesiones sobre bandas de frecuencias del espectro para usos determinados, estableciendo las bases para participar en las licitaciones, en el sentido de determinar, que, tratándose de los servicios de telecomunicaciones, deberán incluir "las acciones coordinadas con la autoridad correspondiente, que permitan combatir los delitos de extorsión, amenazas, el secuestro en cualquiera de sus modalidades o algún delito grave o relacionado con la delincuencia organizada". De forma que el hecho de que se comprenda también a "algún delito grave", encuentra sentido, pues, no sólo se está refiriendo a los casos regulados por el diverso 133 Quáter del Código Federal de Procedimientos Penales, sino también a aquellos supuestos de delitos graves, como se advierte de lo dispuesto en los artículos 16 constitucional y 278 Bis y 278 ter, que prevén lo relativo a las intervenciones de comunicaciones".[392]

En conclusión, el ministro consideró inconstitucional la norma del artículo 133 Quater del Código Federal de Procedimientos Penales y el artículo 40 bis de la Ley Federal de Telecomunicaciones, sin embargo, no consideró la norma del artículo 16, fracción I, apartado D de la Ley Federal de Telecomunicaciones.

1.12. Inviolabilidad de Comunicaciones Privadas y Datos Almacenados en Teléfono Celular

[391] Voto Particular Ministro Sergio A. Valls Hernández, Sentencia Expediente Nº 32-2012 pronunciada por la Suprema Corte de Justicia de México.
[392] Ibídem.

a) Amparo en Revisión 495/2012

Sentencia Expediente Nº 495/2012, pronunciada por la Suprema Corte de Justicia de México con fecha 30 de Enero de 2013. La causa tiene como antecedentes la detención del recurrido, por empleados de seguridad de una empresa, quienes le habrían atribuido que en su vehículo tenía quince rollos de alambrón que momentos antes eran transportados por un tren de la empresa y que se le habrían sido arrojados desde éste en movimiento. El personal de seguridad privada entregó al detenido a la policía estatal que llegó al lugar, junto con los objetos personales que portaba el detenido, entre ellos, su teléfono celular. Posteriormente, el Agente del Ministerio Público de la Procuraduría General de Justicia del Estado de Tlaxcala habría realizado la investigación de los hechos previamente señalados y ejerció acción penal en contra del recurrido como probable responsable de la comisión del delito de robo calificado.

Entre los elementos de prueba destacados por el Agente del Ministerio Público para ejercer acción penal se resaltó la fe ministerial del contenido del teléfono celular, que los agentes de seguridad privada le entregaron a la policía estatal el día de la detención. Luego sus antecedentes se enviaron al Juez Segundo de lo Penal del Distrito Judicial de Sánchez Piedras, Tlaxcala, el cual concluido el procedimiento de preinstrucción, resolvió dictar auto de libertad por falta de elementos para procesar con las reservas de ley a favor del ahora recurrido, al estimar que no se encontraba acreditado uno de los elementos del cuerpo del delito de robo, específicamente, la ajenidad, que se le imputaba.

Ante esto, el Ministerio Público interpuso recurso de apelación, el cual fue resuelto por la Sala Penal del Tribunal Superior de Justicia del Estado de Tlaxcala, quien estuvo por revocar el auto de libertad y decretar formal prisión en contra del ahora recurrido como probable responsable de delito de robo calificado. Razón por la cual el detenido interpuso recurso de amparo, el cual le fue concedido, lo que motivo a la empresa X, actual recurrido, a interponer el presente recurso de revisión.

Debido a los objetos de este estudio señalaremos las consideraciones de la Suprema Corte respecto a la vulneración del derecho fundamental a la inviolabilidad de las comunicaciones en relación a los antecedentes de la causa, el cual fue una de las razones para que en un principio fuera concedido el recurso de amparo del ahora recurrido, y para que el presente recurso de revisión fuera rechazado en lo que respecta a la utilización de la información contenida en el teléfono como medio probatorio. En primer lugar la Suprema Corte determina el contenido del derecho fundamental a la inviolabilidad de las comunicaciones privadas, y señala así varios criterios que se han ido sistematizando por este Tribunal, los cuales serían los siguientes:

“a) En cuanto a su objeto, el derecho a la inviolabilidad de las comunicaciones se configura como una garantía formal, esto es, las comunicaciones resultan protegidas con independencia de su contenido.

“b) Lo que se encuentra prohibido por el párrafo decimosegundo del artículo 16 de la Constitución es la intercepción o el conocimiento antijurídico de una comunicación ajena. La violación de este derecho se consuma en el momento en que se escucha, se graba, se almacena, se lee o se registra —sin el consentimiento de los interlocutores—,

una comunicación ajena, con independencia de que, con posterioridad, se difunda el contenido de la conversación interceptada.

“c) El objeto de protección constitucional no hace referencia únicamente al proceso de comunicación, sino también a aquellos datos que identifican la comunicación.

“d) El registro de los números marcados por un usuario de la red telefónica, la identidad de los comunicantes o la duración de la llamada telefónica, llevado a cabo sin las garantías necesarias para la restricción del derecho fundamental al secreto de las comunicaciones, puede provocar su vulneración.

“e) La inviolabilidad de las comunicaciones se extiende también con posterioridad al momento en el que se produce la comunicación. Esto resulta de especial importancia en aquellos casos en los que el mensaje se materializa en un objeto una vez finalizado el proceso comunicativo, ya que existen muchos medios de comunicación que, por su naturaleza, conservan el contenido de las conversaciones.

“f) El párrafo decimosegundo del artículo 16 constitucional no solo proscribe aquellas interceptaciones de comunicaciones en tiempo real —es decir, durante el tiempo en que efectivamente se entabla la conversación—, sino también aquellas injerencias que se realizan con posterioridad en los soportes materiales que almacenan la comunicación.

“g) Nuestra Constitución no limita los medios a través de los cuales se puede producir la comunicación objeto de protección del derecho fundamental en estudio. Esto resulta acorde con la finalidad de la norma, que no es otra que la libertad de las comunicaciones, siendo que ésta puede ser conculcada por cualquier medio o artificio técnico desarrollado a la luz de las nuevas tecnologías.

“h) Del tradicional correo o telégrafo, pasando por el teléfono alámbrico y el teléfono móvil, hemos llegado a las comunicaciones que se producen mediante sistemas de correo electrónico, mensajería sincrónica o instantánea asincrónica, intercambio de archivos en línea y redes sociales. Las posibilidades de intercambio de datos, informaciones y mensajes se han multiplicado por tantos programas y sistemas como la tecnología es capaz de ofrecer y, por lo tanto, también las maneras en que dichos contenidos pueden ser interceptados y conocidos por aquéllos a quienes no se ha autorizado expresamente para ello.

“i) En definitiva, todas las formas existentes de comunicación y aquellas que sean fruto de la evolución tecnológica, deben quedar protegidas por el derecho fundamental a la inviolabilidad de las comunicaciones privadas.

“j) Las pruebas obtenidas, directa o indirectamente violando derechos fundamentales, no surtirán efecto alguno. Esta afirmación afecta tanto a las pruebas obtenidas por los poderes públicos, como a aquéllas obtenidas, por su cuenta y riesgo, por un particular.

“k) La ineficacia de la prueba no sólo afecta a las pruebas obtenidas directamente en el acto constitutivo de la violación de un derecho fundamental, sino también a las adquiridas a partir o a resultas de aquéllas, aunque en su consecución se hayan cumplido todos los requisitos constitucionales.

“l) Todo elemento probatorio que pretenda deducirse de la violación de derechos fundamentales es de imposible valoración en nuestro ordenamiento”.

