por los Derechos Civiles

LIBERTAD DE EXPRESIÓN

EN EL ÁMBITO DIGITAL

EL ESTADO DE SITUACIÓN EN AMÉRICA LATINA

Un proyecto de la ADC, con la colaboración de Derechos Digitales, Artigo 19, Fundación Karisma y el CELE

adcdigital.org.ar

Área de Libertad de Expresión

Enero de 2016

adc.org.ar | adcdigital.org.ar

El presente trabajo fue realizado con la colaboración de Open Society Foundations.

Índice

Introducción

La Asociación por los Derechos Civiles (ADC) es una organización no gubernamental argentina que, desde su fundación, se propuso contribuir a afianzar una cultura jurídica e institucional que garantice los derechos humanos de las personas. Dentro de su misión, la defensa de la garantía de la libertad de expresión en el ámbito digital ha desempeñado un papel trascendental. Desde la convicción de que Internet debe ser abierta, global, estar libre de censura y ser capaz de promover la creatividad y el intercambio de conocimiento, la asociación ha llevado a cabo diferentes acciones para promover la defensa de la libertad de expresión.

El informe que se presenta a continuación ha sido fruto de una iniciativa llevada a cabo por la Asociación de los Derechos Civiles (Argentina), quien convocó a un grupo de prestigiosas organizaciones de la región para que cada una de ellas elaborara un reporte acerca del estado de situación de la legislación y jurisprudencia sobre las distintas temáticas que abarca la relación entre la libertad de expresión y el entorno digital. Este trabajo se presentará a la Relatoría Especial por la Libertad de Expresión de la Honorable Comisión Interamericana de Derechos Humanos (CIDH) a fin de poner en conocimiento de la Comisión (a través de la RELE) los principales desafíos que afronta la garantía de la libertad de expresión en el ámbito digital y las maneras en que los Estados están respondiendo a los nuevos fenómenos.

El informe está dividido en cinco capítulos. El primero fue redactado por la organización Derechos Digitales (América Latina) y trata sobre Libertad de Expresión y Derecho al Anonimato. El segundo fue elaborado por Artigo 19 (Brasil) y versa sobre el Derecho al Olvido. El tercero se refiere a la Vigilancia Estatal de las Comunicaciones y es obra de Fundación Karisma (Colombia). El cuarto aborda la Criminalización del Discurso Crítico en Internet y fue escrito por el Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Universidad de Palermo (Argentina). Finalmente, el último capítulo trata sobre la Responsabilidad de Intermediarios de Internet y fue redactado por la Asociación por los Derechos Civiles.

La problemática de la libertad de expresión *on line* es de una indudable actualidad y por lo tanto, necesita de la participación de todos los sectores interesados en la defensa de los derechos humanos. Sirva entonces este informe como herramienta de difusión de los últimos desarrollos legislativos y jurisprudenciales llevados a cabo por los gobiernos de la región, para que el deseado debate pueda realizarse con un amplio conocimiento de la temática.

Libertad de Expresión y Anonimato (Derechos Digitales[1])

Valentina Hernández Bauzá[2]

1. Introducción

El derecho a la libertad de expresión es uno de especial relevancia en un régimen democrático, considerado una de las libertades personales de mayor importancia y reconocida en documentos tales como la Declaración Americana sobre los Derechos y Deberes del Hombre, la Convención Americana sobre Derechos Humanos, la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, entre otros instrumentos internacionales y Constituciones de los países de la regiónn[3].

A su turno, y a lo largo de la historia, el anonimato ha cumplido un rol esencial, tanto en el ejercicio como en el resguardo de derechos tales como la libertad de expresión, privacidad y los derechos políticos, especialmente para la participaciónn pública y el debate[4]. La relación entre ambos aspectos de la libertad de expresión nace del resguardo que la protección de este derecho debe proveer al autor de una expresión, como también a su mensajero. No solamente desde el punto de vista de la represión del discurso mismo, sino del aseguramiento de que ese discurso exista sin consecuencias negativas para sus autores o mensajeros a nivel personal.

Las herramientas tecnológicas abren nuevas formas de expresión. A pesar de que ellas tienden a identificar a sus usuarios, existen también mecanismos para evitar la

[1] Derechos Digitales es una organización de alcance latinoamericano, independiente y sin fines de lucro, fundada en 2005 y que tiene como objetivo fundamental el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital https://www.derechosdigitales.org/

[2] Egresada de la carrera de Licenciatura de Ciencias Jurídicas y Sociales de la Facultad de Derecho de la Universidad de Chile. Fue ayudante de los departamentos de Ciencias del Derecho y Derecho Público, colaboró como ayudante en la cátedra de Introducción de Introducción al Derecho y actualmente es ayudante de la cátedra de Derecho Constitucional, todo en la misma Facultad. Actualmente se desempeña como investigadora en Derechos Digitales, trabajando en temas de privacidad, libertad de expresión y seguridad en línea en América Latina.

[3] COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, "*Declaración de Principios sobre Libertad de Expresión*". En línea, disponible en: https://www.cidh.oas.org/basicos/basicos13.htm [Fecha de consulta: 08 de octubre, 2015]

[4] UNITED NATIONS, op. cit., p. 16.

identificación de los individuos (el anonimato propiamente tal), o bien para impedir el conocimiento de las comunicaciones o mantener su confidencialidad (el cifrado). Sin embargo, la viabilidad técnica de tales medidas está todavía limitada por condiciones sociales y legales que pueden poner en riesgo a quien pretenda hacer uso de tales herramientas. La vinculación entre la libertad de expresión y los mecanismos de anonimato y cifrado hacen necesaria la reflexión sobre la protección de la primera en el entorno en línea.

2. Libertad de expresión y anonimato: generalidades

A lo largo de la historia se han proporcionado variados argumentos para fundamentar y resaltar la importancia de la libertad de expresión. Además de ser considerado como parte esencial de un régimen de libertades personales, ha sido definido, defendido y tratado por una larga gama de pensadores a lo largo de la historia de la humanidad, no siendo un objeto del estudio exclusivo del campo jurídico.

El derecho a la libertad de expresión está contenido en el artículo 13 de la Convención Americana sobre Derechos Humanos (en adelante, CADH):

> 1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística o por cualquier otro procedimiento de su elección.
>
> 2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
>
> a) el respeto a los derechos o a la reputación de los demás, o
>
> b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.
>
> 3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.
>
> 4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Está prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquiera otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

La regulación continental incluye, entonces:

- La libertad de emitir opinión, sin censura previa ni requiriendo la autorización previa de ningún tipo de autoridad.
- La libertad de informarse, la cual importa poder buscar, recibir y emitir información de todo tipo y a través de cualquier medio. Esta es activa (derecho a buscar información) como pasiva (derecho a poder recibir información, especialmente la emanada de organismos públicos).

Su ejercicio no está sometido a las fronteras geográficas. No obstante, tiene otros límites: el respeto a los derechos y reputación de los demás miembros de la sociedad, y el rechazo a la apología del odio. La Convención no contempla al anonimato dentro de los límites al derecho a la libertad de expresión, como sí lo hacen las Constituciones de determinados Estados miembros, como se verá más adelante.

Las concepciones clásicas sobre este derecho se han visto puestas a prueba por el avance de la tecnología, que han creado nuevos canales para ejercitar el derecho como también nuevas herramientas para controlar y restringirlo. La red se ha impuesto actualmente como el principal medio de comunicación, información y expresión[5], lo que ha sucedido, en gran parte, gracias a su estructura libre y descentralizada[6].

Esto cobra especial relevancia dentro de la región al momento de mirar las cifras de penetración de servicios de internet en Latinoamérica, sobre todo de internet móvil. Actualmente, las conexiones a internet a través de telefonía móvil se encuentran en alza, constituyendo estas actualmente el 31 % de las mismas, pero para el año 2020 se estima que esta cifra alcanzará al 68 %[7]. También, se estima que en el año 2020 la tasa de conexiones a la red a través de *smartphones* en la región será de 605

---

[5] PR NEWSWIRE. "*Global 'Digital Life' Research Project Reveals Major Changes in Online Behaviour*", Londres, 10 de octubre de 2010. En línea, disponible en: http://www.prnewswire.com/news-releases/global-digital-life-research-project-reveals-major-changes-in-online-behaviour-104660154.html [Fecha de consulta: 16 de Octubre de 2015].

[6] MOYA, R. 2003. "La Libertad de Expresión en la Red Internet" en *Revista Chilena de Derecho Informático*, número 2 (mayo 2003). Chile, Facultad de Derecho de la Universidad de Chile, p. 89.

[7] GSMA, "*The Mobile Economy. Latin America 2014*". En línea, disponible en: http://www.gsmamobileeconomylatinamerica.com/GSMA_Mobile_Economy_LatinAmerica_2014.pdf [Fecha de consulta: 13 de Octubre de 2015], pp. 16-17.

millones, la segunda más alta del mundo[8]. Teniendo la segunda más grande base instalada en el globo es consecuencia previsible que buena parte del contenido de la red será emitido por los habitantes de esta región. Por ello, se hace urgente atender a la protección de la libertad de expresión en línea en Latinoamérica.

No obstante, la tecnología también ha supuesto nuevas formas de interferir de forma ilegítima en su ejercicio, especialmente por los gobiernos y grandes empresas. Según David Kaye, indica que la censura en línea, la vigilancia –tanto masiva como la dirigida específicamente a determinados sujetos- y la recolección de datos, los ataques digitales a miembros de la sociedad civil y la represión llevada a cabo a través de la red han afectado al derecho a emitir opiniones sin interferencia previa y a buscar, recibir y emitir información e ideas de todo tipo[9].

3. Libertad de Expresión, Privacidad y Anonimato

El hecho de que internet haya adquirido tanta relevancia en el ejercicio de este derecho hace que necesariamente se establezca un vínculo entre la libertad de expresión y la privacidad de los usuarios, tal como lo han indicado diversos informes y textos académicos en lo que llevamos de década[10].

Con las herramientas actuales a disposición tanto del gobierno como de entes privados no es complejo poder registrar, procesar y monitorear la actividad en línea de los usuarios. Incluso sin tener que conocer el contenido de las comunicaciones realizadas a través de la web, con el análisis de la metadata asociada a estas, es posible conocer el comportamiento, las relaciones sociales, las preferencias privadas y la identidad del usuario[11]. En caso que este monitoreo sea desproporcionado a su motivo original, derivando en vigilancia masiva, o en aquellos casos en que una persona sepa o sospeche fundadamente que es blanco de monitoreo, ello repercutirá directamente en su conducta en línea, cuidando que dice, con quien se reúne, dónde va, qué información busca y qué recibe[12]. Esto es especialmente preocupante si consideramos que en determinadas partes del globo se han utilizado estos instrumentos para perseguir a opositores políticos, miembros de la sociedad civil y periodistas.

---

8 Ibid., op. cit., p. 5.

9 UNITED NATIONS, Human Rights Council. "*Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression"*. Mayo de 2015, p. 3.

10 En este sentido NACIONES UNIDAS, Consejo de Derechos Humanos, "El Derecho a la Privacidad en la Era Digital", 2014, UNITED NATIONS, op. cit., CORTÉS, C. 2014. "Vigilancia de la Red: ¿Qué Significa Monitorear y Detectar Contenidos en Internet?" en *Internet y Derechos Humanos. Aportes para la Discusión en América Latina*, Universidad de Palermo, pp. 35-60 y COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial para la Libertad de Expresión "Libertad de Expresión e Internet", 2013.

11 UNITED NATIONS, op. cit., p.7.

12 CORTÉS, C. op. cit., p. 55.

Es por ello que el anonimato cobra especial relevancia. El informe del Consejo de Derechos Humanos de Naciones Unidas sobre cifrado y anonimato es claro en este punto: las herramientas de anonimato y cifrado son actualmente las principales vías para resguardar la seguridad en línea. Así, si las grandes compañías y los gobiernos tienen acceso a herramientas tecnológicas protectoras de privacidad, no existe razón para que los usuarios de la red no puedan disponer de herramientas de ocultamiento de identidad o de contenido, es más, es recomendable que así lo hagan, por las circunstancias ya expuestas[13].

Dado este nexo entre anonimato como elemento de resguardo para ejercer el derecho a la libertad de expresión en un entorno digital, ahondaremos más en este punto.

4. ¿Qué es el Anonimato?

La noción de anonimato no es algo nuevo, pues podemos rastrear sus inicios varios siglos atrás, en los albores de la humanidad. El vocablo anonimato proviene del griego *anonymia* que significa "sin nombre", entendiendo que el resto de la gente no podrá saber la identidad de quien no lo tiene[14]. El conocido fallo *McIntyre v Ohio Elections Commissions* de la Corte Suprema de Justicia de los Estados Unidos de América (1995) es decidor. La controversia recayó sobre la prohibición de repartir material anónimo de campaña política, y la Corte decidió que quienes emiten un discurso pueden querer permanecer anónimos por el miedo a represalias físicas, sociales y económicas. Así, definió al anonimato como un escudo protector de la tiranía de la mayoría, siendo este reconocido y considerado como parte del contenido esencial de la primera enmienda de la Constitución estadounidense[15].

Con los medios tecnológicos de procesamiento de datos es posible construir, averiguar y predecir con un alto grado de certeza la identidad y aspectos íntimos de un individuo supuestamente anónimo. Se ha afirmado que el solo hecho de conectarnos a internet hace ilusorio el anonimato, puesto que este mero acto ya entrega de inmediato a los proveedores de internet (o ISP) algún grado de identificación, el cual se va especificando todavía más con el resto de actividades que realizamos en línea[16].

---

[13] UNITED NATIONS, op. cit., pp. 3-6.

[14] VOCABULARY.COM., "Anonymity". En línea, disponible en: http://www.vocabulary.com/dictionary/anonymity [Fecha de consulta: 15 de Octubre de 2015].

[15] McNEALLY, J. 2012. "A Textual Analysis of the Influence of McIntyre v. Ohio Elections Commission in Cases Involving Anonymous Online Commenters" en *First Amendment Law Review*, Vol. 11, pp. 149-171. p. 152.

[16] VOORHOOF, D. 2010. "Internet and the Right of Anonymity" en *Proceedings of the Conference Regulating the Internet*. Belgrado, 2010, p.2.

Dado lo anterior, para poder definir el rango de lo que puede cubrirse bajo el manto del anonimato, es necesario establecer qué compone la identificación de un sujeto. Así, Gary T. Marx en el año 2001[17] señaló que debemos considerar los siguientes elementos:

- El nombre de la persona, tanto completo como parcial. Esto responde a la pregunta "quién".
- Datos de identificación tales que permitan localizar y encontrar al sujeto. Esto responde a la pregunta del "dónde". Acá podemos enmarcar, por ejemplo, el número de teléfono o su correo electrónico.
- Símbolos o secuencias de caracteres que puedan ser ligados a una persona -quién- o a una dirección -dónde-. Por ejemplo, números de tarjetas bancarias, datos biométricos o la fecha de nacimiento.
- Apodos, pseudónimos o símbolos que, a primera vista, no pueden ser rastreada su vinculación a una persona. Ello puede ser porque la misma ley o políticas de uso del servicio otorgan un número para acceder a este o recibir un resultado sin que en en momento alguno se proporcione el nombre del individuo (por ejemplo, un número generado por un servicio de salud para acceder a los resultados de un examen de VIH) o también, aquellos casos en que el sujeto esté usando una identidad falsa en línea.
- Patrones de comportamiento o rasgos identificatorios referidos a la apariencia física de la persona. Hoy en día, en gran medida a consecuencia del uso de herramientas tecnológicas, estos datos se han filtrado y hecho público o incluso, predecidos. Acá es donde quizás más resalta que aunque se desconozca el nombre de alguien, ello no implica que sea totalmente desconocido.
- Las categorías sociales en las cuales puede ser clasificado un sujeto. Sexo, estrato socioeconómico, estado de salud, afiliaciones de cualquier tipo, entre otros ejemplos. El solo hecho de ser amigo de alguien o de encontrarse con un determinado grupo de personas en un lugar y momento puede ser clave para descifrar la identidad del individuo, o para atribuirle características que no posee o enmarcarlo en algún grupo, sin que realmente sea miembro.
- Finalmente, se consideran como parte de la identidad de un individuo aquellas certificaciones que acrediten poseer un conocimiento o una preferencia en particular, los cuales pueden ir desde saber una contraseña,

[17] MARX, G. 2001. "Identity and Anonymity: Some Conceptual Distinctions and Issues for Research" en *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton University Press. En línea, disponible en http://web.mit.edu/gtmarx/www/identity.html [Fecha de consulta: 19 de octubre de 2015], pp. 2-3.

alguna señal visible que otorgue información de una persona (un uniforme o un tatuaje, por ejemplo), la posesión o compra de un objeto (un ticket para un recital) o poseer alguna habilidad ya sea física o intelectual (como lo sería hablar un idioma extranjero o saber conducir).

Por tanto, al hablar de anonimato deberíamos, al menos, considerar los rasgos de identificación recién expuestos. Para gozar de anonimato, actualmente, no basta con solo ocultar el nombre.

A nivel interamericano, es posible encontrar menciones al anonimato y su relación con el derecho a la libertad de expresión. En el informe "Internet y Libertad de Expresión" elaborado el año 2013 por la relatoría especial para la libertad de expresión de la Comisión Interamericana de Derechos Humanos, se trata la especial relación existente entre este derecho y el derecho a la privacidad. En tal oportunidad, la relatoría especial indicó que el respeto a la libertad de expresión presupone la privacidad de las comunicaciones, sin que existan injerencias arbitrarias en estas últimas[18]. En este sentido, para proteger de manera efectiva la privacidad en el ejercicio de la libertad de expresión, la relatoría señala dos políticas concretas: la protección de datos personales y del discurso anónimo[19].

En ese marco, se asocia al anonimato con el ejercicio de la participación en el debate público, como forma de evitar represalias[20]. Además, expresa que los requerimientos de identificación y autenticación en línea deben ser usados únicamente en transacciones e interacciones sensibles y riesgosas, excluyendo su uso generalizado y respetando el principio de proporcionalidad. Igualmente, destaca que debe existir flexibilidad en los mecanismos de identificación exigidos, pues evitando los mecanismos únicos y concentrados, se combate tanto los problemas de seguridad en línea como las intrusiones a la privacidad[21].

La Corte Interamericana de Derechos Humanos se ha referido limitadamente en el caso *Escher y otros v Brasil,* que si bien se refiere al derecho a la privacidad, tiene una vertiente interesante relacionada a anonimato. Siguiendo la línea de los aspectos de identificación que debieran ser cubiertos por el anonimato, en dicho párrafo se discurre que no solo goza de protección el contenido mismo de una comunicación privada, sino que también a "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

[18] COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial Para la Libertad de Expresión. "*Libertad de Expresión e Internet"*. 2013, pp. 62-63.
[19] Ibid., op. cit., p. 63.
[20] Ibid., op. cit., p. 64.
[21] Ibid., op. cit., pp. 64-65.

de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones"[22].

En suma, como podemos apreciar, en el Sistema Interamericano de Derechos Humanos no se define al anonimato en sí mismo, sino como política asociada al ejercicio del derecho a la libertad de expresión. Luego, la Corte Interamericana ha reconocido protección convencional a aspectos de identificación personal, los cuales están en la esfera de lo que una debida interpretación y adaptación del concepto de anonimato requieren.

5. La Importancia del Anonimato Como Forma de Proteger el Derecho a la Libertad de Expresión.

Ya hemos resaltado la íntima relación existente entre el efectivo ejercicio del derecho a la libertad de expresión y el anonimato como política destinada a aquello. Además, ha quedado de manifiesto cómo las tecnologías han potenciado a este derecho humano, pero, a la vez, cómo han creado nuevas amenazas para este y han derivado también en una debilitación del anonimato, llevándonos a reinterpretar este para adecuarlo a la realidad actual.

A continuación, profundizaremos, en primer lugar, cómo se ha enfocado el debate respecto a la regulación del anonimato en línea, tanto la opinión de sus defensores como detractores. Posteriormente, proseguiremos tratando las formas en que el anonimato potencia a la libertad de expresión y a la dinámica de funcionamiento en conjunto.

6.El Debate sobre el Anonimato en Línea.

La estructura de la red, dentro de varios elementos, comprende el anonimato virtual[23], elemento clave para la participación de los usuarios en la generación de contenido y comunicaciones. Por otro lado, es sabido que el anonimato no es absoluto, sino que está supeditado a las responsabilidades legales atribuibles a quienes emitan comentarios que, carentes de todo motivo justificable, vulneran los derechos a la intimidad, propia imagen, honra[24] o promuevan el discurso al odio o supongan actividad criminal.

---

[22] CORTE INTERAMERICANA DE DERECHOS HUMANOS, *Caso Escher y Otros v Brasil* (Sentencia de 06 de julio de 2009). En línea, disponible en http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf [Fecha de consulta: 19 de octubre de 2015], párrafo 114, p.34.

[23] MOYA, R. op. cit., p. 96.

[24] TOBÓN-FRANCO, N y VARELA-PEZZANO, E. 2010. "Libertad de Expresión y Salvaguardia del Anonimato: Panorama Jurisprudencial en Colombia" en *Díkaion*, v.19(1), Cundinamarca, Universidad de La Sabana, junio de 2010, pp. 124-125.

Actualmente, diversos países alrededor del globo han establecido medidas tendientes a eliminar el anonimato en internet, ya sea imponiendo obligaciones tales como el registro de todas las direcciones IP del país, el registro de usuarios de equipos en un locutorio o cibercafé, la prohibición del uso de pseudónimos y obligación de uso del nombre real, por citar algunas[25]. Los argumentos utilizados para lo anterior, por lo general, son el combate de la actividad criminal (especialmente el crimen organizado, estafas en línea, terrorismo, tráfico de sustancias psicotrópicas y pornografía infantil) y como medida tendiente a enfrentar el acoso en línea y comentarios que escapan al contenido protegido por la libertad de expresión. Esto, en la práctica, ha llevado a que en algunos lugares del mundo tales medidas se utilicen para evitar que la ciudadanía acceda a determinada información, para la persecución gubernamental por dichos de opositores o vigilancia masiva, se encuentran entre estas manifestaciones del uso excesivo de estos mecanismos dispuestos a enfrentar los problemas en línea ya enunciados.

Es por ello que la defensa del anonimato en línea se hace compleja. Si bien hay peligros asociados al uso del anonimato, tenemos como contrapartida el abuso que se puede hacer de las medidas tendientes a enfrentar sus usos ilegítimos. Igualmente, hay que sopesar los riesgos que crea el anonimato en línea en relación a los beneficios que aquel conlleva, considerando con especial énfasis que internet es el principal canal de comunicación y de información en el mundo[26].

En el pronunciamiento hecho por Naciones Unidas este año a favor del anonimato y cifrado como herramientas de resguardo de los derechos a la libertad de expresión y privacidad en internet, se recalca su importancia como elementos protectores de la seguridad en línea de los usuarios, para buscar, leer, desarrollar y compartir opiniones e información sin interferencias, además de permitir a periodistas, organizaciones de la sociedad civil, grupos étnicos o religiosos, personas perseguidas por su orientación sexual o identidad de género, activistas, miembros de la academia, artistas y, en general, a todos aquellos que ejerciten sus derechos a la libertad de expresión a través de internet[27].

Si bien los argumentos a favor del anonimato y el cifrado suelen ser aquellos referidos a regiones especialmente conflictivas, este no solo es necesario en aquellos países en los cuales la población no puede expresarse abiertamente sobre sus ideas y actividades sin enfrentar la amenaza de sanciones legales o respuesta gubernamental, sino que también en un régimen democrático menos hostil, para

---

[25] UNITED NATIONS, op. cit. p. 17.

[26] DECCAN HERALD. “Internet Now Single Biggest Source of Global Information”. *Deccan Herald*. 02 de Diciembre de 2010. En línea, disponible en http://www.deccanherald.com/content/117379/internet-now-single-biggest-source.html [Fecha de consulta: 30 de octubre de 2015]

[27] UNITED NATIONS., op. cit., loc. cit.

que así se puedan discutir temas que de otro modo serían muy sensibles, o sencillamente para proteger fuentes de información[28].

Lamentablemente, como hemos expuesto, en discusiones sobre anonimato suelen resaltar los aspectos negativos por sobre sus beneficios. Dificultades en la persecución de los responsables de hechos cometidos bajo el alero del anonimato, como cibercrimen y acoso en línea, son los puntos en los cuales se suele basar esta postura[29]. En los últimos cinco años las voces que proclaman poner fin al anonimato en línea han sido bastante fuertes; el año 2012 en Nueva York se propuso legislar sobre la eliminación del discurso anónimo en internet, imponiendo la obligación de quienes comentan sobre algún tema en la red un plazo de cuarenta y ocho horas para dar a conocer su dirección IP, nombre legal y domicilio[30]. Lo anterior es fiel reflejo de la discusión actual: en los Estados Unidos de América este debate es intenso y variados sitios web han abogado por la eliminación del anonimato, y hasta del uso de pseudónimos, en su sección de comentarios, argumentando la baja calidad de la discusión que generan (normalmente centrada en insultos) y el acoso en línea[31].

Esta tendencia a eliminar el anonimato en internet no es exclusiva de la prensa o de las plataformas de opinión. En diferentes partes del globo se ha impuesto tanto la obligación de usar nombres reales en internet tanto como la de otorgar a organismos públicos las facultades técnicas necesarias para poder averiguar la identidad de quien está detrás de un teclado a través de medidas tales como: solicitar registros de números de teléfonos móviles o IP y asociarlos a un sujeto en particular, imponer a los ISPs llevar registro de la actividad en línea de sus abonados o el uso de de herramientas de espionaje digital por parte de las policías. Especialmente, se han alzado cuestionamientos sobre el uso real de nombres en internet, tanto en redes sociales como en la sección de comentarios de diversos sitios, para poder perseguir de forma más eficiente las responsabilidades legales asociadas al comentario realizado, sobre todo, por la actividad de los llamados

---

[28] HARRIS, M y HUGHES, K. "Privacy and Free Expression: Competing or Complementary Rights?" en *Media Law and Ethics in the 21st Century*. Protecting Free Expression and Curbing Abuses. Londres, Palgrave Macmillan, 2014. p. 159.

[29] DAVENPORT, D. "Anonymity on the Internet: Why the Price May Be Too High" en *Communications of the ACM*, abril 2002, v. 45(4), pp. 33-34. En línea, disponible en http://www.csl.mtu.edu/cs6461/www/Reading/Davenport02.pdf [Fecha de Consulta: 14 de octubre de 2015].

[30] HOLPUCH, A. "New York Lawmakers Propose Bill to Ban Anonymous Online Speech". *The Guardian*. 23 de Mayo de 2012. En línea, disponible en http://www.theguardian.com/technology/us-news-blog/2012/may/23/anonymous-comment-ban-new-york [Fecha de consulta: 30 de octubre de 2015]

[31] TARSI, M y WALLSTEN, K. "It's Time to End Anonymous Comments Sections". *The Washington Post*. 19 de Agosto de 2014. En línea, disponible en https://www.washingtonpost.com/news/monkey-cage/wp/2014/08/19/its-time-to-end-anonymous-comments-sections/ [Fecha de consulta: 30 de octubre de 2015]

"trolls" de internet y en casos de acoso en línea, o en que el contenido subido pueda generar responsabilidades al intermediario[32].

A pesar de lo anterior, se ha sostenido que el mal uso del anonimato en la red no puede respaldar el uso de medidas que vulneren el principio de proporcionalidad, aun cuando se busque la persecución criminal. Para el relator especial de Naciones Unidas David Kaye, las medidas tecnológicas establecidas a encontrar a determinadas agujas en un pajar no son suficientes en sí, sino que lo relevante es el impacto que ellas pueden tener en todo el pajar en relación con el riesgo de que se trate, mirando a la necesidad y proporcionalidad de cada medida[33]. Estas medidas, utilizadas de forma indiscriminada, inevitablemente afectan al derecho a la libertad de expresión, en tanto los individuos temen que se sepa su actividad en internet, como lo sería los sitios que visita, que opina o a qué información accede[34].

En efecto, no todo el pajar, en los términos usados por Naciones Unidas, utiliza el anonimato para desplegar un comportamiento legalmente reprochable. Pacientes que utilizan el anonimato para hablar de las enfermedades que padecen, discusiones políticas llevadas a cabo tras un pseudónimo que evita que gente real sea estigmatizada en su entorno no virtual, *whistleblowers* e incluso las mismas víctimas de acoso o mensajes de odio en línea para denunciar y contar su testimonio[35].

Un estudio realizado por el Departamento de Psicología de la Universidad de Carnegie Mellon en 2013[36] sobre los motivos por los cuáles las personas buscan ser anónimos en internet arrojó que no siempre se realiza para cometer ilícitos, sino que las razones podían ser divididas en cinco grandes grupos: protegerse de los "depredadores en línea" (criminales, hackers, acosadores, estafadores) y de organizaciones (estatales como corporaciones privadas), evitar ser reconocido por usuarios de una comunidad, o reconocer a otros miembros de una comunidad y por

---

[32] Entendiendo intermediario de internet como aquellos que reúnen o facilitan las transacciones realizadas entre terceros a través de internet. Ellos dan acceso a alojar, transmitir e indexar contenido, productos y servicios elaborados por terceros y puestos a disposición en línea como, también, pueden proporcionar acceso a servicios de internet. Definición disponible en OECD. 2011. "*The Role of Internet Intermediaries in Advancing Public Policy Objectives*". En línea, dsponible en http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives_9789264115644-en#page21 [Fecha de consulta: 27 de octubre de 2015], p. 20.

[33] NACIONES UNIDAS, op. cit., p.9.

[34] UNITED NATIONS, op. cit., p.8

[35] COLLEMAN, G. "Anonymity Online Serves us All" en *New York Times*. 24 de Agosto de 2014. En línea, disponible en http://www.nytimes.com/roomfordebate/2014/08/19/the-war-against-online-trolls/anonymity-online-serves-us-all [Fecha de consulta: 26 de Octubre de 2015].