Luego la Suprema Corte señala que la jurisprudencia de la corte ha definido los alcances del derecho fundamental a la inviolabilidad de las comunicaciones en relación a la información almacenada en un teléfono celular asegurado a una persona detenida por la posible comisión de un delito, motivo por el cual se utilizó dicha jurisprudencia para resolver el presente caso. En un primer momento se preocupa de definir lo que es un teléfono celular, y señala que es “un dispositivo móvil, pequeño, con capacidades de procesamiento (cada vez más parecidos a una PC), móviles y portátiles, con conexión permanente o intermitente a una red (internet), con memoria limitada, diseñados para llevar a cabo funciones generales, como de correo electrónico, hablar por teléfono, mensajes, manejo de imágenes, música y video”. .

A continuación, señala que el teléfono celular está al alcance de cualquier persona, sin importar su estatus socioeconómico, dados los bajos costos en que se puede adquirir un equipo en el mercado, destaca que hoy estos teléfonos permiten entre sus funciones, además de la comunicación verbal, las de servicios de Internet, correo electrónico, mensajes, manejo de imágenes, música y video. Por lo que cualquiera que cuente con un celular, tiene el derecho de guardar información en la memoria del aparato, por lo que, acorde a los alcances de su jurisprudencia esa información se clasificaría como privada, es decir, que pertenece exclusivamente a la intimidad de la persona.

Por otro lado, la Suprema Corte señaló que no es ajena al mal uso de los teléfonos celulares, pues su experiencia revela las prácticas delictivas que se originan con su utilización, como es el caso de extorsiones, chantajes, secuestros, etc. Hecho este alcance, señala que el legislador en el referido artículo 16 constitucional, impuso como límite para la inviolabilidad de las comunicaciones privadas, su intervención previa autorización exclusiva por parte de la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente. Así, la Corte señala que “dicho precepto no hace distinción alguna tratándose de las personas sujetas a investigación, es decir, la norma se concibió como una medida proteccionista de tutela general, por lo que aplicando el principio de derecho que afirma “donde la ley no distingue, no hay por qué distinguir”, no existe argumento válido para restringir los derechos fundamentales a cualquier sujeto, por el sólo hecho de estar detenida”.

En este sentido la Suprema Corte señala que, si la autoridad encargada de la investigación de un delito, advirtiera que cualquier detenido tiene en su poder un teléfono celular y el mismo pudo haber sido utilizado como medio para fines antisociales, está constitucionalmente facultada para solicitar a la autoridad judicial la intervención de las comunicaciones privadas almacenadas en ese dispositivo, en los términos descritos en el citado artículo 16. Así, considera que la información que se extraiga, vía autorización judicial, de los archivos electrónicos, ya sea en forma de texto, audio, imagen o video, relacionada estrictamente con la posible comisión de un hecho delictivo, podría ser incorporada al procedimiento penal y, por ende, sería lícita. Pese a esto, la Suprema señala que si esa actividad de búsqueda y obtención de información se hubiera

realizado sin autorización judicial, cualquier prueba que se hubiera extraído o que derive de ésta, debería ser considerada como ilícita al ser incorporada incumpliendo con la normativa constitucional.

La Suprema Corte señala que en conformidad al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos se requeriría para intervenir una comunicación privada, autorización exclusiva por parte de la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, por lo que todas las formas existentes de comunicación y aquellas que sean fruto de la evolución tecnológica, deben quedar protegidas por el derecho fundamental a su inviolabilidad; tal como sucede con el teléfono móvil en el que se guarda información que ha sido clasificada como privada, de ahí que el ámbito de protección se extiende a los datos almacenados en ese dispositivo, ya sea en forma de texto, audio, imagen o video.

De esta forma el Tribunal Supremo de México al analizar la diligencia consistente en la fe ministerial de contenido de teléfono celular, señaló que del contenido de la diligencia, la inspección no sólo había recaído en la existencia del teléfono celular, sino que se accedió a diversos mensajes de texto almacenados el teléfono que se decía que pertenecían o le fue encontrado al recurrido durante la detención ciudadana realizada por los agentes de seguridad privada. Señaló además que de los antecedentes no se advirtió que dicha intervención haya estado precedida por el consentimiento del detenido o por la orden de un juez federal que autorizara a conocer dicha comunicación privada, razón por la cual determinó que el Juez de Distrito había acertadamente considerado que dicha diligencia debía excluirse del caudal probatorio por haber sido obtenida vulnerando la garantía de inviolabilidad de las comunicaciones privadas por lo que su valoración habría sido imposible.

Uruguay

1.13. Habeas Data y Cámaras de Vigilancia

a) Bega Bonilla, Ana y otros c/ Copropiedad Edificio Poseidón

Sentencia Nº SEF-0007-000025/2014, pronunciada por el Tribunal de Apelaciones en lo Civil de Tercer Turno con fecha 25 de febrero de 2014. La causa se refiere al recurso de apelación presentado en contra de la sentencia que rechaza la demanda presentada por doña Ana. Los fundamentos que tuvo para interponer la demanda eran los siguientes: i) La Asamblea del Edificio Poseidón había violado sus derechos fundamentales al decidir instalar cámaras de video vigilancia, señaló además que estaría amparada por la ley de protección de datos por las imágenes y videos que se grabaran respecto a ella; ii) El acuerdo al que se habría llegado por parte de la Asamblea de Copropietarios no podía significar una renuncia a sus derechos fundamentales; iii) señala además que no hubo consentimiento informado previo y libre, ya que la Asamblea no era la titular del derecho, y estos son irrenunciables; iv) pidió la supresión de los datos por la prohibición de tratamiento. En esta instancia, solicitó que se revocará la sentencia recurrida, ordenando el cese de la recolección ilegítima de datos personales mediante el retiro de

las cámaras de video vigilancia de la Copropiedad, y la supresión de todos los datos almacenados en bases sin consentimiento de los accionantes.

El Tribunal primero hace referencia a que las pretensiones de doña Ana se encuentran en el marco de su Ley de Habeas Data, luego analizó su petición de eliminación del sistema de video vigilancia. Respecto a esto el Tribunal señaló que, en primer lugar, el sistema de video vigilancia debía entenderse como parte del concepto de registro de la Ley de Habeas Data. Luego señala que, de la lectura de la Ley de Habeas Data, no emergería como pretensión propia de la acción establecida en los artículos 37 y 38 de la misma, la supresión o declaración de ilegalidad de un registro de datos, de tal forma de prohibirlo o eliminarlo totalmente. Ya que de estas normas solo se podría solicitar la modificación de la base de datos, es decir, la rectificación, inclusión, supresión o lo que entienda corresponder, pero siempre en relación a los datos, no a la procedencia o improcedencia de la existencia del registro.

Señala además que esta norma debe ser interpretada de forma estricta, no pudiendo aplicarse la analogía, razón por la cual el mismo queda reducido a las específicas situaciones emergentes de sus artículos 37 y 38. Luego de señalado lo anterior, el Tribunal comparte la opinión del tribunal de primera instancia en cuanto no cabía hacer lugar a la petición relativa a la supresión de un registro que fue establecido por una Asamblea de Copropietarios legitima, por lo que el Registro no podría entenderse como ilegal.

Luego el Tribunal analiza la segunda pretensión de la recurrente, y señala que al ser la video vigilancia y el registro de imágenes decidido por la Asamblea de Copropietarios del Edificio, en base a un acuerdo transaccional del que fue parte la demandante, habría existido por ello consentimiento informado. El Tribunal señala a su vez que la decisión de la Asamblea sobre el control y vigilancia de los espacios comunes de uso común, es un tema propio de la Copropiedad, por lo que podría ser regulado por ésta.