[36] BROWN, S, KANG, R, KIESLER, S and HUMAN COMPUTER INTERACTION INSTITUTE. "Why do People Seek Anonymity on the Internet? Informing Policy and Desing" en *CHI '13 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, 2013. En línea, disponible en https://www.cs.cmu.edu/~kiesler/publications/2013/why-people-seek-anonymity-internet-policy-design.pdf [Fecha de Consulta: 26 de Octubre de 2015], pp. 4-5.

el resto de la sociedad. En estos últimos tres grupos, se incluye el propósito de evitar que en la vida real hagan comentarios de su actividad en línea, ser reconocidos por compañeros de trabajo, familiares o exparejas o evitar que la información emitida por la persona luego le pueda jugar una mala pasada, tanto por el uso de sus datos personales como por sus opiniones vertidas.

Informes como el anterior dan cuenta de una dimensión positiva del anonimato, una que protege a los usuarios de la red de estafas, suplantaciones, acoso, consecuencias negativas en la vida real por hacer un comentario o por compartir o ser fan de un determinado pasatiempo. Como enfatizamos al inicio de este informe, el derecho a la libertad de expresión comprende una dimensión individual la cual ampara la expresión de ideas y preferencias personales de un sujeto.

A modo de conclusión, si bien no todos los usos del anonimato pueden ser tutelados por la ley, es necesario establecer límites claros a su intromisión, los cuales deben estar marcados por un estricto respeto a los requisitos de necesidad y proporcionalidad. En ningún caso se puede permitir el detrimento masivo del derecho a la libertad de expresión justificando aquel en el actuar reprochable de unos pocos. Hay que ponderar los beneficios y perjuicios, y no solo focalizarse en uno de los platillos de la balanza a la hora de elaborar políticas públicas y legislar en torno a internet y anonimato.

7. La Utilidad del Anonimato en Relación al Derecho a la Libertad de Expresión.

En base a lo anterior, el anonimato es útil al menos para las siguientes manifestaciones del derecho a la libertad de expresión:

<u>Difusión de Opiniones, Testimonios y Preferencias Personales:</u>

- Las opiniones vertidas en la red pueden tener consecuencias en la vida real. Los motivos para querer ser anónimo varían dependiendo de la persona a quien preguntamos, por tanto existen tantas razones como individuos en el mundo.
- Debido a esta amplia diversificación de intereses, características y realidades, el anonimato no solo es utilizado aquellos países en los cuales el gobierno persigue activamente a los opositores, sino que también es necesario para todas aquellas manifestaciones de la personalidad que podamos imaginarnos.

- En el marco del proyecto de Youth IGF con Childnet International (2013)37 se realizó una encuesta global a jóvenes a partir de los trece años, que en forma similar al estudio universitario ya citado, se preguntó a los participantes el uso que le daban al anonimato en internet. Los resultados fueron similares, siendo los mayores usos los siguientes: para proteger su información personal (65 % del total de encuestados), para sentirse más seguros (47 % del total de encuestados), para proteger su reputación (29 %), para evitar meterse en problemas (29 %), para decir algo de lo cual se sienten avergonzados (27 %), para decir algo que tienen miedo de decir (23 %), para sentirse seguros de sí mismos (23 %), porque es divertido (23 %), para emitir una opinión controvertida (17 %) y, finalmente, para realizar actividades ilegales (3 %). La mayoría de las respuestas de los encuestados dan cuenta de usos legítimos. Tal y como se indicó por parte de Naciones Unidas, quienes se guarnecen en el anonimato para abusar del mismo son una cantidad pequeña de personas en comparación a quienes les dan usos amparados por el derecho a la libertad de expresión u otros derechos fundamentales.
- Incluso si sus usos pueden generar gran daño, el mismo anonimato en línea puede ser útil para las mismas víctimas de esos abusos. The Telegraph indicó que las mujeres que han sufrido de acoso a través de la red pueden utilizar esta misma para dar a conocer su testimonio y denunciar tales hechos. Igualmente, han encontrado en internet un lugar para poder discutir sin temor a ser juzgadas temas como sexualidad, problemas de violencia que hayan sufrido y política, lo cual se hace especialmente útil en los casos de mujeres de comunidades aisladas, que puedan tener consecuencias en su vida familiar o profesional o que vivan en regímenes donde dichos temas no puedan ser abiertamente discutidos[38].
- Las comunidades LGBT también han encontrado un nicho de vital importancia en la red para el pleno desarrollo de su plan de vida. Dentro de los beneficios39 para esta comunidad están obtener información relevante a su orientación sexual y al descubrimiento y exploración de la misma, buscar potenciales parejas, crear grupos de discusión y reunión, entre otros, los

---

[37] YOUTH IGF PROJECT y CHILDNET INTERNATIONAL. 2013. "*Global Perspectives on Online Anonymity: Age Trends in the Use of Anonymity Online and its Impact on Human Behaviour and Freedom of Expression*". En línea, disponible en: http://www.youthigfproject.com/uploads/8/5/3/6/8536818/global_perspectives_on_online_anonymity.pdf [Fecha de Consulta: 27 de octubre de 2015], p. 4.

[38] MAGNANTI, B. "Why Women Need the Internet to Remain Anonymous?". *The Telegraph*. 12 de septiembre de 2013. En línea, disponible en http://www.telegraph.co.uk/women/womens-life/10304593/Why-women-need-the-internet-to-remain-anonymous.html [Fecha de consulta: 27 de octubre de 2015].

[39] STEIN, E. 2003. "Queers Anonymous: Lesbians, Gay Men, Free Speech, and Cyberspace". *Harvard Civil Rights-Civil Liberties Law Review* v.38, pp. 161-162.

cuales son incluso más importantes en aquellos casos en que una persona no puede hablar abiertamente de su condición sexual minoritaria. Esto adquiere mayor relevancia si consideramos que, a diferencia del descubrimiento de la identidad heterosexual, para parte de la sociedad el ejercicio de la libertad de expresión por parte de miembros de las minorías sexuales pueden ser parte del discurso impopular[40], el cual es un argumento muy recurrente en los estudios ya nombrados sobre las motivaciones que llevan a buscar ser anónimo.

- El anonimato genera una sensación de protección en quien goza de su cobertura puesto que hace que no pueda rastrearse quien en la vida real es el emisor del mensaje. Si bien esto supone riesgos y problemáticas que deben enfrentarse, tal regulación debe tomar en cuenta esta arista positiva, puesto que actualmente existe un grupo importante de personas y transversal en la edad (el estudio de la Universidad de Carnegie Mellon tenía un foco más adulto, a diferencia del de Youth IGF y Childnet International) que requiere de este para poder alzar su voz en entornos complejos y/o aislados. Esto último se ha encontrado con nuevas trabas, debido, entre otros, a la actual tendencia de solicitar el uso de nombres reales para poder hacer uso de plataformas que permitan dejar comentarios en línea, comenzada a ser exigida por gigantes como Huffington Post o Facebook[41]. Una de las respuestas ante esta política indica que si bien es deseable controlar a los "trolls" de internet, eliminar el anonimato no es deseable en ningún caso, ello puesto que, dentro de varios motivos, los comentarios realizados en sitios web noticiosos por usuarios que utilizaban pseudónimos solían ser de una calidad superior que la de los sujetos que lo hacían con su nombre real[42]. El mismo hecho de ser fácilmente identificable y poder rastrear al emisor, disuade enormemente a este para manifestarse libremente, temiendo por las repercusiones que sus ideas puedan tener.

Derecho a Emitir y Recibir Información:

[40] Ibid., op. cit., p. 163.

[41] Para mayor información, visitar DARROW, B. "Huffington Post to End Anonymous Comments", 21 de Agosto de 2013. *Gigaom*. En línea, disponible en https://gigaom.com/2013/08/21/huffington-post-to-end-anonymous-comments/ [Fecha de consulta: 27 de octubre de 2015] y BEJERANO, P. "Facebook, Más Estricto con su Política de Nombres Reales", 18 de Septiembre de 2014. *El Diario.es*. En línea, disponible en: http://www.eldiario.es/turing/redes_sociales/facebook-nombre-real-drag-queen_0_303770449.html [Fecha de consulta: 27 de octubre de 2015]

[42] NAUGHTON, J. "Banish the Trolls but Web Debate Needs Anonymity", 25 de Agosto de 2013. *The Guardian*. En línea, disponible en http://www.theguardian.com/technology/2013/aug/25/web-trolls-anonymity-huffington-post [Fecha de consulta: 27 de octubre de 2015]

- El derecho a emitir información es crucial en aquellos casos en que las circunstancias sociales, familiares, laborales o políticas pueden generar una gran presión en el sujeto informante y condenarlo por dar a saber una situación en particular. En caso de encontrarse el periodista o informante en un contexto como aquellos, donde la represión es predecible, el anonimato es, sin lugar a dudas, imprescindible. Pero la utilidad del anonimato respecto a esta manifestación del derecho a la libertad de expresión no se agota allí, sino que es igualmente útil en otros aspectos de la libertad de emitir información.
- La Corte Interamericana de Derechos Humanos, refiriéndose a la actividad informativa, ha interpretado que no solo los controles o prohibiciones previas afectan al derecho a la libertad de expresión, sino que también las restricciones ilegítimas de condicionamientos indirectos impuestos a la búsqueda y recepción de informaciones[43]. Así, en el fallo *Bronstein, Ivcher vs. Perú,* la Corte expresó que: "Es fundamental que los periodistas que laboran en dichos medios gocen de la protección y de la independencia necesarias para realizar sus funciones a cabalidad, ya que son ellos los que mantienen informada a la sociedad, requisito indispensable para que ésta goce de una plena libertad"[44].
- De lo anterior se desprende, entonces, que el Estado no puede poner trabas previas de ningún orden ni tampoco entorpecer la actividad informativa. Entendiéndose de otro modo, se puede interpretar como el deber de dejar que se ejecuten labores periodísticas de forma libre y con los medios que se estimen adecuados, dado su alta relevancia social, sin perjuicio de las responsabilidades legales en caso de vulnerar el ordenamiento jurídico o de excederse de los límites tutelados por el derecho de la libertad de expresión.
- En relación al anonimato, hay dos puntos de especial consideración al tratar la vertiente informativa de este derecho humano: la reserva de fuentes periodísticas y los denunciantes o *whistleblowers*. Respecto al primer punto, en ciertos casos en que la persona entrevistada no quiera revelar su identidad para informar o dar su testimonio, aquello debe ser respetado. Varias constituciones y legislaciones dentro de la región han protegido

[43] GARCÍA, L. 2004. "La Protección de la Identidad de las Fuentes Periodísticas a la Luz de los Instrumentos Internacionales de Derechos Humanos y de los Estándares de sus Órganos de Aplicación" en *Anuario de Derecho Constitucional Latinoamericano*. Buenos Aires, Konrad-Adenauer-Stiftung y Centro Interdisciplinario de Estudios sobre el Desarrollo Latinoamericano (CIEDLA), v.10(2), p. 645.

[44] CORTE INTERAMERICANA DE DERECHOS HUMANOS, "*Ivcher Bronstein v Perú*". Sentencia de 24 de Septiembre de 1999, citada en GARCÍA, L. op.cit, loc. cit.

específicamente la reserva de fuentes[45]. Por otro lado, en países donde no cuenta con resguardo legal expreso, se ha construido tal obligación a partir del secreto profesional, como en el caso colombiano[46].

- Al igual que las limitaciones reconocidas por la Convención Interamericana de Derechos Humanos a la libertad de expresión, la reserva de fuentes, enmarcada dentro de este derecho, no es absoluta. Así, en caso que la información concedida por este individuo anónimo vulneren el respeto a los derechos o a la reputación de los demás o la protección de la seguridad nacional, el orden público o la salud o la moral públicas, en los términos de la convención, se podría solicitar que se dé a conocer su identidad.
- No obstante, en los casos en que no existan conflictos con los límites del derecho a la libertad de expresión, como ya se dijo, la Comisión Interamericana de Derechos Humanos en clara en su postura: "*La censura previa, interferencia o presión directa o indirecta sobre cualquier expresión, opinión o información difundida a través de cualquier medio de comunicación oral, escrito, artístico, visual o electrónico, debe estar prohibida por la ley. Las restricciones en la circulación libre de ideas y opiniones, como así también la imposición arbitraria de información y la creación de obstáculos al libre flujo informativo, violan el derecho a la libertad de expresión*"[47]. La prohibición de uso de fuentes reservadas por parte del Estado en aquellos casos en que tal utilización no entre en conflicto con el sistema legal es ilegítima y contraria a la convención, puesto que supone una creación de obstáculos al flujo informativo como también actúa como presión en el informante, quien teme de poder ser castigado por una narración supuestamente otorgada bajo el alero protector de la libertad de expresión.
- Un tipo de fuente anónima específica son los llamados *whistleblowers* (o "soplones"), individuos que llaman la atención y denuncian algún tipo de irregularidad que tiene lugar dentro de una organización, lo cual se puede manifestar de los siguientes modos: denunciar esta irregularidad ante los organismos legales o autoridades competentes, rehusarse a participar de dicho acto que se denuncia, prestar testimonio en el proceso legal o filtrando información y evidencia a la prensa sobre tales hechos[48]. Se ha justificado la

---

[45] Las Constituciones de Argentina, Brasil, Ecuador y Paraguay protegen la reserva de fuentes mientras que Chile, El Salvador, Panamá, Perú, Uruguay y Venezuela lo tutelan con rango legal. El detalle de esta lista fue extraído de UNITED NATIONS, op. cit., p. 17.

[46] TOBÓN-FRANCO, F. y VARELA-PEZZANO, E. op. cit., p. 134.

[47] COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, "Declaración sobre la Libertad de Expresión". En línea, disponible en https://www.cidh.oas.org/Basicos/Basicos13.htm [Fecha de consulta: 29 de octubre de 2015]

[48] NADLER, J y SCHULMAN, M. "*Whistle Blowing in the Public Sector*". 2006. Santa Clara University. En línea, disponible en

función de ellos indicando que si bien las personas tienen el derecho a acceder a información verídica, este debe ser complementado por el derecho a revelar información de interés público, incluyendo aquellos casos en que quien realiza tal exposición no podría hacerlo de forma pública[49].

- Usualmente, la utilidad de la práctica del *whistleblowing* se ha asociado al combate de la corrupción, fraude y malas prácticas[50], ya sea dentro de un entorno laboral, una empresa, una institución pública, entre otros. Adicionalmente, se ha sostenido que no solo debe asociarse el aporte que pueden realizar los *whistleblowers* respecto a los ámbitos anteriormente indicados, sino que también pueden cumplir un relevante rol en la denuncia y combate a la violaciones de derechos humanos[51].
- Actualmente, en Latinoamérica52 si bien Perú es el único país que, a nivel administrativo, protege expresamente a los *whistleblowers*, los países de la región cuentan con algún grado de tutela legal aplicables a estos, ya sea en la legislación penal o laboral, siendo Nicaragua el único país que no les proporciona protección alguna. La vigilancia en línea y problemas de privacidad que han surgido en el uso de internet ponen en serio riesgo a los *whistleblowers*. Frank La Rue señaló que los periodistas y *whistleblowers* requieren de especial protección, gozando sus comunicaciones de real privacidad, seguridad y anonimato53. En este sentido, el uso de programas de vigilancia por parte de los gobiernos del mundo y que aquellos informantes puedan ser objetivos específicos de interferencia estatal, puede derivar en un desincentivo a realizar una actividad legítima de denuncia por temor a las represalias legales (*chilling effect*).
- Pero no solo para quienes proveen información como fuente anónima es relevante el anonimato. Los periodistas también se ven beneficiados por este,

---

http://www.scu.edu/ethics/practicing/focusareas/government_ethics/introduction/whistleblowing.html#q1 [Fecha de consulta: 30 de octubre de 2015]

[49] HUMAN RIGHTS WATCH. 2013. "US: Statement on Protection of Whistleblowers in Security Sector". 18 de junio de 2013. *Human Rights Watch*. En línea, disponible en https://www.hrw.org/news/2013/06/18/us-statement-protection-whistleblowers-security-sector [Fecha de consulta: 31 de octubre de 2015]

[50] OECD. 2012. "*Study on Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation*". En línea, disponible en http://www.oecd.org/g20/topics/anti-corruption/48972967.pdf [Fecha de consulta: 30 de octubre de 2015], p. 4.