El Tribunal de Apelaciones, considera que los acuerdos de la Asamblea en el contexto de regular normas de vigilancia y control de los espacios comunes es legítimo siempre que no se vulneren derechos fundamentales, siendo justamente eso lo que la recurrente alega en la causa. Es así como el Tribunal analiza el derecho a la intimidad y señala que, en este caso, “el derecho a la intimidad del que hacen caudal los accionantes no refiere al ámbito de su espacio inviolable –el hogar-, sino a uno compartido con otros, sus copropietarios. Y allí ha de privar la voluntad general por sobre la particular, se insiste que si no se viola ni se limita ilícitamente un derecho humano”.

Agrega el Tribunal, que incluso los copropietarios sabrían donde se encontrarían los lugares donde se filma porque existirían carteles que avisan, razón por la cual afirma que esto significa que los copropietarios aceptarían que los registraran al exponerse en esos lugares.

Por lo tanto, concluye que no habría ilicitud en la registración por video cámara, por ser resultado de una decisión tomada en el ámbito contractual, con renuncia a un derecho dentro de los límites aceptados.

Finalmente, el Tribunal de Apelaciones se refiere a lo aludido por la recurrente respecto al destino de los datos, se estableció que los datos se eliminaban cada 15 días, obligación que no se acreditó incumplida; que no se realizaban respaldos en lugares diferentes al que se encontraban los equipos por lo que la preservación de la seguridad de las filmaciones y la destrucción de los datos, permitían que coexistieran el derecho a la intimidad de los ocupantes del edificio y la seguridad de los bienes que reclamaba la Asamblea.

De esta forma el Tribunal de Apelaciones confirma la sentencia apelada y rechaza las pretensiones de la recurrente.

Capítulo IV
Condiciones de Acceso a Internet

1. La penetración de internet en Latinoamérica

El uso de internet en los países de Latinoamérica ha visto un crecimiento sostenido en el uso de internet. La Tabla 1 muestra los niveles de penetración en los países antes revisados respecto de sus condiciones de acceso en relación con la población con acceso a internet. Chile, Argentina y Uruguay tienen en tal sentido las tasas más altas de acceso.

En promedio, sobre el 41 % de la población en Latinoamérica tiene acceso a internet, sea en su trabajo, en dispositivos móviles, en su hogar, o mediante servicios privados o públicos como infocentros y bibliotecas. Si bien no alcanza a cubrir a la mitad de la población, y las tasas de crecimiento anual son relativamente estables, el acceso por la mayoría de la población como promedio general (superado hoy por apenas seis países) debiera ser alcanzado entre 2015 y 2016.

Tabla 1: Porcentaje de individuos que usan internet

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Argentina	7,04	9,78	10,88	11,91	16,04	17,72	20,93	25,95	28,11	34,00	45,00	51,00	55,80	59,90
Bolivia	1,44	2,12	3,12	3,51	4,44	5,23	6,20	10,50	12,50	16,80	22,40	30,00	35,50	39,50
Brasil	2,87	4,53	9,15	13,21	19,07	21,02	28,18	30,88	33,83	39,22	40,65	45,69	48,56	51,60
Chile	16,60	19,10	22,10	25,47	28,18	31,18	34,50	35,90	37,30	41,56	45,00	52,25	61,42	66,50
Colombia	2,21	2,85	4,60	7,39	9,12	11,01	15,34	21,80	25,60	30,00	36,50	40,35	48,98	51,70
Costa Rica	5,80	9,56	19,89	20,33	20,79	22,07	25,10	28,40	32,29	34,33	36,50	39,21	47,50	45,96
República Dominicana	3,70	4,43	6,82	7,90	8,87	11,48	14,84	17,66	20,82	27,72	31,40	38,00	41,20	45,90
Ecuador	1,46	2,67	4,26	4,46	4,83	5,99	7,20	10,80	18,80	24,60	29,03	31,37	35,14	40,35
El Salvador	1,18	1,50	1,90	2,50	3,20	4,20	5,50	6,11	10,08	12,11	15,90	18,90	20,32	23,11
Guatemala	0,71	1,74	3,39	4,55	5,10	5,70	6,50	7,30	8,30	9,30	10,50	12,30	16,00	19,70
Honduras	1,20	1,42	2,60	4,80	5,60	6,50	7,80	9,40	9,60	9,80	11,09	15,90	18,12	17,80
México	5,08	7,04	11,90	12,90	14,10	17,21	19,52	20,81	21,71	26,34	31,05	37,18	39,75	43,46
Nicaragua	0,98	1,45	1,71	1,88	2,32	2,57	2,81	3,90	5,30	7,30	10,00	10,60	13,50	15,50

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Panamá	6,55	7,27	8,52	9,99	11,14	11,48	17,35	22,29	33,82	39,08	40,10	42,70	40,30	42,90
Paraguay	0,75	1,10	1,79	2,11	3,45	7,91	7,96	11,21	14,27	18,90	19,80	24,76	29,34	36,90
Perú	3,08	7,58	8,97	11,60	14,10	17,10	20,70	25,20	30,57	31,40	34,77	36,01	38,20	39,20
Uruguay	10,54	11,12	11,42	15,94	17,06	20,09	29,40	34,00	39,30	41,80	46,40	51,40	54,45	58,10
Venezuela	3,36	4,64	4,91	7,50	8,40	12,55	15,22	20,83	25,88	32,70	37,37	40,22	49,05	54,90
PROMEDIO	**4,14**	**5,55**	**7,66**	**9,33**	**10,88**	**12,83**	**15,84**	**19,05**	**22,67**	**26,50**	**30,19**	**34,32**	**38,51**	**41,83**

Fuente: UIT

2. El acceso de banda ancha

Si bien los niveles de acceso son similares a los que UIT estima como promedio mundial, lo cierto es que hay realidades profundamente disímiles en la región. Diferencias que se profundizan en el análisis de los mecanismos de acceso, considerando que no todos los lugares físicos tienen conectividad disponible. En tal sentido, constituye una diferencia sustantiva el nivel de acceso a internet de alta velocidad, que hoy en día aparece como necesaria para la utilización de servicios de internet que involucran audio, video y despliegue de contenidos gráficos. La Tabla 2 muestra el número de suscriptores de internet de banda ancha, mediante una línea digital, cable u otra tecnología que permite descargas de a lo menos 256 kilobits por segundo (Kbps). También en esto el aumento es significativo; manteniéndose como promedio regional por sobre la media mundial.

Tabla 2: Porcentaje de suscriptores de internet de banda ancha

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Argentina		0,25	0,39	0,68	1,42	2,40	4,06	6,61	7,85	8,77	9,96	11,19	12,53	13,86
Bolivia		0,00	0,04	0,06	0,09	0,14	0,18	0,35	0,81	0,96	0,94	0,64	1,05	1,33
Brasil	0,06	0,19	0,41	0,53	1,72	1,74	2,53	4,01	5,05	5,84	6,80	8,56	9,15	10,08
Chile	0,05	0,43	1,19	2,20	2,96	4,34	6,18	7,73	8,48	9,68	10,37	11,54	12,33	12,25
Colombia	0,02	0,03	0,08	0,15	0,30	0,74	1,43	2,71	3,90	4,55	5,59	7,00	8,16	9,29
Costa Rica		0,00	0,22	0,36	0,66	1,04	1,89	2,13	2,37	3,91	8,49	8,73	9,32	9,72

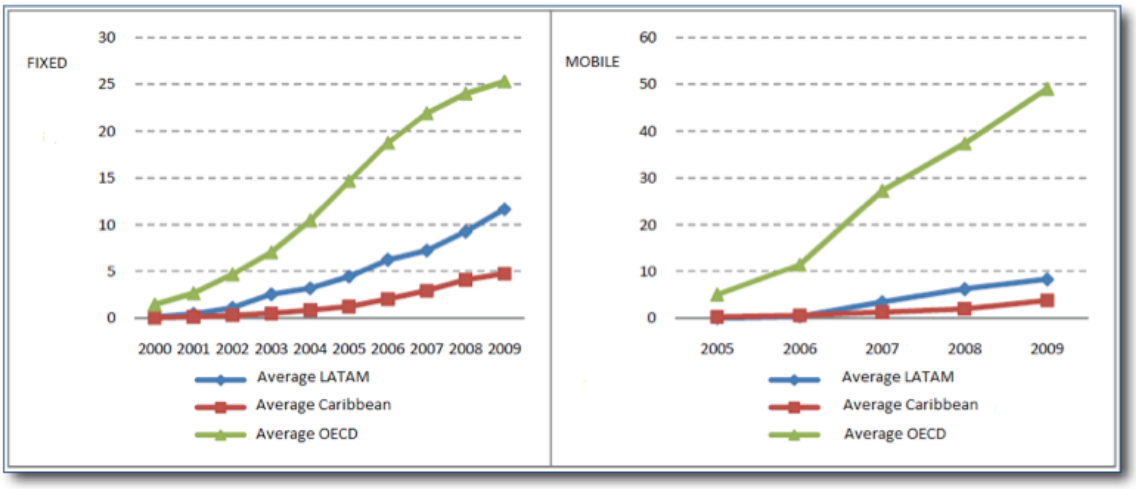
	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
República Dominicana		0,00	0,00	0,17	0,40	0,65	1,09	1,60	2,32	2,98	3,69	3,98	4,35	4,66
Ecuador		0,02	0,05	0,05	0,09	0,19	0,33	0,70	1,07	1,63	1,32	4,06	5,28	6,34
El Salvador		0,00	0,00	0,33	0,48	0,70	1,01	1,47	2,01	2,42	2,82	3,29	3,84	4,45
Guatemala		0,00	0,00	0,00	0,00	0,21	0,30	0,43	0,69	1,12	1,81		1,81	1,80
Honduras		0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00		0,01	0,74	0,77	0,84
México	0,01	0,05	0,22	0,40	0,97	1,74	2,69	3,94	6,46	7,97	9,42	9,94	10,52	11,14
Nicaragua	0,01	0,03	0,04	0,08	0,09	0,19	0,34	0,49	0,76	1,37	1,26	1,44	1,69	2,17
Panamá		0,25	0,38	0,46	0,51	0,52	3,29	4,30	5,52	6,48	7,02	7,56	7,75	7,71
Paraguay	0,00	0,01	0,01	0,01	0,05	0,09	0,10	0,14	0,21	0,25	0,44	0,94	1,19	1,58
Perú	0,00		0,14	0,35	0,83	1,27	1,73	2,01	2,53	2,80	3,12	4,02	4,74	5,18
Uruguay		0,00	0,00	0,00	0,81	1,46	2,79	4,55	6,80	8,95	10,90	13,45	16,59	21,13
Venezuela	0,02	0,13	0,29	0,44	0,78	1,32	1,96	3,09	3,88	4,70	5,60	6,04	6,70	7,31
PROMEDIO	**0,02**	**0,08**	**0,19**	**0,35**	**0,68**	**1,04**	**1,77**	**2,57**	**3,37**	**4,38**	**4,97**	**6,07**	**6,54**	**7,27**

Fuente: UIT

3. El acceso a internet móvil

Uno de los puntos más significativos del crecimiento de internet en Latinoamérica está dado por la prescindencia de la infraestructura para la conectividad fija, con un crecimiento marcado en la suscripción a internet móvil, de forma mucho más pronunciada que las conexiones de internet de banda ancha fija, como se muestra en el Gráfico I.

Gráfico 1: Porcentaje de conexiones a internet fija y móvil



Fuente: BID[393], datos de UIT.

Respecto de los planes de banda ancha móvil, la UIT incluyó en su Medición de la Sociedad de la Información 2013 el estudio de planes de prepago y postpago de 500 megabytes (MB) para *smartphones* y 1 gigabyte (GB) para computadoras. En los países desarrollados, los planes representan entre 1% y 2% del PIB per cápita, mientras en los países en desarrollo, el precio está entre 11% y 25% del PIB per cápita.

Tabla 3: planes de banda ancha móvil y precio

Ranking	País	Como % del PIB p.c.	USD	PPA$	PIB per cápita (USD)
85	Argentina	4,5	36,5	58,7	9740
124	Bolivia	14,4	24,5	51,9	2040
55	Brasil	2	17,8	16,6	10720
67	Chile	2,5	25,8	31,1	12280
78	Colombia	3,7	18,7	26,7	6110
66	Costa Rica	2,5	15,8	22,3	7660
100	Ecuador	5,8	20,2	37,4	4140
111	Guatemala	8,6	20,6	32,1	2870
62	México	2,3	17,6	26,7	9240
61	Panamá	2,1	14	25,5	7910
112	Paraguay	8,8	21,8	32,6	2970
80	Perú	3,9	18	30,9	5500
95	Rep. Dominicana	5,3	23,3	41,6	5240
37	Uruguay	1,5	14,9	16,3	11860
39	Venezuela	1,5	15,4	18,3	11920

Fuente: UIT

[393] Zaballos & López-Rivas, *Socioeconomic Impact of Broadband in Latin American and Caribbean Countries*. BID, 2011.

4. La velocidad en el acceso a internet

Una de las más relevantes características del acceso a internet en Latinoamérica está constituida por las diferencias en las velocidades de conexión. En tal sentido, si bien es razonable entender que las conexiones fijas de banda ancha constituyen probablemente la más segura forma de conexión rápida a internet, la geografía de los países no permite en todos los casos que exista el mismo nivel de acceso a conexiones fijas. De este modo, es posible verificar diferencias sustantivas de velocidades entre los países latinoamericanos; pero del mismo modo, es posible notar que las diferencias dentro de cada país entre la velocidad de conexión fija y la de conexión móvil dan cuenta de los mecanismos de uso dentro de cada uno de ellos. Los datos del Ookla Net Index[394] demuestran esas diferencias en las tasas de descarga en megabits por segundo (Mbps) en cada país, que frente al promedio mundial son más bajas en toda Latinoamérica, con excepción de Uruguay.

Tabla 4: Velocidad de conexión según descarga en Mbps

	fija	móvil
Argentina	5.54	1.83
Bolivia	2.33	2.35
Brasil	10,81	5,01
Chile	15,39	6,27
Colombia	6,04	8,33
Costa Rica	4,22	1,78
República Dominicana	4,52	5,38
Ecuador	7,13	4,80
El Salvador	3,56	2,22
Guatemala	3,75	2,44
Honduras	4,18	1,69
México	12,59	6,95
Nicaragua	4,32	2,79
Panamá	5,89	2,07
Paraguay	2,91	2,33
Peru	5,13	6,05
Uruguay	21,08	18,49
Venezuela	2,16	2,94
PROMEDIO	7,11	4,97

Fuente: Ookla Net Index

[394] Ookla Net Index, http://www.netindex.com/download/allcountries/

Conclusiones

Lo primero que cabe destacar, luego de analizar la normativa y jurisprudencia emanada de países latinoamericanos en materia de privacidad, es que el tema viene siendo fuertemente relevado desde, al menos, las últimas dos décadas.