[51] HUMAN RIGHTS WATCH. op. cit., loc. cit.

[52] OEA, et al. 2013. "Latin American Meeting on Private Sector Responsibility in the Fight Against Corruption. Summary Report" en *Latin American Meeting on Private Sector Responsibility in the Fight Against Corruption*. 7-8 de Marzo 2013, Bogotá, Colombia. En línea, disponible en http://www.oas.org/juridico/PDFs/enc_summary.pdf [Fecha de consulta: 30 de octubre de 2015] p.6.

[53] NACIONES UNIDAS, Consejo de Derechos Humanos. 2013. "*Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*". En línea, disponible en http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf [Fecha de consulta: 31 de octubre de 2015], p. 14.

ya que les da la libertad suficiente para poder usar tal información, además de poder manifestar lo que ellos quieren, sin tener lineamientos, miedos ni barreras impuestas por una fuente plenamente identificada54. Por otro lado, existe otro argumento por el cual periodistas han encontrado la utilidad en ser anónimo: dirigir la discusión al contenido y no a quien lo emite. Quizás el mayor exponente de esto último es el conocido periódico The Economist, el cual se caracteriza porque sus artículos son anónimos o escritos tras un pseudónimo. Al revisar el sitio web de este medio55, explican que la elección por ocultar los nombres de sus contribuyentes responden a varios motivos (textos muy editados, cooperación entre más de un escritor, entre otros), pero que la razón principal para esto es, en palabras de un editor histórico del medio: "no es el maestro sino quien sirve a algo mucho mayor que incluso él mismo. Pueden llamar a esto culto a los ancestros, si así lo desean, pero le da a un periódico un increíble moméntum de línea de pensamiento y principios".

- The Guardian añade a lo anterior no solo una línea histórica de pensamiento de un medio donde grupo de personas han y seguirán contribuyendo a una empresa mayor, sino que también insiste en la utilidad del anonimato a la hora de informar como medio de dirigir la atención del lector a la sustancia y no al nombre de quien escribe56. Con ello se evita que el lector realice juicios ajenos a la calidad del aporte, como lo serían la fama del escritor, sus alineaciones ideológicas, sexo, edad, condición socioeconómica, entre otros.
- Además de lo anterior, está la igualmente importante arista pasiva: poder recibir y leer información de forma anónima. Al navegar por la red, vamos dejando rastros de nuestra actividad. Los sitios web usan "cookies", pequeños archivos de texto que los sitios visitados escriben y que se vinculan a nuestro disco duro, para así poder determinar si visitamos la página usualmente, qué clase de productos o información buscamos, entre otros datos57. A lo anterior, no solo las cookies recopilan datos, sino que también el navegador que usamos, el sistema operativo, las aplicaciones y

---

54 BOSUA, R, MILTON, S, et al. 2014. "Going Public: Researching External Whistleblowing in a New Media Age" en BROWN, A, et al (editores) *International Handbook on Whistleblowing Research*. Massachusetts, Edward Elgar Publishing Limited, p. 269.

55 About us. *The Economist*. En línea, disponible en http://www.economist.com/help/about-us [Fecha de consulta: 28 de octubre de 2015]. El original, en inglés, se expresa en los siguientes términos: "not the master but the servant of something far greater than himself. You can call that ancestor-worship if you wish, but it gives to the paper an astonishing momentum of thought and principle."

56 CLARK, T. 10 de enero de 2011. "Why Do Editorials Remain Anonymous?". *The Guardian*. En línea, disponible en http://www.theguardian.com/commentisfree/2011/jan/10/editorial-leading-article-anonymous [Fecha de consulta: 28 de octubre de 2015].

57 MACHRONE, B. 2000. "Cookies are Good, Bad, Good…" en *PC Magazine*. 22 de Febrero de 2000, p. 101.

extensiones, tanto en uso como desactivadas, también pueden filtrar información sobre nosotros, incluso los avisos publicitarios disponibles en internet58. Sumado a lo anterior, tenemos la obligación impuesta a gran parte de los servicios proveedores de internet del mundo por parte de la legislación penal de retener por cierto tiempo el historial de navegación de cada dirección IP asociada a su compañía y entregársela a las agencias gubernamentales que cumplan con los requisitos legales para solicitar dicho registro.

- Es por eso que el informe de David Kaye hace énfasis en la importancia del anonimato y de la cifrado para poder, entre otros, proveer a los individuos de los medios necesarios para proteger su privacidad y fortalecerlos para poder navegar y leer sin interferencias[59]. Ante las facultades y herramientas tecnológicas de las cuales dispone el Estado (y privados), el individuo debe poder contar con los medios para poder asegurar su anonimato de forma real, por tanto, no basta con solo usar un pseudónimo y cuentas de con datos falsos, sino que aquello debe ser acompañado por herramientas tales como VPNs, servicios de proxy, redes anónimas como Tor, entre otros[60].
- Cabe señalar, en todo caso, que actualmente ni las herramientas que se creían más idóneas para garantizar la privacidad de los usuarios de la red son impenetrables o totalmente seguras. En julio de 2015 un grupo de científicos encontraron una falla de seguridad en Tor que permite encontrar sus servidores (normalmente ocultos) con un 88 % de probabilidad[61]. Por tanto, siguiendo las conclusiones de Naciones Unidas, además de no restringir el derecho a navegar anónimo, los Estados igualmente deberían permitir el uso de este tipo de herramientas, apoyando a grupos más vulnerables en la implementación de las mismas y con los más altos estándares tecnológicos disponibles para así garantizar un anonimato real[62].
- No solo periodistas, activistas, artistas y miembros de grupos humanos especialmente vulnerables necesitan del anonimato para poder efectivamente ejercitar su derecho a la libertad de expresión. Los académicos e investigadores son un grupo de especial interés respecto de la vertiente de libertad de informarse e informar, ello en cuanto para poder desarrollar su

---

58 GILBERTSON, S. "Your Digital Fingerprint Makes You Easy to Track". *Wired*. 29 de Enero de 2010. En línea, disponible en www.wired.co.uk/news/archive/2010-01/29/your-digital-fingerprint-makes-you-easy-to-track [Fecha de consulta: 29 de octubre de 2015]

59 UNITED NATIONS, op. cit., loc cit.

60 Ibid., pp. 4-5.

61 RUSSON, M. "MIT Cracks Tor Anonymity Network and Identifies Hidden Servers with 88 % Accuracy". *International Business Times*. 30 de Julio de 2015. En línea, disponible en http://www.ibtimes.co.uk/mit-cracks-tor-anonymity-network-identifies-hidden-servers-88-accuracy-1513402 [Fecha de consulta: 29 de octubre de 2015]

62 UNITED NATIONS, op. cit., pp. 19-20.

trabajo es posible que tengan que investigar sobre temas sensibles o a grupos asociados a actividad criminal. Para evitar ser rastreados, perfilados e incluso detenidos[63] por sus búsquedas en la red respecto a su tema de estudio, estimamos que deben gozar de la misma protección que los grupos ya tratados.

Manifestaciones Artísticas:

- A lo largo de la historia de la humanidad, numerosos artistas han recurrido al anonimato o al uso de pseudónimos para llevar a cabo su obra, con el fin de denunciar, criticar o ironizar, sin ponerse en riesgo[64], tratando temas de la más variada índole, tales como: religión[65], política[66], reivindicar la posición de la mujer en la sociedad[67], expresión de grupos que normalmente no serían tomados en cuenta (como reos)[68], e, incluso, llamar la atención sobre desperfectos en la vía pública (con exitosos resultados)[69].
- El anonimato también es utilizado por artistas para poder publicar su trabajo sin sentir las presiones y expectativas que puede generar su fama previa[70]. Igualmente, músicos anónimos[71] han señalado como motivos para permanecer anónimos la autenticidad, que las miradas se dirijan a la calidad

---

[63] CURTIS, P y HOGDSON, M. "Student Researching al-Qaida Tactics Held for Six Days". 24 de mayo de 2008. *The Guardian*. En línea, disponible en http://www.theguardian.com/education/2008/may/24/highereducation.uk [Fecha de consulta: 29 de octubre de 2015]

[64] WALDEN, L. "The Anonymous Artist Leaving Empowering Notes for Women". Julio de 2015. *Dazen*. En línea, disponible en http://www.dazeddigital.com/artsandculture/article/25146/1/the-anonymous-artist-leaving-empowering-notes-for-women [Fecha de consulta: 01 de novimebre de 2015]

[65] MC DONALD, W. "Søren Kierkegaard (1813—1855)". *Internet Encyclopedia of Philosophy*. En línea, disponible en http://www.iep.utm.edu/kierkega/ [Fecha de consulta: 01 de noviembre de 2015]

[66] BROWN, J. "Anonymous Art: The Posters That Inspired the Uprising of 1968". 22 de octubre de 2011. *The Independent*. En línea, disponible en http://www.independent.co.uk/arts-entertainment/art/news/anonymous-art-the-posters-that-inspired-the-uprising-of-1968-795006.html [Fecha de consulta: 01 de noviembre de 2015]

[67] WALDEN, L. op. cit., loc cit.

[68] FINN, C. "The Power of Anonymous Art". 21 de agosto de 2007. *The Guardian*. En línea, disponible en: http://www.theguardian.com/artanddesign/artblog/2007/aug/21/thepowerofanonymousart [Fecha de consulta: 01 de noviembre de 2015]

[69] TELEGRAPH MEN. "Meet the Man Using Penises to Fill Potholes". 29 de abril de 2015. *The Telegraph*. En línea, disponible en http://www.telegraph.co.uk/men/the-filter/11570595/Meet-the-man-using-penises-to-fill-potholes.html [Fecha de consulta: 01 de noviembre de 2015]

[70] EL CONFIDENCIAL. "Escritores Tras la Máscara: El Seudónimo Vuelve a las Librerías". 22 de julio de 2013. *El Confidencial*. En línea, disponible en http://www.elconfidencial.com/cultura/2013-07-22/escritores-tras-la-mascara-el-seudonimo-vuelve-a-las-librerias_231278/ [Fecha de consulta: 01 de noviembre de 2015]

[71] FULTON, N. "The Curious Case of an Anonymous Artist". 08 de abril de 2015. *Cuepoint*. En línea, disponible en https://medium.com/cuepoint/the-curious-case-of-an-anonymous-artist-94c2aeb9a76d#.lgg8m22pq [Fecha de consulta: 01 de noviembre de 2015]

de la obra, más que a la persona del creador, tanto para evitar el culto al artista como para eludir críticas específicamente dirigidas a este.

Discusión Política y Fortalecimiento del Régimen Democrático:

- La importancia del derecho a la libertad de expresión en relación a la discusión política y pluralidad de opiniones como salvaguardia del régimen democrático es una de las más utilizadas a la hora de defender este derecho. En este sentido se pronunció la Comisión Interamericana de Derechos Humanos señalando que el efectivo ejercicio de la libertad de expresión es un instrumento indispensable para el funcionamiento de la democracia representativa, mediante la cual los ciudadanos ejercen su derecho a recibir, difundir y buscar información72, ligando a la participación política no solo con la emisión de opiniones sino también con el derecho a informar y ser informado.
- Internet ha tenido un gran efecto en la forma de ejercitar el derecho a la manifestación y participación política, ofreciendo nuevos canales o modificando los ya existentes, ya sea facilitando la capacidad de reunir corrientes de opinión en una estructura que disminuye los costos de transacción asociados a buscar, congregar y movilizar a dichas personas en el entorno material, como también ha generado un impacto en la apertura y expansión del mensaje que se quiere comunicar, liberándolo de barreras geográficas y pudiendo incluso hacerlo llegar a países extranjeros como también coordinar acción política a nivel transnacional[73].
- La Relatoría Especial para la libertad de expresión de la Comisión Interamericana ha subrayado la importancia del anonimato en relación a la libertad de expresión[74], indicando expresamente que la participación del debate público sin revelar la identidad del emisor es una práctica usual en las democracias modernas, por tanto, fortalecer el uso del anonimato favorece a dicha participación, en tanto los emisores pueden desplegar su opinión sin temer a las represalias injustas derivadas del ejercicio de este derecho fundamental. Igualmente, caracterizó a este derecho a ejercitar anónimamente la libertad de expresión del discurso como uno que va más allá de solo escribir notas de opinión o a participar de foros de debate en

---

72 COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS. "*Declaración de Principios sobre Libertad de Expresión*". En línea, disponible en https://www.cidh.oas.org/Basicos/Basicos13.htm [Fecha de consulta: 02 de noviembre de 2015].

73 ANDUIZA, E, CANTIJOCH, M y GALLEGO, A. 2009. "Political Participation and Internet: A Field Essay". *Universitat Autònoma de Barcelona*. En línea, disponible en http://llet-131-198.uab.es/grep/images/publications/Political_participation_internet.pdf [Fecha de consulta: 02 de noviembre de 2015], pp. 2-3.

74 COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial para la Libertad de Expresión. 2013. "*Libertad de Expresión e Internet*", pp. 63-64.

línea, sino que también conlleva la facultad de llamar a movilizaciones sociales, de convocar a otros individuos a manifestarse, organizarse políticamente o de cuestionar a las autoridades, incluso en caso de riesgo[75].

Resguardo ante la Vigilancia Masiva:

- Desde las revelaciones de Edward Snowden en 2013, hasta la filtración que dio a conocer el uso del software de Hacking Team en Latinoamérica el 2015[76], existe certeza de que actualmente diferentes gobiernos de la región cuentan con mecanismos digitales que permiten vigilar a la población. Por ello, como David Kaye hizo notar, el anonimato adquiere una gran relevancia ante este nuevo panorama, el cual puede producir efectos nocivos en el ejercicio del derecho a la libertad de expresión[77].
- El año 2013 tanto Naciones Unidas como la Relatoría Especial para la libertad de expresión de la Comisión Interamericana emitieron un pronunciamiento en conjunto sobre los programas de vigilancia masiva y sus consecuencias negativas en el ejercicio, promoción y resguardo de los derechos fundamentales. En aquella ocasión78, en resumidas cuentas, se expuso que la actividad de espionaje masivo va en detrimento del derecho a la libertad de expresión y que los Estados miembros deben disponer de medidas legales de resguardo a la población ante tal riesgo.
- Luego recalca la importancia de este derecho para el sistema democrático, por tanto, una injerencia al mismo debe realizarse sólo en circunstancias muy excepcionales y claramente definidas en la ley, además de estar justificadas en caso de existir un riesgo cierto a los intereses protegidos por la medida y cuando el daño que se busca evitar con la intrusión a este derecho sea superior y competa al interés superior de la sociedad[79].
- Finalmente, dichas medidas solo debieran estar dirigidas a estos casos especiales y fundamentados en la ley y en requisitos de necesidad y proporcionalidad. Dada su alta capacidad intrusiva, no deben ser usadas de forma clandestina, alejándose de su propósito original que los legitima, como lo sería destinarlos a realizar seguimiento de opositores políticos, periodistas

---

[75] Ibid., loc. cit.

[76] EL PAÍS. "Los Gobiernos de la Región Potencian su Capacidad de Espiar", 11 de julio de 2015. *El País.uy*. En línea, disponible en http://www.elpais.com.uy/informacion/gobiernos-region-potencian-capacidad-espiar.html [Fecha de consulta: 02 de noviembre de 2015].

[77] NACIONES UNIDAS. 2013., op. cit. p.4.

[78] NACIONES UNIDAS y ORGANIZACIÓN DE ESTADOS AMERICANOS. 2013. "*Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión*". En línea, disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&IID=2 [Fecha de consulta: 02 de noviembre de 2015].

[79] Ibid., op. cit., loc. cit.

o medios independientes80. A ello podemos sumar activistas, académicos e investigadores y, en general, cualquier persona que sea blanco de investigación y vigilancia únicamente por su postura personal sobre algún tema en particular.

8. La Regulación del Anonimato en Latinoamérica.

Luego de haber hecho una construcción general sobre el derecho a la libertad de expresión y del anonimato como condición para un real ejercicio y defensa del mismo, dirigiremos la atención hacia la regulación latinoamericana de este último, tanto aquellas que lo garantizan como las disposiciones que lo prohíben.

8.1. Protección del Anonimato

Se revisarán las disposiciones legales que supongan una protección expresa como indirecta al anonimato, así como también aquellas que lo protejan en algún ámbito en específico, como lo sería en las leyes de prensa. Así, el anonimato se resguarda en América Latina de acuerdo a las siguientes formas:

- Resguardo constitucional del anonimato: En las constituciones latinoamericanas no es posible encontrar alguna referencia a una protección amplia al anonimato en todas las circunstancias. No obstante, las cartas fundamentales de Argentina, Brasil y Paraguay revisten de resguardo constitucional a la protección de fuentes informativas, siendo esta la única manifestación del mismo presente.
- En Argentina, tal protección puede encontrarse en el artículo 43 de la Constitución el cual, en relación a la regulación de la acción de amparo, establece que si bien aquella puede interponerse para conocer los datos personales contenidos en registros públicos o privados, en ningún caso puede afectar la reserva de fuentes periodísticas[81].
- La Constitución federal brasileña, por su parte, si bien proscribe el anonimato considerándolo como un límite a la libertad de expresión, lo acepta excepcionalmente en el caso de las fuentes periodísticas. Así, en el título II, capítulo I, artículo 5 XIV establece que el acceso a la información es garantizado a todos y la confidencialidad de la fuente será resguardada, cada vez que aquello sea necesario para el desempeño de la labor profesional[82].

---

[80] Ibid., op. cit., loc. cit.

[81] KONRAD-ADENAUER-STITFUNG. "*Constitución de la Nación Argentina*". En línea, disponible en http://www.kas.de/upload/auslandshomepages/medioslatinos/argentina/argentina_constitucion.pdf [Fecha de consulta: 04 de noviembre de 2015]

[82] BRASIL, Cámara de Diputados. "*Constitución Federal de la República de Brasil*". 2010. En línea, disponible en http://english.tse.jus.br/arquivos/federal-constitution [Fecha de consulta: 04 de noviembre de 2015]

- Paraguay le otorga tutela a la reserva de fuentes en el artículo 29 de su carta fundamental, el cual establece que el ejercicio del periodismo, en cualquiera de sus formas, es libre y no está sujeto a autorización previa, para luego indicar que los periodistas de los medios masivos de comunicación social en cumplimiento de sus funciones, no serán obligados a actuar contra los dictados de su conciencia ni a revelar sus fuentes de información[83].

- Finalmente, si bien la Constitución ecuatoriana la protege en su artículo 20 indicando que el Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación [84], la modificación al reglamento de infracciones administrativas de la ley orgánica de comunicación que data de marzo de 2015, establece en su artículo quinto que los órganos públicos y particulares que deban entregar información a la Superintendencia de la Información y de la Comunicación en las investigaciones están obligados a hacer tal entrega en las denuncias que aquella tramite, incluso la información que está sujeta a reserva [85], introduciendo una excepción enorme a la garantía constitucional que ya ha tenido reacciones de preocupación provenientes de la sociedad civil[86].

- Protección al anonimato en leyes de prensa: Si bien no todos los países de la región le otorgan respaldo constitucional al anonimato respecto, al menos, a la reserva de fuentes, si existen disposiciones de resguardo al mismo de rango legal. Dentro de este listado, podemos incluir a Chile, Panamá, Uruguay y Venezuela.

- En Chile, la ley Nº 19.733 sobre libertades de opinión e información y ejercicio del periodismo[87] contiene dos artículos de particular relevancia. El primer artículo de esta ley señala que la libertad de emitir opinión y la de

---

[83] PARAGUAY, Convención Nacional Constituyente. "*Constitución Nacional*". 1992. En línea, disponible en http://www.oas.org/juridico/spanish/par_res3.htm [Fecha de consulta: 04 de noviembre de 2015]

[84] EL DIARIO. "Reserva de Fuentes Sería Vulnerada". 05 de abril de 2015. *El Diario*. En línea, disponible en http://www.eldiario.ec/noticias-manabi-ecuador/351804-reserva-de-fuente-se-veria-vulnerada/ [Fecha de consulta: 04 de noviembre de 2015]

[85] ECUADOR, Consejo de Regulación y Desarrollo de la Información y Comunicación. "*Reglamento de Infracciones Administrativas de la Ley Orgánica de Comunicación*". 2015. En línea, disponible en http://www.supercom.gob.ec/documents/Normativa/Reglamento%20Infracciones%20Administrativas%20Ley%20Organica%20De%20Comunicacion.pdf [Fecha de consulta: 04 de noviembre de 2015]

[86] FUNDAMEDIOS. "Cordicom Reforma Reglamento y Vulnera el Derecho a Reserva de Fuente". 01 de abril de 2015. *Fundamedios*. En línea, disponible enhttp://www.fundamedios.org/alertas/consejo-de-regulacion-reforma-un-reglamento-y-vulnera-el-derecho-la-reserva-de-la-fuente/ [Fecha de consulta: 04 de noviembre de 2015]

[87] CHILE, Ministerio Secretaría General de Gobierno. 2001. "*Ley Nº 19.733 Sobre Libertades de Opinión e Información y Ejercicio del Periodismo*". En línea, disponible en http://www.leychile.cl/Navegar?idNorma=186049 [Fecha de consulta: 05 de noviembre de 2015]

informar, sin censura previa, constituyen un derecho fundamental de todas las personas. Añade que el ejercicio de aquel incluye no ser perseguido ni discriminado a causa de las propias opiniones, buscar y recibir informaciones, y difundirlas por cualquier medio, sin perjuicio de responder de los delitos y abusos que se cometan, en conformidad a la ley. Como podemos ver, repite a nivel legal el derecho fundamental a la libertad de expresión constitucionalmente garantizado, además de profundizar en la extensión del mismo. El artículo 7º se refiere expresamente a la reserva de fuentes indicando que los directores, editores de medios de comunicación social, periodistas y alumnos de las escuelas de periodismo y los corresponsales extranjeros que ejerzan su actividad en Chile, tendrán derecho a mantener reserva sobre su fuente informativa, la que se extenderá a los elementos que obren en su poder y que permitan identificarla y no podrán ser obligados a revelar esta ni aun judicialmente. En el inciso que sigue, esta disposición extiende la aplicación de la reserva también a todos aquellos que por el ejercicio de su oficio o actividad informativa de cualquier clase hayan estado presentes al recibirse información sujeta a dicha protección.

- Panamá igualmente otorga protección legal expresa a la reserva de fuentes en la Ley Nº 22 de 200588, disponiéndose en el artículo 4 de la misma que el responsable de la información o la noticia difundida por los medios de comunicación social no estará obligado a revelar la identidad de su fuente, sin perjuicio de las responsabilidades en que incurra por sus afirmaciones.
- En Uruguay, la Ley Nº 16.099 que establece normativa referente a la libertad de expresión, opinión y difusión del año 200089, en su primer artículo se refiere de forma general a la libertad de comunicación de pensamientos y de información. Así, de manera similar a la ley chilena, comienza con un reconocimiento legal del derecho ya constitucionalmente consagrado, para luego especificar en su contenido. El inciso final de esta norma contempla la reserva de fuentes informativas anónimas en los siguientes términos: "Los periodistas tendrán el derecho a ampararse en el secreto profesional respecto, a las fuentes de información de las noticias que difundan en los medios de comunicación".

---

[88] PANAMÁ, Asamblea Nacional Legispam. 2005."*Ley Número 22 de 2005 Que Prohíbe la Imposición de Sanciones por Desacato, Dicta Medidas en Relación al Derecho a Réplica, Rectificación o Respuesta y Adopta Otras Disposiciones*". En línea, disponible en http://www.oas.org/juridico/spanish/mesicic2_pan_anexo_34_sp.pdf [Fecha de consulta: 05 de noviembre de 2015]

[89] URUGUAY, Comunicaciones e Informaciones. 2002. "*Ley Nº 16.099 Díctanse Normas Referentes a Expresión, Opinión y Difusión, Consagradas por la Constitución de la República*". En línea, disponible en http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=16099&Anchor= [Fecha de consulta: 05 de noviembre de 2015]

- Respecto a los *whistleblowers*, Perú es el único país de la región que les concede expresa protección, aun cuando lo hace a nivel administrativo y respecto de denuncias en el sector público[90]. El resto de los países contempla un grado de protección indirecto, el cual puede ser encontrado en legislación procesal penal (encubrimiento de testigos o respecto de la interposición de denuncias confidenciales o con reserva de identidad) y en leyes laborales, igualmente, sobre denuncias confidenciales[91].
- Todo lo anterior debe ser complementado con las disposiciones procesales penales que eximen del deber de prestar testimonio en virtud del secreto profesional, ampliamente presentes en las legislaciones latinoamericanas.
- Protección al anonimato en legislación sobre protección de datos personales: Las leyes de protección de datos personales de algunos gobiernos de la región incorporan medidas tendientes a anonimizar a la persona cuyos datos se tratan, imponiendo la obligación de llevar a cabo procesos de anonimización de los sujetos cuyos datos se recaban a la hora de tratar estos en determinados casos. Generalmente, es posible encontrar aquellas en las normativas más actualizadas y dictadas dentro de los últimos diez años. Si bien no es una regla general en la región, se presentan a continuación los casos en que existen garantías al anonimato expresas.
- En Argentina, el artículo 28 de la Ley Nº 25.326 sobre Protección de Datos Personales, al referirse a los trabajos de encuestas de opinión, mediciones y estadísticas, prospección de mercado, investigaciones científicas o médicas y otras actividades análogas dispone que no le serán aplicables esta ley protectora en tanto dicha información no pueda ser atribuible a persona determinada o determinable. Ahora, en aquellos casos -indica- en que no resulte posible el anonimato en el proceso de recolección informativa, se debe aplicar la técnica de la disociación, para que así no se pueda identificar persona alguna[92].

---

[90] PERÚ, Presidencia de la República. "*Decreto Supremo Nº 038-2011-PCM que aprueba el Reglamento de la Ley Nº 29542, Ley de protección al Denunciante en el Ámbito Administrativo y de Colaboración Eficaz en el Ámbito Penal*". En línea, disponible en http://www.contraloria.gob.pe/wps/wcm/connect/3aed82a7-c033-4c1f-bc29-1652b7b6bbf2/REGLAMENTO%2BLEY%2BDE%2BPROTECCI%C3%93N%2BAL%2BDENUNCIANTE.pdf?MOD=AJPERES [Fecha de consulta: 05 de noviembre de 2015]

[91] SILVESTRE, M.. " Protección de Denuncias de Actos de Corrupción. Alcances de las Estrategias en América Latina y Europa" en E*ncuentro Regional sobre Responsabilidad del Sector Privado en la Lucha Contra la Corrupción*, Bogotá, 7-8 de marzo de 2013. Presentación en Diapositivas en línea, disponible en http://www.oas.org/juridico/pdfs/enc_silvestre.pdf [Fecha de consulta: 05 de noviembre de 2015]

[92] ARGENTINA, Cámara de Diputados de la Nación. 2008. "*Ley Nº 25.326 Sobre Protección de Datos Personales Y Normas Reglamentarias y Complementarias*". En línea, disponible en http://www1.hcdn.gov.ar/dependencias/dip/textos%20actualizados/25326.010408.pdf [Fecha de consulta: 05 de noviembre de 2015]

- En Perú, la nueva ley de datos personales93 igualmente se pronuncia sobre anonimato, incorporando a los procesos de anonimización, definiéndolos a estos como el tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos, de forma irreversible. Para la regulación peruana, este proceso permite usar los datos recopilados más allá de la finalidad con la que se obtuvieron, así, si se quiere romper con este principio y tratar los fines con otros motivos o retenerlos con posterioridad al término de su uso original, ambas cosas pueden realizarse, pero con posterioridad a haberlos anonimizado por completo.

8.2. Prohibición del Anonimato

Si bien varios países latinoamericanos conceden protección a la reserva de fuentes periodísticas, algunos rechazan el anonimato en términos generales, llegando al punto de prohibirlo a nivel constitucional en algunos casos. No todos aquellos se refieren al anonimato de forma expresa, pero pueden tener efectos negativos sobre el mismo, como las medidas de registro obligatorio de teléfonos sujetos a servicios de prepago o de registro de tarjetas de transporte público, por enunciar algunos ejemplos.

Dentro de las fuentes formales del derecho en los países de la región, podemos encontrar los siguientes obstáculos al anonimato.