Así, y con la finalidad de salvaguardar este derecho, las Constituciones han ido consignando derechos fundamentales en torno a la privacidad, ya sea resguardándola como tal o en alguna de sus facetas, entre las que encontramos la vida privada, intimidad, inviolabilidad del hogar y las comunicaciones, principalmente.

Otra vía que han utilizado las Cartas Fundamentales para resguardar la privacidad, no excluyente de la indicada anteriormente, consiste en la incorporación dentro del ordenamiento jurídico de la acción de habeas data, permitiendo a los ciudadanos, a través de ella, acceder a los datos que sobre ellos detenten organismos públicos o privados. Incluso, en muchos casos, encontramos que en la misma Constitución también se indica el procedimiento para ejercer este derecho a acceder a los datos que trata el organismo requerido (e.g. Bolivia, Panamá y Perú), e incluso al organismo encargado de ejercer dicha acción (Paraguay y Uruguay).

Luego, pudimos apreciar cómo el grueso de los países latinoamericanos analizados ha desarrollado las garantías fundamentales que sus Constituciones consignan en leyes de aplicación general, y también en normativa sectorial de carácter más específico.

En consecuencia, el proceso normativo deja en evidencia que la privacidad es una materia que cruza las más variadas áreas del derecho, y que, con el transcurso del tiempo, ha resultado insoslayable contemplarla entre los elementos a considerar a la hora de emitir nuevas regulaciones. Esto se vuelve aún más crucial en la actualidad, tras las revelaciones del último año que han mostrado que existe una masiva vigilancia efectuada a través de las redes, tanto por parte de los gobiernos como de privados.

Por otra parte, analizada la jurisprudencia reciente, es posible constatar que numerosas sentencias hacen explícita referencia a los tratados internacionales vigentes y aplicables en los países respectivos, lo que evidencia la importancia de los instrumentos internacionales en materia de privacidad, y cómo se hacen esfuerzos evidentes por armonizar su interpretación con la normativa nacional en los fallos de las altas cortes de justicia.

También destacan aquellos fallos en que se ha citado incluso jurisprudencia extranjera, o internacional (proveniente de la Corte Interamericana), en un esfuerzo por dar una acabada y correcta interpretación de la extensión de este derecho a la privacidad.

En cuanto a la injerencia que la tecnología tiene en estas materias, tanto la jurisprudencia reciente como los proyectos de ley actualmente en discusión, dan cuenta del modo en que ella afecta a la vida privada, la intimidad, e incluso el honor, debiendo hacerse cargo de las dificultades propias de regular en un área en permanente evolución, y bajo el riesgo de resultar anacrónica o desfasada. Además se trata de un área no ajena a la polémica contingente, tal como nos recuerda el caso de las filtraciones por parte de Edward Snowden de los programas de vigilancia masiva llevados a cabo por el gobierno de los Estados Unidos, información que provocó molestia en varios gobiernos del mundo, y puso en evidencia la fragilidad actual del estado del arte en materia de derecho a la privacidad.

En este punto destacan los fallos en contra de los buscadores Google y Yahoo, que se muestran como los principales sitios en que, actualmente, se indexa información. Si bien ellos, por sí mismos, no realizan la actividad que vulnera la privacidad, los resultados que arrojan las búsquedas en sus sitios sí se han estimado lesivas, a tal punto que se ha ordenado eliminar dicha información. Lo destacable de estos fallos, en general, radica en la importancia que se asigna a la privacidad como bien jurídico digno de protección, ya que bien podrían discutirse los alcances de una decisión judicial de esta naturaleza cuando se encuentra involucrado Internet, en el que una vez que ha ingresado un nuevo contenido, resulta muy difícil de eliminar de manera definitiva, a diferencia de lo que sucede en el entorno análogo. Esta es un escenario muy distinto al que estábamos usualmente acostumbrados a enfrentar en el llamado "mundo real", y obliga a todo un replanteamiento y nuevos análisis para captar cuán afectada puede verse la privacidad en la actualidad.

Con todo, este tipo de jurisprudencia plantea desafíos adicionales: cómo evitar la censura por parte de privados –asunto que resulta, a todas luces, inaceptable en una sociedad democrática-, fundada en la asignación de responsabilidad basada en su calidad de intermediarios de contenidos. Claramente el derecho a la privacidad requiere tomar en cuenta tanto los intereses públicos como privados que se hallan en juego, y es en esta ponderación en que resulta clave el rol que han de tomar los tribunales de justicia en la materia.

Finalmente, sólo resta señalar que, como es lógico, se debe esperar un alza en la judicialización de los conflictos que involucren lesión a la privacidad, conforme continúe el indetenible avance tecnológico. En este sentido resulta fundamental que las legislaciones nacionales se encuentren bien preparadas para enfrentar esta nueva demanda social, y que los cauces de la justicia internacional se encuentren también llanos para hacerse cargo de esta creciente necesidad, teniendo siempre presente la enorme importancia que reviste la protección de la privacidad para la democracia y las libertades, tanto de expresión como de asociación.

Fundación Getulio Vargas

Liberdade de Expressão, Privacidade, Neutralidade de Rede e Acesso à Cultura no Marco Civil da Internet Brasileira[395]

A Lei 12.965/2014 (Marco Civil da Internet) foi aprovada no dia 22 de abril de 2014 no Senado Federal e sancionada imediatamente pela Presidenta Dilma Rousseff durante o NetMundial - Encontro Global Multissetorial sobre o Futuro da Governança de Internet - realizado em São Paulo nos dias 23 e 24 do mesmo mês.

A legislação traz notável avanço em assuntos fundamentais para o desenvolvimento nacional, como a inclusão digital (art. 4º) a afirmação de importantes diretrizes para a atuação do Estado (arts. 24 a 28). Houve forte disputa torno de questões mais polêmicas, como neutralidade de rede, privacidade e liberdade de expressão. Nelas pode-se notar que houve avanços e retrocessos.

Mesmo com a aprovação da Lei, as discussões sobre estes temas não devem se encerrar. Muitas questões precisam ser detalhadas em regulação posterior e serão alvo de interpretação pelo judiciário. A guarda compulsória de dados por parte dos provedores, por exemplo, deverá ser regulamentada pela Presidência da República, gerando debates sobre privacidade e segurança. Da mesma forma, é possível antever grande disputa pela regulamentação da neutralidade de rede. A jurisprudência definirá os limites e contornos da liberdade de expressão a partir das novas regras para remoção de conteúdo em casos de calúnia, injúria e difamação e tratará da implementação de aspectos relativos ao acesso à cultura.

1) O DIREITO À PRIVACIDADE

O direito à privacidade está previsto na Constituição Federal brasileira, que o colocou no rol dos direitos fundamentais. Esses direitos fazem parte das cláusulas pétreas, que não podem ser alteradas pelo poder constituinte derivado. Em seu art. 5º, X, a Constituição determina que a intimidade e a vida privada são invioláveis. Logo em seguida, no inciso XII, diz ser inviolável o sigilo de correspondência, dados e comunicações telefônicas e telegráficas. No caso das comunicações por telefone, há uma ressalva para os casos em que houver ordem judicial, para fins de investigação criminal.

[395] Documento elaborado por Luiz Moncau, Pedro Augusto e Marilia Maciel, pesquisadores do Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getulio Vargas do Rio de Janeiro (www.direitorio.fgv.br/cts).

A regulação da privacidade se dá de maneira esparsa na legislação brasileira. Entre as leis que tangenciam a proteção da privacidade, estão o Código de Defesa do Consumidor (Lei 8.078/90[396], que traz regras em seus artigos 43 e 44 sobre a constituição de bancos de dados sobre os consumidores), a Lei de Sigilo Financeiro (Lei Complementar nº 105/2001[397]), a Lei de Interceptação Telefônica (Lei nº 9.296/1996[398]), o Código Civil (Lei 10.406/2002[399], que em seu artigo 21 afirma a inviolabilidade da vida privada) e a Lei de Acesso à Informação (Lei 12.527/2011[400]), entre outras. Entretanto, não há uma lei específica sobre o tema.