- Prohibición expresa del anonimato: Los tres ejemplos típicos al referirnos a esto son las legislaciones brasileña, venezolana y ecuatoriana, las cuales contemplan normativa expresa que prohíbe el discurso anónimo, en los dos primeros casos a nivel constitucional y en Ecuador, a nivel legal.
- La Constitución Federal Brasileña en su artículo 5º, inciso quinto, al regular la libertad de expresión, señala que "e*s libre la manifestación del pensamiento, quedando prohibido el anonimato*"[94]. La doctrina ha llamado la atención sobre la redacción de este punto, indicando que no da cuenta de un derecho y deber correlativo, sino que es más bien una limitación a la libertad de expresión[95]. Al respecto, se puede citar un fallo del año 2012 del Tribunal Superior de Justicia brasileño (RESP 1308830/RS) en el cual queda de manifiesto cómo funciona la prohibición del anonimato en dicho país. Así,

93 PERÚ, Congreso de la República. 2013. "*Ley Nº 29.733 de Protección de Datos Personales*". En línea, disponible en http://www.claro.com.pe/portal/recursos/pe/pdf/Ley29733.pdf [Fecha de consulta: 05 de noviembre de 2015]

94 KONRAD-ADENAUER-STITFUNG. "*Cláusulas de Libertad de Expresión: Brasil*". En línea, disponible en http://www.kas.de/upload/auslandshomepages/medioslatinos/brasil/clausulas_de_libertad_de_expresion_-_brasil.pdf [Fecha de consulta: 02 de noviembre de 2015]

95 DE SIQUEIRA, J. 2011. "Los Deberes Fundamentales y la Constitución Brasileña" en *Revista de Derecho*, v. XXIV (1), Julio 2011. En línea, disponible en http://www.scielo.cl/pdf/revider/v24n1/art03.pdf [Fecha de consulta: 02 de noviembre de 2015], p. 52.

este tribunal dictaminó que: "Al ofrecer un servicio mediante el cual se posibilita que los usuarios expresen libremente su opinión, el proveedor de contenido debe tener cuidado de propiciar los medios para que se pueda identificar a cada uno de esos usuarios, cohibiendo el anonimato y atribuyendo a cada manifestación una autoría cierta y determinada. Bajo la óptica de la diligencia general que se espera del proveedor, este debe adoptar todas las medidas que, de acuerdo con las circunstancias específicas de cada caso, estén a su alcance para la individualización de los usuarios del sitio web, so pena de responsabilización subjetiva por '*culpa in omittendo*'"[96].

- Como podemos ver, la prohibición del anonimato como límite al ejercicio del derecho a la libertad de expresión se aplica plenamente en la práctica, alcanzando a la manifestación de este en la red. Para el efectivo cumplimiento de la ley, los tribunales brasileños directamente han exigido a las empresas disponer de su capacidad técnica para cumplir con dicha prohibición, como lo sería hacer que tomen las medidas adecuadas para identificar a los usuarios o sacar de circulación e inhabilitar el uso de un software por contravenir este mandato constitucional.
- En relación a esto último, un caso reciente es el requerimiento hecho por la justicia brasileña a Google, Microsoft y Apple de retirar aplicaciones móviles que permitían comunicarse de forma anónima[97]. Además de lo anterior, se solicitó a dichas compañías que debían borrar dicho software de todos los teléfonos en los cuales se instalaron. Respecto de la aplicación Secret (respecto a la cual se condenó a Google y Apple), el juez civil Paulo Cesar de Carvalho, quien conoció de la causa, señaló que: "La libertad de expresión no constituye un derecho absoluto, siendo numerosas las hipótesis en que su ejercicio entra en conflicto con otros derechos fundamentales o bienes jurídicos colectivos protegidos constitucionalmente, las que serán resueltas mediante una ponderación de intereses en juego, a modo de garantizar el derecho a la honra, privacidad, igualdad y dignidad humana y, asimismo, proteger la infancia y adolescencia (...)" [98] . Ello se decidió también considerando que este tipo de aplicaciones de chat se usarían para *bullying* escolar, dirigiendo el razonamiento solo al aspecto negativo del uso del

[96] JAPIASSÚ, C y DE SOUZA, R. 2013. "Informe de Brasil en Coloquio Preparatorio Sección IV. Helsinki (Finlandia), 10-12 de junio de 2013" en Revista Electrónica de la AIDP 3(1). En línea, disponible en http://www.penal.org/sites/default/files/files/RH%20-3.pdf [Fecha de consulta: 02 de noviembre de 2015]

[97] COTTRELL, L. "Brazil Enforcing Ban on Anonymity". 20 de agosto de 2014. *The Privacy Blog*. En línea, disponible en http://www.theprivacyblog.com/international/brazil-enforcing-ban-on-anonymity/ [Fecha de consulta: 02 de noviembre de 2015]

[98] G1. "Justiça do ES Determina Remoção do Secret de Lojas de Aplicativos no Brasil". 20 de agosto de 2014. *Globo.com*. En línea, disponible en http://g1.globo.com/tecnologia/noticia/2014/08/justica-do-es-determina-remocao-do-secret-de-lojas-de-aplicativos-no-brasil.html [Fecha de consulta: 02 de noviembre de 2015]

anonimato y no sus beneficios. La aplicación que se solicitó que Microsoft sacase de su tienda, Cryptic, también consistía en un servicio de mensajería anónimo y encriptado. En ambos casos de prohibición de uso de software de comunicaciones, podemos ver el nexo en común: búsqueda del anonimato en comunicaciones privadas.

- En 2014, Brasil dictó la ley que establece principios, garantías, derechos y deberes para el uso de internet en Brasil, ampliamente conocida como "ley marco civil de internet", de gran relevancia para la región por garantizar tanto la neutralidad en la red como los derechos a la libertad de expresión y privacidad en línea, reconociendo a estos como principios de internet[99]. Lamentablemente, la prohibición constitucional al anonimato, hoy en día, afecta enormemente a la plena realización de dichos principios, como ya se ha expuesto.
- Venezuela, utilizando un modelo similar, trata la prohibición del anonimato a nivel constitucional. En este sentido, el artículo 57 de la carta fundamental de la República Bolivariana de Venezuela estipula que: "Toda persona tiene derecho a expresar libremente sus pensamientos, sus ideas u opiniones de viva voz, por escrito o mediante cualquier otra forma de expresión, y de hacer uso para ello de cualquier medio de comunicación y difusión, sin que pueda establecerse censura. Quien haga uso de este derecho asume plena responsabilidad por todo lo expresado. No se permite el anonimato, ni la propaganda de guerra, ni los mensajes discriminatorios, ni los que promuevan la intolerancia religiosa"[100]. De este modo, al igual que la Constitución brasileña, la prohibición se encuentra justo después de reconocer el derecho a la libertad de expresión, como límite a su ejercicio.
- La jurisprudencia venezolana ha establecido la forma en que procede esta prohibición al anonimato, fallando que sólo actúa como límite al derecho a la libertad de expresión, siendo, por tanto, permitido el anonimato respecto a otros derechos y circunstancias, como un proceso penal, por ejemplo[101].

---

[99] CONGRESO INTERACTIVO. "Traducción al Castellano del Marco Civil de Internet de Brasil". *Congreso Interactivo*. En línea, disponible en http://blog.congresointeractivo.org/traduccion-al-castellano-del-marco-civil-de-internet-de-brasil/ [Fecha de consulta: 03 de noviembre de 2015]

[100] KONRAD-ADENAUER-STITFUNG. "*Cláusulas de Libertad de Expresión: Venezuela*". En línea, disponible en http://www.kas.de/upload/auslandshomepages/medioslatinos/venezuela/clausulas_de_libertad_de_expresion_-_venezuela.pdf [Fecha de consulta: 02 de noviembre de 2015]

[101] REPÚBLICA BOLIVARIANA DE VENEZUELA. Circuito Judicial Penal del Estado de Zulia, Corte de Apelaciones, Sala Primera. 2009. Ponencia de la Jueza Profesional Jacquelina Fernández González en "Asunto VP02-R-2009-000134". En línea, disponible en http://zulia.tsj.gob.ve/decisiones/2009/junio/588-1-VP02-R-2009-000134-229-09.html [Fecha de consulta: 02 de noviembre de 2015]

- En sintonía con el mandato constitucional, la ley venezolana de responsabilidad social en radio, televisión y medios electrónicos de 2004 (también conocida como "ley resorte") contempla en su artículo 29 sobre suspensión y revocatoria, donde están las conductas prohibidas por esta ley, así como su sanción en específico. Dentro de las infracciones se considera la difusión de mensajes anónimos[102].
- Finalmente, Ecuador es otro país en el cual se prohíbe el anonimato, pero esta vez no a nivel constitucional, sino que en la Ley Orgánica de Comunicaciones de 2013. Su artículo 20 contempla que los comentarios formulados al pie de las publicaciones electrónicas de los medios de comunicación en internet deben contar con registros de los datos personales de quienes emiten dichas opiniones para poder identificarlos, así, deben solicitarse datos como nombre, correo electrónico, cédula de identidad o ciudadanía, además de implementar mecanismos para denunciar y eliminar los comentarios que lesionen los derechos garantizados en la constitución y la ley. De no cumplirse con lo anterior, los medios de comunicación serán responsables civil, penal y administrativamente por los comentarios[103].
- Esto ha llevado que el periódico El Comercio de Ecuador, con posterioridad a la entrada en vigencia de esta ley, haya suprimido la sección de comentarios debido a una supuesta amenaza por parte del Presidente de la República, quien habría protestado por comentarios críticos respecto a su gestión o insultos dirigidos a él, realizados a través de dicho medio. Ante dicho reclamo, el periódico manifestó negarse a borrar comentarios y a prohibir la libre manifestación de sus lectores, por tanto, hicieron pública su decisión de clausurar dicha sección, hasta encontrar una fórmula que permita el flujo libre de ideas, evitando los excesos verbales[104].
- Pero el actuar gubernamental no ha afectado únicamente a medios de comunicación tradicionales, sino que también a individuos que a través de las redes sociales hacen público su malestar y oposición al gobierno. Videos en Youtube, comentarios en Facebook y Twitter (además de la supresión de cuentas de todos estos sitios) comenzaron a desaparecer luego de la entrada

---

[102] REPÚBLICA BOLIVARIANA DE VENEZUELA, Asamblea Nacional. 2004. "*Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos*". En línea, disponible en http://www.nci.tv/archivos/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electr%C3%B3nicos.pdf [Fecha de consulta: 03 de noviembre de 2015]

[103] ECUADOR, Asamblea Nacional. "*Ley Orgánica de Comunicación*". 25 de junio de 2013. En línea, disponible en http://www.cncine.gob.ec/imagesFTP/63228.5_LEY_ORGANICA_COMUNICACION.pdf [Fecha de consulta: 02 de noviembre de 2015]

[104] EL TIEMPO. "El Comercio de Ecuador Suspende Comentarios en Internet por Amenazas". 30 de septiembre de 2012. *El Tiempo*. En línea, disponible en http://www.eltiempo.com/archivo/documento/CMS-12268162 [Fecha de consulta: 03 de noviembre de 2015]

en vigencia de la ley de comunicaciones, indicándose que se han valido de mecanismos de todo tipo: acosadores en redes sociales, bajada de contenido alegando infracciones a la ley de propiedad intelectual, creación de portales de denuncia de contenido en línea que se considera "abusivo" y responder a tales mensajes, además de por cadena televisiva hacer públicos los datos de identificación personal de los responsables tras cuentas de redes sociales abiertamente críticas de la administración ecuatoriana[105][106].

- Quizás el caso más polémico de los últimos años es el de "Crudo Ecuador", cuenta satírica de Facebook famosa por ser abiertamente opositora al gobierno del Presidente de la República de dicho país. En el punto más álgido de las tensiones entre el opositor y el gobierno ecuatoriano, recibió un ramo de flores en su casa, el cual fue interpretado como un acto de amenaza a la integridad física tanto de él como de su familia. Posteriormente, Crudo Ecuador publicó en la red una nota en la cual señala a Rafael Correa que ganó y que pondría fin a dicha cuenta, cerrándola[107].
- La Relatoría Especial sobre Libertad de Expresión de la Comisión Interamericana se pronunció expresamente sobre este caso, condenándolo como acto de estigmatización en contra de Crudo Ecuador, además de criticar los dichos del mandatario ecuatoriano en repetidos capítulos del programa televisivo "Enlace Ciudadano" en los cuales, además de criticar la actividad en línea de esta cuenta como de otros usuarios más, instó a la ciudadanía a ayudar a descubrir la identidad de estos sujetos y exponerlas públicamente. Igualmente, pidió que se garantizara la seguridad de Crudo Ecuador[108].
- En Cuba, en tanto, existen limitaciones al cifrado. Si bien en Cuba no existe una prohibición expresa sobre el anonimato como en los casos anteriormente

---

[105] BERTONI, E y VIVANCO, J. "La Censura en Ecuador Llegó a Internet". 15 de diciembre de 2014. *El País*. En línea, disponible en http://elpais.com/elpais/2014/12/12/opinion/1418385250_354771.html [Fecha de consulta: 03 de noviembre de 2015]

[106] DIARIO DE CUBA. "Rafael Correa Busca Presionar a Detractores a Través de Redes Sociales". 05 de febrero de 2015. *Diario de Cuba*. En línea, disponible en http://www.diariodecuba.com/internacional/1423094745_12710.html [Fecha de consulta: 03 de noviembre de 2015]

[107] HIGUERA, S, "Críticas del Presidente de Ecuador y Amenazas de Muerte Llevan al Cierre de Cuenta Satírica de Facebook". 27 de febrero de 2015. *Journalism in the Americas, the University of Texas at Austin*. En línea, disponible https://knightcenter.utexas.edu/es/blog/00-15945-amenazas-de-muerte-y-criticas-del-presidente-de-ecuador-llevan-al-cierre-de-cuenta-sat [Fecha de consulta: 03 de noviembre de 2015]

[108] ORGANIZACIÓN DE ESTADOS AMERICANOS, Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. 2015. "*Press Release R 17/15 The Office of the Special Rapporteur Urges Ecuador to Ensure the Safety of the Citizen "Crudo Ecuador" and Expresses Concern Regarding Comments Made by Higher Authorities*". En línea, disponible en "http://www.oas.org/en/iachr/expression/showarticle.asp?artID=979&lID=1 [Fecha de consulta: 03 de noviembre de 2015]

expuestos, la Resolución 179/2008 sobre Proveedores de Internet al Público, modificada el año 2011 por la Resolución 102/2011, en su artículo 19, enumera las obligaciones de dichos proveedores, estableciendo en la letra e de dicha disposición que "para la utilización de cualquier tipo de aplicación que implique el encriptamiento de la información a transmitir, es requisito tramitar la aprobación, de conformidad con lo establecido por las disposiciones vigentes que lo regulan"109. Así, es el Ministerio del Interior quien evaluará si concede o no tal autorización.

- Las prohibiciones al anonimato no solo tienen una manifestación digital, sino que también en fuera de este. Colombia[110], Brasil[111] y Chile[112], por citar algunos países, han proscrito o han intentado prohibir el uso de máscaras u otro tipo de coberturas faciales en protestas. Aunque eso puede tener repercusiones en el ejercicio del anonimato y la libertad de expresión en línea, como lo sería, por ejemplo, subir un video a la red en la cual se difunda un mensaje de protesta.
- Registro de teléfonos prepago: Actualmente, los teléfonos celulares no solo sirven para realizar llamadas y enviar mensajes de texto sino que la forma de comunicarse a través de aquellos se ha desplazado a los servicios y aplicaciones en línea como correo electrónico, servicios de mensajería a través de internet, telefonía en línea y redes sociales. Por tanto, las preocupaciones sobre anonimato en línea y libertad de expresión se aplican plenamente respecto de estos dispositivos.
- Desde los atentados terroristas ocurridos en el hemisferio norte a inicios de la década anterior (Nueva York, Londres y Madrid) es posible notar una tendencia global a implementar obligaciones de registro de teléfonos sujetos a servicios de prepago, puesto que se asocia el uso de dichos servicios anónimos a la comisión de crímenes de alta peligrosidad e impacto social como lo son el terrorismo, pornografía infantil, tráfico de sustancias

---

109 CUBA, Ministerio de la Informática y las Comunicaciones. 2011. "*Resolución 102/2011*". En línea, disponible en http://www.di.sld.cu/documentos/resol/resol_102_2011.pdf [Fecha de consulta: 03 de noviembre de 2015]

110 REDACCIÓN JUSTICIA. "Usar Capucha en Protestas Será Agravante en Judicialización". 11 de septiembre de 2013. *El Tiempo*. En línea , disponible en http://www.eltiempo.com/archivo/documento/CMS-13058400 [Fecha de consulta: 04 de noviembre de 2015]

111 EFE. "Aprueban Ley en Brasil que Prohíbe Usar Máscaras en Protestas". 10 de septiembre de 2013. *Excelsior*. En línea, disponible en http://www.excelsior.com.mx/global/2013/09/10/918024 [Fecha de consulta: 04 de noviembre de 2015]

112 PIQUIER, A. "¿Qué Significa la Ley Hinzpeter?". *Acuerdos.cl*. En línea, disponible en http://acuerdos.cl/columna/que-significa-la-ley-hinzpeter/ [Fecha de consulta: 04 de noviembre de 2015]

estupefacientes ilícitas y crimen organizado113. Así, todos los usuarios de servicios de telecomunicaciones, tanto sujetos a plan mensual como prepago, quedan plenamente individualizados, ligándose cada equipo a un usuario en particular. A esto debe añadirse la obligación impuesta a los ISP de registrar el tráfico de navegación de las direcciones IP y podemos saber con certeza qué sitios visita cada teléfono y toda la información relativa a la utilización de software de comunicación a través de la red, además del uso de las funciones de telefonía mismas.

- En varios países de América Latina existe este mandato legal, en otros se discute su implementación, en México se derogó y en otros si bien no existe, están presentes otras normas imperativas que a final de cuentas producen efectos similares.

- Colombia es de aquellos países en donde el registro de tarjetas SIM de todos los teléfonos móviles es obligatorio, justificando tal política pública para generar una lista tanto de los aparatos inscritos como una lista negra con los equipos robados, debiendo entregar los siguientes datos: Cédula de identificación, nombre, dirección y número de contacto[114], lista de datos que deben recoger (además de añadir las especificaciones técnicas del equipo como el número telefónico, IP, flota) todas las empresas de telecomunicaciones a la hora de habilitar un servicio de dicha categoría, información que posteriormente debe ser entregada a la policía[115].

- Ecuador comenzó a aplicar la obligación de registro a partir del año 2014116, respecto de teléfonos móviles de prepago como de aquellos sujetos a pago mensual. Al igual que el caso colombiano, los motivos esgrimidos para fundamentar esta medida están relacionados a combatir el robo de equipos. En este registro se recopilaran los siguientes datos: nombre completo del usuario, número de cédula de identidad, ciudadanía o pasaporte y domicilio, añadiendo la razón social en caso de tratarse de personas jurídicas.

---

[113] CENTRE FOR POLICY RESEARCH ON SCIENCE AND TECHNOLOGY SIMON FRASER, UNIVERSITY OF VANCOUVER. 2006. "*Privacy Rights and Prepaid Communications Services*". En línea, disponible en http://www.sfu.ca/cprost-old/prepaid/docs/Gow-PrivacyRightsAndPrepaidCommunicationServices.pdf [Fecha de consulta: 03 de noviembre de 2015], pp. 1-3.

[114] COLOMBIA, Ministerio de la Información y de las Comunicaciones. 2011. "*Decreto Número 1630 de 2011*". En línea, disponible en http://www.mintic.gov.co/portal/604/articles-3558_documento.pdf [Fecha de consulta: 03 de noviembre de 2015]

[115] COLOMBIA, Ministerio de Defensa Nacional. 2009. "*Resolución 912 de 2008*". En línea, disponible en https://www.redjurista.com/documents/r_mdef_0912_2008.aspx [Fecha de consulta: 03 de noviembre de 2015]

[116] ECUADOR, Arcotel. 2013. "C*odificación de la Norma que Regula el Procedimiento para el Empadronamiento de Abonados del Servicio Móvil Avanzado (SMA) y Registro de Terminales Perdidos, Robados o Hurtados*". En línea, disponible en http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/codificacion_norma_empadronamiento.pdf [Fecha de consulta: 03 de noviembre de 2015].

- Guatemala es, quizás, uno de los países de la región con la realidad más compleja. Al igual que en los dos casos previos, se aprobó una ley de registro de teléfonos celulares el año 2013, con la cual se buscaba combatir el alza en los robos de estos dispositivos, además de establecer duras penas en caso de cometer dicho ilícito (hasta quince años de prisión)117. Esta ley118 exige que, para registrar el equipo móvil, el sujeto debe entregar los siguientes datos: nombre completo, cédula de identidad, dirección y ubicación del punto de venta, número de identificación tributaria, solicitando igualmente datos similares a las personas jurídicas. En Guatemala no existe una ley de protección de datos, solo una iniciativa legal que aún no se aprueba, por tanto, una ley que crea una base de datos personales sin disponer la ciudadanía de legislación de resguardo ante posibles abusos o uso indebido de dicha información es algo que no deja de causar preocupación.
- En Perú el proceso de identificación de los equipos móviles sujetos a servicios de prepago comenzó el año 2010 con el Decreto Supremo 024-2010 MTC que aprueba el procedimiento para la subsanación de la información consignada en el registro de abonados pre pago, el registro de los mismos se justificó en el uso delictivo que puede darse a estas líneas anónimas119. De forma similar a las legislaciones comparadas, el registro se hace al momento de contratar el servicio, solicitándose el nombre completo, documento de identidad y número telefónico del titular del teléfono. Resulta preocupante que a partir de este año no solo basta con la obligación de registro anteriormente descrita sino que también se exige un registro biométrico de cada equipo, arguyendo que esto es necesario para el combate de la actividad criminal120. La proporcionalidad de la medida respecto del fin que se busca con ella es discutible, considerado que acá se tiene una plena identificación de cada usuario.

---

117 LÓPEZ, J. "APROBADA Ley contra Robo de Celulares". 17 de septiembre de 2013. *Publinews*. En línea, disponible en http://www.publinews.gt/nacionales/aprobada-ley-contra-robo-de-celulares/bQDmiq---cdCSvxjJZzBaM/ [Fecha de consulta: 03 de noviembre de 2015]

118 GUATEMALA, 2013. "*Decreto Número 8-2013. Ley de Equipos Terminales Móviles*". En línea, disponible en: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2013/pdfs/decretos/D08-2013.pdf [Fecha de Consulta: 03 de noviembre de 2015]

119 PERÚ, Presidencia de la República. 2010. "*Decreto Supremo Nº 024-2010-MTC que Aprueba el Procedimiento para la Subsanación de la Información Consignada en el Registro de Abonados Pre Pago*". En línea, disponible en transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_1902.pdf [Fecha de consulta: 04 de noviembre de 2015]

120 TV PERÚ. "Inició Registro Biométrico para Líneas Prepago: Sepa más del 'Apagón Telefónico'". 05 de junio de 20145. *TV Perú*. En línea, disponible en www.tvperu.gob.pe/informa/nacional/inicio-registro-biometrico-lineas-prepago-como-sera-apagon-telefonico [Fecha de consulta: 04 de noviembre de 2015]

- Chile no tiene ley sobre registro obligatorio de tarjetas SIM y equipos telefónicos de prepago, pero actualmente se están discutiendo en el Congreso Nacional dos proyectos de ley que buscan instaurarlo, uno proveniente de la Cámara de Diputados[121] y otro del Senado[122].
- Brasil tampoco exige legalmente la inscripción de teléfonos obligatoria, la agencia nacional de telecomunicaciones (ANATEL) en la Regulación Nº 477 de 2007 que contiene el reglamento de servicio móvil personal123. En los artículos 42 y 53 de la misma, respectivamente, se exige a la empresa de telecomunicaciones que presta el servicio de telefonía móvil que deben conservar el nombre, cédula de identidad y dirección del abonado. Cabe señalar que al igual que Guatemala, en este país tampoco existe una ley de protección de datos personales.
- Como contrapunto a los casos enunciados, está el caso mexicano donde en 2009 comenzó a regir el registro obligatorio de tarjetas SIM, en agosto de 2011 se puso fin a dicha medida por varios motivos, entre ellos124: no ayudó a disminuir la comisión de la clase de delitos que se buscaban combatir estableciendo tal medida, es más, la tasa de aquellos aumentó mientras estuvo vigente; hubo muchos problemas en la práctica para implementar el registro de forma óptima, muchas veces siendo las compañías de telecomunicaciones incapaces de comprobar con veracidad si la información concedida por los clientes era real; además, había pocos incentivos a los privados para procurar la calidad y veracidad de tales datos. Además, se subestimó la capacidad de los delincuentes, quienes recurrieron a otros métodos para realizar llamadas anónimas (roaming, mercado negro de tarjetas SIM y aumento del robo de teléfonos celulares, los cuales eran posteriormente usados para coordinar actividad criminal, por señalar algunos ejemplos) y se subestimaron los riesgos creados para los usuarios, cuyos datos podrían ser accedidos de forma fraudulenta en cualquier momento. Es clave la experiencia mexicana, considerando que ella fue implementada

---

[121] Este puede ser encontrado en el siguiente enlace http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=9767-15 [Fecha de consulta: 04 de noviembre de 2015]

[122] Este puede ser encontrado en el siguiente enlace http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=9894-15 [Fecha de consulta: 04 de noviembre de 2015]

[123] BRASIL, ANATEL. "*Resolução nº 477, de 7 de agosto de 2007 que Aprova o Regulamento do Serviço Móvel Pessoal – SMP*". En línea, disponible en http://www.anatel.gov.br/legislacao/resolucoes/2007/9-resolucao-477 [Fecha de consulta: 04 de noviembre de 2015]

[124] GSMA. 2013. "The Mandatory Registration of Prepaid SIM Card Users". En línea, disponible en http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf [Fecha de consulta: 04 de noviembre de 2015]. p. 11.

prácticamente por los mismos motivos que en los otros países de la región y que no dio resultados positivos, restando de idoneidad a estas para obtener los fines buscados.

- Registros de tarjetas de identificación, transporte y datos biométricos: Como ya pudimos ver en el caso peruano sobre datos biométricos y registro de teléfonos celulares, existe una tendencia en Latinoamérica a recolectar una serie de datos de la población en los más diversos ámbitos y servicios.

- El año 2011 en Argentina se presentó el SIBIOS, un software de sistema automatizado de huellas digitales que, en cooperación con el Registro Nacional de Personas, permitirá a las fuerzas nacionales contar con información que individualice a todos los ciudadanos, buscando dar apoyo en la investigación criminal, procesando tanto dichas huellas como las fotografías de cada uno de los individuos[125]. Esta situación se hace más compleja cuando se analizan los otros cruces de información que se realizan, así, la modificación a la cédula de identidad argentina (la cual será el único documento de identificación a partir de 2016) añadió dos chips a estas, los cuales permiten asociar los vínculos familiares, historial clínico, datos de seguridad y apoyo social, la tarjeta de transporte público y su conectividad a internet[126]. Paralelamente, se está tramitando la provincia de Buenos Aires la puesta en marcha de un registro de ADN de la población[127]. Esta clase de medidas, si bien se refiere a la acumulación de información sobre ciudadanos ya identificados, hace cada vez más difícil el ejercicio del anonimato, al aumentar los factores de posible identificación de quien pretenda permanecer en el anonimato.

- Paraguay, en una línea similar, busca implementar dentro del plazo de un año un sistema de tarjeta magnética de transporte público nominal e intransferible, con el cual se permitirán conocer los viajes realizados por cada uno de los pasajeros[128].

---

[125] MINISTERIO DE SEGURIDAD, "La Presidenta Presentó el SIBIOS". 07 de noviembre de 2011. *Ministerio de Seguridad*. En línea, disponible en http://www.minseg.gob.ar/la-presidenta-present%C3%B3-el-sibios [Fecha de consulta: 04 de noviembre de 2015]

[126] DIARIO HOY. "El Nuevo DNI de Randazzo en la Mira: Privacidad en Peligro". 30 de junio de 2014. *Diario Hoy*. En línea, disponible en http://diariohoy.net/politica/el-nuevo-dni-de-randazzo-en-la-mira-privacidad-en-peligro-30932 [Fecha de consulta: 04 de noviembre de 2015]

[127] BEA, "Avanza en la Legislatura de la Provincia de Buenos Aires un Proyecto para Registro Compulsivo de ADN". 15 de septiembre de 2015. *Fundación Vía Libre*. En línea, disponible en http://www.vialibre.org.ar/2015/09/15/avanza-en-la-legislatura-de-la-provincia-de-buenos-aires-un-proyecto-para-registro-compulsivo-de-adn/ [Fecha de consulta: 04 de noviembre de 2015]

[128] http://www.abc.com.py/nacionales/privacidad-esta-garantizada-1408393.html [Fecha de consulta: 04 de noviembre de 2015]

- Por otro lado, gobiernos como el mexicano129 y el peruano130, han dictado leyes sobre geolocalización, permitiendo ambas ubicar los teléfonos que estén involucrados en actividad criminal, sin ser necesaria una orden judicial previa.
- El requisito de legalidad parece cumplirse, concentrándose los problemas de estas medidas en relación a la idoneidad y proporcionalidad entre el detrimento causado al anonimato y libertad de expresión y los objetivos perseguidos con aquellas. Mas existe una segunda arista problemática: el riesgo de acceso ilegítimo y posterior filtración de la información contenida en aquellas bases de datos estatales, tal y como ya ha acaecido131. Ante la carencia de leyes de protección de datos en algunos países de la región, como ya vimos, además de legislaciones anquilosadas en otros, dejan a los usuarios en un panorama de desprotección.
- En suma, los mandatos legales de recolección y creación de bases de dato no solo son cuestionables desde una perspectiva netamente jurídica, sino que también hay que mirarlas con detención desde la óptica de la seguridad informática. Dichas bases no son totalmente seguras e inaccesibles, y disponer de tales volúmenes de información de la ciudadanía y concentrada y asociada entre sí, también puede someter a altos riesgos a la población en caso que ella sea obtenida, utilizada y filtrada por terceros que no debieran tener acceso a la misma.

9. Conclusiones y Recomendaciones

Las tecnologías digitales han influido de gran manera en la forma que ejercemos nuestro derecho a la libertad de expresión, así como también, han permitido la elaboración de nuevos métodos de entorpecer o hacer ilusoria su puesta en práctica.

Dado el alto poder penetrador de aquellas en la intimidad del sujeto, por primera vez en la historia de la humanidad tanto gobierno como privados tienen a su disposición las herramientas técnicas para observar, analizar y predecir las conductas de los

---

[129] FORBES STAFF. "¿De qué va la Ley de Geolocalización?". 16 de enero de 2014. *Forbes México*. En línea, disponible en http://www.forbes.com.mx/de-que-va-la-ley-de-geolocalizacion/ [Fecha de consulta: 04 de noviembre de 2015]

[130] PERÚ, Presidencia de la República. "Decreto Legislativo Nº 1182". 27 de julio de 2015. En línea, disponible en http://www.elperuano.com.pe/NormasElperuano/2015/07/27/1268121-1.html [Fecha de consulta: 04 de noviembre de 2015]

[131] MUÑOZ, D. "Registro Civil Denuncia Copia Irregular de Bases de Datos de Carnés y Pasaportes". 22 de marzo de 2014. *La Tercera*. En línea, disponible en http://www.latercera.com/noticia/nacional/2014/03/680-570673-9-registro-civil-denuncia-copia-irregular-de-bases-de-datos-de-carnes-y-pasaportes.shtml [Fecha de consulta: 04 de noviembre de 2015]

miembros de la sociedad. Lo anterior no solo afecta al derecho a la privacidad, sino también a la libertad de expresión. Un sujeto que sabe que su actividad en línea está siendo rastreada y que es plenamente identificable por estas instituciones, inevitablemente afectan su comportamiento en línea, pensando muy bien qué información va a buscar, con quién se comunicará o qué manifestará.