Tendo em vista a existência dessa lacuna, o legislador incluiu no Marco Civil o direito à privacidade na Internet como uma das suas principais bases. A privacidade e a proteção dos dados pessoais estão presentes no rol de princípios elencados art. 3º. Os direitos decorrentes desses princípios gerais encontram-se detalhados no art art 7º, transcrito abaixo. Esse artigo sofreu modificações[401] com o intuito de reforçar o direito à privacidade após as revelações de Edward Snowden sobre o monitoramento em massa das comunicações pela Agência Nacional de Segurança (NSA) dos Estados Unidos e seus parceiros. O poder Executivo colocou o Marco Civil em regime de urgência constitucional para a votação no Congresso Nacional e passou a defender a célere aprovação do texto como uma forma de proteger a privacidade dos cidadãos brasileiros.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
>
> (...)
>
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem

[396] Acessível em http://www.planalto.gov.br/ccivil_03/leis/l8078.htm

[397] Acessível em http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm

[398] Acessível em http://www.planalto.gov.br/ccivil_03/leis/l9296.htm

[399] Acessível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm

[400] Acessível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

[401] Essas alterações foram feitas no texto substitutivo V, de 5/11/2013. Uma tabela comparativa das diferentes versões do projeto de lei pode ser acessada em http://www.ufrgs.br/cegov/files/gtgov_marcocivilaprovado.pdf

como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

(...)

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Apesar de ter havido a inserção de dispositivos que reforçavam a privacidade, parte das modificações ia ao encontro de pleitos dos órgãos de investigação. Isso voltou a evidenciar a tensão entre privacidade e segurança, que esteve presente durante todo o processo de discussão do Marco Civil.

Uma das propostas de modificação - que não foi aprovada no texto final da lei - determinava que empresas de Internet que armazenassem informação de cidadão brasileiros deveriam, obrigatoriamente, manter esses dados em território nacional, criando assim data-centers locais. A proposta foi amplamente rejeitada por representantes da sociedade civil, engenheiros, legisladores e, evidentemente, pelas próprias empresas que seriam afetadas. A pressão negativa exercida por esses agentes fez com que o governo brasileiro abandonasse esse dispositivo.

No entanto, a tensão se manteve no que tange à guarda de dados para fins de investigação. Houve um importante debate entre orgãos da sociedade civil e autoridades com poder investigatório (notadamente a Polícia Federal brasileira), que defenderam que a guarda dos

dados por períodos mais longos (de até 5 anos para os registros de conexão) seria essencial para a persecução criminal.

O texto final do Marco Civil tornou obrigatório o armazenamento de registros de conexão[402] pelo prazo de um ano por parte dos provedores de serviços de conexão. Além disso, acrescentou-se a obrigação de armazenamento dos registros de acesso a aplicações de Internet[403] pelo prazo de seis meses, por parte dos provedores desses serviços.

A medida foi mal recebida por entidades de defesa do consumidor, instituições acadêmicas e outros membros da sociedade civil, que entenderam ser desproporcional a guarda compulsória e generalizada dos dados de todos os cidadãos, afetando negativamente o direito à privacidade dos usuários. A seção II do Marco Civil, intitulada "Da Proteção aos Registros, Dados Pessoais e Comunicações Privadas" trata das condicões gerais de guarda e requerimento dos registros de conexão e do registro de acesso a aplicações. De modo a impedir qualquer abuso e violação à privacidade dos usuários, os registros de conexão e acesso só poderão ser fornecidos às autoridades mediante ordem judicial. Uma regulamentação mais pormenorizada, por meio de decreto, sera necessária.

Apesar dos avanços trazidos pelo Marco Civil em alguns aspectos relacionados à privacidade, o Brasil ainda carece de uma lei específica para a proteção de dados pessoais, que regule como os dados dos cidadãos podem ser tratados e como devem ser protegidos em diferentes contextos.

Com a crescente capacidade de processamento e tratamento de dados, a aprovação de leis que definam um regime de proteção dos dados pessoais é imprescindível. O Brasil já deu os primeiros passos nesse sentido. Pouco mais de um ano após o fim do processo de consulta pública para a criação do Marco Civil, o Ministério da Justiça iniciou um processo semelhante para criar o anteprojeto de lei (APL) para a Proteção dos Dados Pessoais. Entre os dias 30 de novembro de 2010 e 30 de abril de 2011, o texto apresentado recebeu cerca de 800 contribuições de vários membros da sociedade. Entretanto, o APL não foi encaminhado para o Congresso Nacional, encontrando-se sob revisão pelo Poder Executivo Federal. Além disso, havia a avaliação por parte de membros do governo e do parlamento de que submeter este anteprojeto à apreciação do Congresso Nacional simultaneamente com o Marco Civil - que propõe normas de caráter mais geral para a privacidade - atrapalharia o andamento dos dois projetos. Entretanto,

[402] Art 5º, VI: registro de conexão: conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

[403] Art. 5º, VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

mesmo após a aprovação do Marco Civil, não existem perspectivas claras sobre os próximos passos dessa importante discussão.

2) LIBERDADE DE EXPRESSÃO

A liberdade de expressão é um direito humano essencial não apenas para o desenvolvimento individual, mas também para o funcionamento coletivo da sociedade. Por este motivo, muitas vezes associada à liberdade de imprensa, a livre expressão é considerada um dos pilares das sociedades democráticas, tendo papel fundamental para que os cidadãos possam receber informações de origens e conteúdos diversos, formando adequadamente suas opiniões sobre os assuntos de interesse social.

O fundamento jurídico da proteção à livre expressão no Brasil está na Constituição Federal, que em seu artigo 5°, incisos IV, V e IX estabelece que: IV - é livre a manifestação do pensamento, sendo vedado o anonimato; V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; e IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença.

Além da Constituição, o Brasil possui um grande volume de regras que afetam o direito à livre expressão, como a Lei de Acesso à Informação (Lei 12.527/2011[404]) , o Código Civil (Lei 10.406/2002[405], especialmente no artigo 20, que se refere ao direito à imagem dos cidadãos[406]), a Lei Eleitoral (Lei 9.504/97[407]), o Código Penal (Decreto-Lei 2.848/40[408], que define os crimes de calúnia, injúria e difamação), a Lei de Direitos Autorais (Lei 9.610/98[409]) e a Lei de Propriedade Industrial (Lei 9.279/96[410], especialmente no que diz respeito ao uso de marcas).

---

[404] Acessível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

[405] Acessível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm

[406] "Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais."

[407] A Lei Eleitoral traz regras sobre a propaganda eleitoral e direito de resposta em período eleitoral, tendo previsões tanto para mídia tradicional quanto para a Internet. Acessível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm

[408] Acessível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm

[409] Acessível em: http://www.planalto.gov.br/ccivil_03/leis/l9610.htm

[410] Acessível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm

O debate sobre liberdade de expressão, entretanto, muitas vezes encontra-se revestido de aspectos técnicos e permeado por normas e legislações de difícil compreensão pelo cidadão não especializado. É seguro, nesse sentido, afirmar que as regras referentes aos serviços de telecomunicações (como as emitidas pela Agência Nacional de Telecomunicações - ANATEL[411]) e radiodifusão são indissociáveis do direito à liberdade de expressão, e acabam por delimitar os contornos e amplitude deste direito.

O Brasil teve recentes modificações com impacto direto sobre o direito à livre expressão com a aprovação do Marco Civil da Internet (Lei 12.965/2014).

O direito à livre expressão é mencionado expressamente em vários trechos do texto do Marco Civil da Internet. Em seus artigos iniciais, a lei afirma que a liberdade de expressão é um fundamento (Art. 2°) e um princípio (Art. 3°, I) para a disciplina do uso da internet no Brasil. No artigo 8°, a lei estabelece que "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet." Estes dispositivos, entretanto, apenas reafirmam o direito à livre expressão como um princípio norteador, servindo para assegurar uma interpretação correta da Lei, sem contudo especificar em detalhes a forma como este direito se materializará em casos concretos.

Entretanto, o texto avança neste detalhamento em outros pontos, proibindo a desconexão do usuário (salvo por falta de pagamento), definindo responsabilidade dos intermediários pelo conteúdo produzido pelos seus usuários e ao tratar do que ficou conhecido como "pornografia de vingança" (*revenge porn*). Estes pontos serão brevemente desenvolvidos abaixo. No item 4, outro ponto crucial para a liberdade de expressão será abordado: a neutralidade de rede.

Proibição da desconexão do usuário

O artigo 7°, inciso IV, o Marco Civil assegura aos usuários o direito de "não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização". Para compreender a importância desse dispositivo para a livre expressão, é preciso conhecer um pouco da história do Marco Civil da Internet.

Desde o início de sua elaboração, o projeto de lei do Marco Civil não se propôs a regular questões relativas à proteção dos direitos de autor, que estavam sendo discutidas paralelamente em uma proposta de reforma da Lei de Direitos Autorais[412]. Apesar disso, alguns pontos do texto do Marco Civil afetam o *enforcement* dos direitos autorais na Internet. Toda a

[411] Acessível em: www.anatel.gov.br

[412] Mais informações sobre a reforma da Lei de Direitos Autorais podem ser encontradas, em inglês, em: http://infojustice.org/archives/31993

parte da lei que trata da guarda de registros de conexão e de aplicações para fins de investigação, por exemplo, pode servir como infraestrutura jurídica para a persecução criminal e para permitir a requisição, pelas autoridades, dos dados de usuários que realizem alguma violação de direitos autorais.

Diante do forte lobby das empresas detentoras de direitos autorais, o texto que trata da responsabilidade dos intermediários por conteúdos de terceiros (analisado abaixo), incorporou uma exceção explicíta apontando que no caso de infração a direitos de autor, aplica-se a legislação autoral vigente.

Por outro lado, há regras que limitam o *enforcement* dos direitos de autor, protegendo a liberdade de expressão e de comunicação, como a contida no artigo 7°, IV. Ao proibir a suspensão da conexão de um usuário, o Marco Civil contrariou a lógica dos mecanismos de resposta graduada para a punição a infrações de direitos de autor no ambiente digital. A resposta graduada foi aprovada (na forma de lei) em diversos países, prevendo a notificação do usuário que for identificado compartilhando arquivos protegidos por direito de autor. Após um determinado número de notificações (normalmente três), o usuário poderia ter sua conexão suspensa pelo provedor.

A criação de um mecanismo de resposta graduada chegou a ser brevemente discutida no Brasil, por meio do Projeto de Lei 5461/2009, de autoria do Deputado Bispo Gê Tenuta[413]. Diante da reação dos usuários, o Deputado acabou retirando o projeto.[414]

Responsabilidade dos intermediários

Um dos principais pontos do Marco Civil diz respeito à responsabilidade dos intermediários por conteúdo produzido e postado por terceiros. O sistema do marco Civil estabelece que estes intermediários somente podem ser responsabilizados se não obedecerem à ordem judicial determinando explicitamente a remoção de um conteúdo. A ordem judicial que determinar a remoção de conteúdo deve identificar clara e especificamente o conteúdo infringente.

A regra é importante para a liberdade de expressão por criar uma salvaguarda para os intermediários. Sem esta regra, os provedores de aplicações que têm como modelo de negócio a

[413] Mais informações sobre o projeto em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=437323. A íntegra do projeto pode ser acessada em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=10AA9EF88CA8AC4F9DB906A6D9AF5DFE.proposicoesWeb1?codteor=661984&filename=PL+5361/2009

[414] Mais informações em: http://info.abril.com.br/noticias/internet/bispo-ge-pede-retirada-do-projeto-contra-p2p-19082009-35.shl

disponibilização de uma plataforma para circulação de conteúdo gerado pelos seus usuários (como as redes sociais, por exemplo), viam-se muitas vezes incentivados a remover conteúdos diante de uma simples notificação, evitando assim o risco de serem responsabilizados pelo conteúdo supostamente infringente.

Com a regra, a decisão sobre o que é um conteúdo infringente cabe ao judiciário. Além disso, eliminou-se o risco para os intermediários, que em casos em que não há clareza sobre a ilegalidade de um conteúdo podem recusar-se a removê-lo diante de uma simples notificação.

É importante destacar que, na ausência de regras, o Brasil chegou a ter algumas decisões emblemáticas responsabilizando as plataformas por conteúdo dos seus usuários. Na mais notável, um juiz determinou, em decisão liminar, que os provedores de conexão suspendessem o acesso de todos os brasileiros ao YouTube. O motivo foi a dificuldade do Google em remover um video de uma modelo brasileira flagrada em cenas íntimas com seu namorado em local público. O YouTube chegou a ficar dois dias fora do ar, em 2007.[415]

Essa regra referente a responsabilidade dos intermediários, entretanto, comporta algumas exceções, não se aplicando às infrações de direitos autorais, que serão objeto de regulamentação espescífica por ocasião da futura reforma da Lei de Direitos Autorais.

Pornogragia de vingança

O artigo 21 do Marco Civil da Internet cria uma exceção ao regime geral de responsabilidade dos intermediários especificado acima, buscando dar uma solução mais rápida e efetiva para os casos em que há "a divulgação, sem autorização de seus participantes, de imagens, videos, ou outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado". Nesses casos, o provedor de aplicações poderá ser responsabilizado se, após "notificação pelo participante ou seu representante legal", não tomar as medidas possíveis para indisponibilizar o conteúdo.

Este artigo foi inserido no texto do Marco Civil nos últimos momentos de sua tramitação na Câmara dos Deputados, numa reação a episódios extremos, inclusive um em que a repercussão da divulgação de cenas íntimas de uma mulher pelo Whatsapp a levou a cometer suicídio[416].

[415] Mais informações em: http://g1.globo.com/Noticias/Tecnologia/0,,AA1412609-6174-363,00.html

[416] Mais informações, em português, em: http://g1.globo.com/pi/piaui/noticia/2013/11/policia-investiga-morte-de-garota-que-teve-video-intimo-divulgado-no-piaui.html

3) ACESSO À CULTURA

O direito à cultura é parte integrante dos direitos humanos. Entende-se que a cultura, além de refletir o modo de vida de uma sociedade, é fundamental para a construção do modo de agir e pensar de um indivíduo, sendo fator de fortalecimento da identidade de um povo e também do desenvolvimento humano. Tendo isso como pano de fundo, o ordenamento jurídico brasileiro recepcionou o direito à cultura desde a Constituição Federal de 1988. Contudo, seguindo as características gerais deste diploma legal, os dispositivos que versam sobre o acesso à cultura possuem caráter programático, estabelecendo diretrizes para a atuação do Estado.

O art. 23, que determina as competências comuns dos entes federativos, dispõe no seu inciso V a obrigação de garantir os meios acesso à cultura, à educação e à ciência. O art. 215, por sua vez, reforça a obrigação do Estado em garantir o pleno exercício dos direitos culturais e do acesso às fontes da cultura. Em seu § 3º, o art. 215 vai determinar a criação do Plano Nacional de Cultura (PNC), que tem entre seus objetivos a democratização do acesso aos bens de cultura.

Muitas vezes anunciado publicamente como "uma Constituição para a Internet", o Marco Civil de fato se assemelha a um diploma constitucional no que diz respeito ao direito de acesso à cultura, na medida em que afirma princípios gerais e estabelece diretrizes para a ação do poder público, porém sem determinar suas especificidades.

Em seu art. 2º, II, o Marco Civil declara os direitos humanos e o desenvolvimento da personalidade como um dos fundamentos que vai disciplinar o uso da internet no Brasil. Tratam-se, conforme mencionamos acima, de aspectos diretamente relacionados ao acesso à cultura. A lei segue, afirmando no seu art. 4º, II, que um dos objetivos da disciplina do uso da Internet será o acesso à participação na vida cultural.

É a partir do Capítulo IV que o Marco Civil trata o acesso à cultura de modo mais concreto, para além do caráter principiológico, abordando a atuação do poder público em relação à Internet. No art. 24, IX, a promoção da cultura consta como uma das diretrizes do Estado. A preferência por padrões livres e abertos também está expressa no inciso V. Indiretamente, as tecnologias que apresentam esse formato atendem ao fim de ampliação do acesso, uma vez que permitem seu uso por uma parcela da população que não teria recursos para arcar com os custos de ferramentas digitais privadas. No art. 26, a lei inclui o dever do Estado de, no cumprimento da sua prestação da educação, sempre capacitar as pessoas para o uso da Internet, considerando-a como ferramenta para a promoção da cultura.

Diante disso, é possível concluir que, no que concerne o acesso à cultura, o Marco Civil se insere em um conjunto de ações que há pouco mais de uma década passaram a ser desenvolvidas pelo Estado Brasileiro, principalmente pelo Ministério da Cultura. Em 2003, o cantor e compositor Gilberto Gil foi nomeado ministro da cultura e começou a instituir políticas de democratização da cultura que levavam em consideração a Internet não apenas como

ferramenta de produção e consumo de cultura - o que por si só já era um avanço - mas também como ambiente integrado ao cenário cultural brasileiro. A então chamada "cultura digital" passou a ser objeto de políticas de governo. Assim, ao reconhecer o acesso e a promoção da cultura como parte essencial do tratamento que o Estado brasileiro dará à Internet, o Marco Civil contribui de maneira fundamental para consolidar e institucionalizar uma visão e uma política cultural transformadora, pela qual o Brasil já vem sendo reconhecido.

4) NEUTRALIDADE DE REDE

A neutralidade de rede está prevista no artigo 9° da Lei 12.965/2014 (Marco Civil da Internet):

> Art. 9° - O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
>
> § 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
>
> I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
>
> II - priorização de serviços de emergência.
>
> § 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no **caput** deve:
>
> I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;
>
> II - agir com proporcionalidade, transparência e isonomia;
>
> III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e
>
> IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
>
> § 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

O artigo 9° estabelece que é dever das empresas que fornecem conexão à Internet tratar todos os dados enviados e recebidos de maneira igual. Isso significa que estas empresas não podem bloquear ou degradar a qualidade de qualquer tipo de serviço ou aplicação.

A aprovação deste ponto justifica-se não apenas para a preservação da liberdade de expressão, mas também para assegurar a competição e inovação na rede, evitando que os provedores de conexão bloqueiem a entrada de novas empresas e a prestação de serviços que utilizam a Internet como plataforma.

No Brasil, há relatos de violações de neutralidade de rede[417], afetando a concorrência e a capacidade de comunicação dos usuários. Em 2005, a empresa Telemar chegou a estabelecer no contrato de prestação do serviço de Internet que não era permitido "o tráfego de voz sobre IP" em seu serviço Velox. Um exemplo de serviço de Voz sobre IP (VoIP) é o Skype, concorrente direto dos serviços de telefonia ofertados pela Telemar. A prática foi objeto de Ação Civil Pública e forçou a ANATEL a se manifestar contra a proibição estabelecida em contrato. Diante das pressões, a empresa acabou por retirar do seu contrato de serviço a cláusula que proibia o uso de serviços VoIP.

A violação da neutralidade de rede, entretanto, pode afetar também o exercício de direitos humanos fundamentais, notadamente a liberdade de expressão. Isso porque acordos e práticas comerciais podem reduzir a habilidade dos cidadãos de buscar e acessar informação.[418] Num exemplo hipotético, os provedores de conexão poderiam degradar ou bloquear o acesso dos seus usuários a serviços de empresas concorrentes ou outras com quem não detenham acordo comercial, privilegiando conteúdos de grupos parceiros. No extremo, este tipo de bloqueio ou degradação poderia ser feito com base no conteúdo, reduzindo a diversidade de opiniões e informação em circulação, com graves consequências para a formação da opinião pública e para a democracia.

Nos últimos meses de tramitação do Marco Civil, este tema ganhou importância diante de práticas comerciais das empresas de telefonia móvel, que vêm ofertando acesso gratuito a redes sociais, como Twitter e Facebook. Mesmo com a aprovação da Lei, as empresas de telecomunicações têm afirmado que a neutralidade de rede não proíbe este tipo de prática

[417] Mais informações sobre práticas contrárias à neutralidade de rede e o estado da arte da regulação na Europa podem ser encontradas em: http://www.openforumacademy.org/library/ofa-research/OFA%20Net%20Neutrality%20in%20the%20EU%20-%20Country%20Factsheets%2020130905.pdf [acesso em 20.05.2014]

[418] O direito de acessar informação está contemplado como uma dimensão da liberdade de expressão no artigo 19 da Declaração Universal de Direitos Humanos e no Artigo 13.2 da Convenção Americana de Direitos Humanos.

comercial[419], apesar das autoridades de outros países que regulamentaram a neutralidade de rede, como o a Subtel do Chile, apontarem em sentido contrário.[420]

O debate, portanto, não se encerrou com a aprovação do Marco Civil. Apesar de o texto da lei ser claro o suficiente para proibir práticas como a de ofertar gratuitamente alguns serviços em detrimento de outros, sua interpretação será disputada pelas empresas de telecomunicações. Além disso, a lei deverá ser regulamentada por Decreto Presidencial, abrindo novo espaço para disputas em torno do conceito de neutralidade. Uma das modificações positivas introduzidas no texto final do Marco Civil foi a previsão de que a regulamentação da neutralidade da rede deve ser elaborada após consulta ao Comitê Gestor da Internet (CGI.br) e a Agência Nacional de Telecomunicações (Anatel).

A inclusão do CGI.br no texto inicial enfrentou resistências por parte do Ministério das Comunicações e da Anatel. Essa disputa replicava internamente as divergências que ocorrem no ambito internacional acerca de onde traçar a linha divisória entre telecomunicações e Internet. A menção ao CGI.br for retirada do projeto e só voltou a ser inserida na última versão do texto. A composição multissetorial do CGI.br - cujo conselho é formado por órgãos do governo, empresas, Academia, comunidade técnica e terceiro setor - pode levar a uma avaliação mais plural acerca de como deve ser regulamentada, na prática, a neutralidade de rede.

[419] Mais informações sobre o posicionamento das empresas de telecomunicações sobre este tema em: http://www.teletime.com.br/03/06/2014/anatel-se-alinha-as-teles-e-defende-trafego-gratuito-na-regulamentacao-da-neutralidade/tt/379757/news.aspx

[420] O assunto foi noticiado na mídia especializada brasileira. Como exemplo, ver: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=36898&sid=4