Es por ello que importantes organismos internacionales como Naciones Unidas y la Organización de Estados Americanos, principalmente a través de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, han resaltado el rol fundamental del anonimato y de las herramientas de cifrado para combatir lo anterior y asegurar el ejercicio pleno de los derechos fundamentales, sin temor a represalias de ningún tipo.

Este panorama no solo afecta al individuo que se expresa, sino también a los canales de opinión en la red, quienes en los últimos años han llegado al punto de clausurar el debate a través de sus sitios para evitar responsabilidades ulteriores.

Lamentablemente, existen individuos que se escudan en el anonimato y cifrado para realizar actos ilegítimos o derechamente ilegales, que escapan de los márgenes tutelados por el derecho a la libertad de expresión. Actividad criminal, ciberacoso o promoción del discurso de odio claramente no están amparados. Como ya se demostró en estudios realizados, no todos los usos del anonimato responde a estos objetivos de dudosa legalidad, sino que la mayoría de ellos son una manifestación clara del derecho a la libertad de expresión por parte de individuos recelosos de su seguridad en línea, o que desean expresar un mensaje que no podrían hacerlo revelando su real identidad, ya sea por las consecuencias inicuas que ello podría desencadenar considerando la realidad en la cual viven o simplemente, por vergüenza o querer ser partícipes de una obra mayor a los individuos que la componen o por desear dirigir la atención del receptor al mensaje mismo y no al emisor, entre muchas otras razones válidas.

Tanto el debate como la regulación sobre el anonimato suele tender a mirar con mucho detenimiento a esta arista problemática del mismo, infravalorando sus beneficios. Los tests de necesidad, idoneidad y, sobre todo, de proporcionalidad debieran ser llevados a cabo de forma más concienzuda, teniendo plena conciencia que hoy en día internet es el mayor medio de comunicación y expresión. Cualquier medida que lo restringe fuertemente causará un gran impacto en una serie de derechos fundamentales.

Considerando la importancia del derecho a la libertad de expresión en un sistema democrático y como el anonimato hoy es una política de resguardo para el real ejercicio de este derecho, es que consideramos como necesarias las siguientes recomendaciones:

1. Realizar un efectivo test de proporcionalidad entre los bienes jurídicos que se quieren proteger con su restricción (seguridad pública, combate a la

discriminación, integridad física y psíquica, entre otros) con el detrimento que aquello generará en los derechos a la privacidad y libertad de expresión de la población en caso de buscar regular el ejercicio del anonimato en línea, ya sea directa o indirectamente.

2. No prohibir de manera generalizada el uso de herramientas tecnológicas de cifrado y anonimato ni someterlas a requisitos que hagan ilusoria su utilización (como lo sería exigir autorización previa a alguna institución estatal).
3. Promoción y apoyo gubernamental para uso de herramientas cifrado y anonimato a aquellos sectores de la población más vulnerables, como lo serían minorías, activistas, periodistas, artistas e investigadores.
4. Implementación gubernamental de herramientas de anonimato y cifrado en sus servicios públicos que requieran del conocimiento de datos sensibles de sus usuarios para resguardarlos adecuadamente ante intentos maliciosos de robo de los mismos y vigilancia.
5. No perseguir ni amedrentar a quienes realicen un legítimo ejercicio del derecho a la libertad de expresión amparándose en el anonimato.
6. Eliminar de los límites al derecho a la libertad de expresión al anonimato, tanto en los textos reglamentarios como legales, pero especialmente de las Constituciones Nacionales. Es manifiesta la importancia del anonimato para un real ejercicio de este en el mundo hiperconectado que vivimos hoy.
7. No exigir la renuncia del anonimato para el ejercicio de derechos fundamentales.

O Direito ao Esquecimento na América Latina (Artigo 19[132])

A. Introdução

As tecnologias digitais trouxeram um novo paradigma para a relação dos indivíduos com os mais diversos usos da informação. Hoje, grande parte do conhecimento humano está disponível `a distancia de apenas alguns cliques de mouse. A maneira como o conhecimento humano é documentado, gravado e lembrado mudou completamente com a otimização das capacidades de buscar e compartilhar informações decorrentes da ampliação do uso da internet e suas ferramentas.

Entretanto, diversos problemas emergem com essa disponibilização facilitada de informações e dados na internet. A maioria dos que navegam na rede acabam por ter sua atividade registrada, deixando uma espécie de "rastro" digital. Esse rastro digital pode ter enorme impacto sobre o exercício da liberdade de expressão e da privacidade no entorno digital.

Nos dias atuais os mecanismos de busca tornaram-se uma necessidade básica da navegação na rede, já que facilitam imensamente o acesso e a navegabilidade e acabam tendo papel central na potencialização da troca de dados, informações, imagens, vídeos e todo tipo de conteúdo disponível em formato digital. Por outro lado, esses mecanismos de busca também acabam por permitir, por exemplo, que informações privadas possam estar disponíveis a estranhos em questão de segundos. Esse fenômeno leva ao que muitos pesquisadores e ativistas tem apontado como uma fragilização do domínio sobre nossas "identidades digitais". Como reação a esse fenômeno, indivíduos tem buscado reassumir controle de sua autonomia e senso de identidade on line.

A reafirmação de controle sobre essas informações no mundo digital se estabelece

[132] Organización independiente de Derechos Humanos que trabaja alrededor del mundo para proteger y promover el derecho a la libertad de expresión. El presente trabajo fue realizado por el equipo residente en Brasil. http://artigo19.org/

como um novo paradigma, que se concretiza, por exemplo, na tentativa de remover tais informações tanto de ferramentas de busca como de outros âmbitos na rede. A idéia de um “direito ao esquecimento” emerge dessas tentativas.

A noção de um direito ao esquecimento não ‘e fruto da internet, mas tem evoluído com a evolução da tecnologia para registro de informações, com a consolidação da transição da cultura de memória oral para memória escrita. Com a acumulação e proliferação desses registros e a cada vez maior facilidade de acesso aos mesmos, vem-se desenvolvendo também a idéia de que certas informações devem, afinal, ser deixadas para trás.

Por exemplo, as leis de diversos países já reconhecem que, após um período de tempo, alguns registros criminais devem ser apagados para permitir que os indivíduos tenham maior capacidade de ressocialização. A ampliação dos sistemas de proteção de dados pessoais, principalmente na Europa, a partir dos anos 60, também tem considerado o direito dos usuários de pedirem a exclusão dos seus dados pessoais quando a informação for inadequada, irrelevante ou não mais relevante. A ideia de perda de relevância de uma informação ao longo do tempo é um conceito igualmente familiar em redações de jornal, onde a notícia é um elemento perecível.

O direito ao esquecimento ‘e hoje visto por muitos como uma ferramenta para equilibrar direitos, especialmente para proteção da privacidade em um contexto digital de vultosa e acelerada circulação de informações.

Porém, é preciso lembrar que existem diversos aspectos problemáticos e perigosos quando se fala de um “direito a ser esquecido”, já que informações que parecem triviais para alguns podem ter extrema relevância para outros, como por exemplo para o trabalho de historiadores, arquivistas e bibliotecários.

Arquivos públicos e arquivos de notícias têm funcionado como repositórios de memória coletiva sobre os mais diversos tipos de acontecimento, seja em escala mundial ou local. Muitos destes dados, principalmente os de caráter público, usualmente são vistos como informações que devem permanecer acessíveis por períodos indefinidos de tempo.

A criação de um mecanismo como o direito ao esquecimento deve ser analisada quando relacionada às ideias de memória coletiva e interesse público. Para contextos como o de países latinoamericanos, por exemplo, o “direito ao esquecimento” poderia ser utilizado por remanescentes e descendentes do legado de regimes militares e autoritários, recorrentes na região, e que ainda hoje tem

consequências diretas nas dinâmicas políticas e sociais destes países[133]. A ideia de memória – com o objetivo de manter viva a lembrança desses momentos históricos e sua superação - é diretamente conflitante com a de esquecimento, já que tais lembranças são diretamente relevantes não só para os que querem lembrar, mas também para revelar aquilo que tentou-se apagar ou que ainda nem foi revelado.

Na sua essência, o "direito ao esquecimento" está relacionado à tornar determinadas informações mais difíceis de serem de encontradas, mesmo nos casos em que tenha permanecido legitimamente em domínio público por décadas. Partindo da perspectiva que muitos indivíduos tentam esconder informações de interesse público verdadeiras, mas comprometedoras, o potencial para o abuso torna-se claro.

B. Avanços Recentes – Aspectos legais do direito ao esquecimento online

Com a aparente infinita disponibilização de informações sobre qualquer coisa ou qualquer pessoa online, a pressão para ampliação da compreensão e uso do direito ao esquecimento tem aumentado. Mas a verdade é que a expressão “direito ao esquecimento” induz ao erro, uma vez que não existe um tal direito expressamente reconhecido em instrumentos internacionais de direitos humanos ou constituições nacionais. Esse direito sequer é formalmente reconhecido na vasta maioria dos países ao redor do mundo. Alem disso, o escopo de tal direito continua grandemente indefinido. Ele varia desde um direito mais restrito decorrente de leis de proteção de dados na Europa, a vagas noções que englobariam a proteção da reputação ou honra em países como Brasil ou Rússia. De forma geral, as seguintes principais base legais podem ser identificadas:

- **Proteção de dados**

Como já mencionado, o direito ao esquecimento tem sido visto como derivando de leis de proteção de dados em muitos países. Na União Européia, por exemplo, o Tribunal de Justiça da União Européia reconhece o direito de indivíduos de requisitar o desindexação de resultados de busca gerados com base em buscas usando seu nome. Como esse ‘direito’ decorre de princípios de proteção de dados, o principal teste para verificar se o direito ao esquecimento pode ser aplicado é a verificação se a informação pessoal em questão é “inadequada, irrelevante ou não possui mais relevância”. Ao mesmo tempo, a informação pessoal não pode ser desindexada quando for de interesse publico, por exemplo, informações sobre a vida de um individuo publico. Alem disso, a informação não pode ser removida do

133 http://www.huffingtonpost.com/eduardo-bertoni/the-right-to-be-forgotten_b_5870664.html

site original e pode ser acessada com a utilização de outros argumentos de pesquisa que não o nome da pessoa. Na Rússia, em contraste, não existe na legislação qualquer balanceamento entre o direito ao esquecimento e a liberdade de expressão. Não existem isenções para informação de interesse publico ou sobre figuras publicas. Alem disso, não fica claro se a informação deve ser inteiramente removida independente dos termos de busca estarem sendo utilizados. Um aspecto comum entre a normativa da EU e a lei russa, no entanto, é que tal direito pode ser invocado apenas contra servidores de busca, mas não contra outros provedores de internet.

- **Privacidade, Direitos da Personalidade e Difamação**

A internet apresenta novos desafios para casos judiciais relacionados ao direito à privacidade, os direitos da personalidade e difamação, uma vez que a publicação de informações privadas ou difamatórias não esta mais limitada a copias impressas de jornais ou revistas, mas são replicadas indefinidamente e podem potencialmente permanecer online para sempre. Por essa razão, demandantes podem desejar "ser esquecidos" pela internet, seja por ferramentas de busca, operadores de sites ou arquivos online de noticiais. Embora no passado esses casos pudessem ser remediados por indenizações por danos, eles hoje são muitas vezes tratados em termos de remoção de conteúdo, com base em contratos de Termos de Serviço de provedores, ou outras normas relacionadas a responsabilidade de intermediários. Esses tipos de casos tem sido descritos como "direito ao esquecimento" apesar de dizerem respeito a remoção de informações de sites, e não a desindexação de resultados de busca. No entanto, é importante ter em mente que a remoção dos sites, ou seja, de sua fonte primaria, significa que em principio a informação não estará mais disponível. Esses casos diferem portanto do direito ao esquecimento reconhecido em decorrência das leis de proteção de dados da União Européia, mais limitado, que apenas define a desindexação de alguns termos de busca; ou seja, no caso europeu, a informação torna-se apenas mais difícil de encontrar.

C. O Direito ao Esquecimento na America Latina

Vários desdobramentos na forma de leis, projetos de lei e jurisprudência podem ser também observados na America Latina. Abaixo, traçamos um panorama das discussões legais sobre o direito ao esquecimento na região.

1. Brasil

1.1 Normativa

No Brasil, as espécies principais de normas em vigor que tocam no tema do direito ao esquecimento são as que regem o uso da internet e normas sobre condenações

penais.

Adotado em 2014, o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e dá diretrizes para atuação do Estado em relação à matéria. Tal norma afirma que os provedores de internet só poderão ser responsabilizados pela disponibilização de conteúdo caso não obedeçam ordem judicial que exija sua remoção, segundo o seu artigo 19. Assim, a retirada de conteúdo deve ser realizada judicialmente. A ponderação entre o direito de personalidade e o da liberdade de expressão deve sempre ser realizada em um caso de retirada de conteúdo. Ou seja, embora o Marco Civil não trate de maneira direta do direito ao esquecimento, versa sobre a retirada de conteúdo das redes, que pode ser usada como uma ferramenta deste direito.

Por sua vez o artigo 93 do Código Penal assegura ao condenado o sigilo do seu processo e da sua condenação para que se efetive sua reabilitação. Vale ressaltar que a jurisprudência não aplica o direito ao esquecimento apenas ao condenado, mas também a vítima que deseja manter a sua privacidade. Já o artigo 748 do Código de Processo Penal se relaciona com a reabilitação do condenado. Afirma que as condenações anteriores não serão mencionadas nas folhas de antecedentes do reabilitado, salvo quando requisitadas por juiz criminal.

Alem dessas normas já em vigor, existem no país várias propostas para regulação específica do direito ao esquecimento, definindo o escopo de tal direito das mais variadas formas.

- PL 7881/2014[134] – O projeto de lei ainda esta em discussão no plenário e seu conteúdo é bastante enxuto:

  "Art. 1º É obrigatória a remoção de links dos mecanismos de busca da internet que façam referência a dados irrelevantes ou defasados, por iniciativa de qualquer cidadão ou a pedido da pessoa envolvida".

  O projeto é bastante problemático. Ele deixa em aberto os critérios utilizados para definir o que poderia ser esquecido e utiliza termos muito vagos - como as expressões "irrelevantes ou defasados" - que podem ser interpretados de forma a restringir ilegitimamente o acesso à informações de relevante interesse púbico. Outro ponto problemático diz respeito a obrigatoriedade da remoção sem a necessidade de apreciação do conteúdo do link pelo judiciário. Além disso, possibilita que qualquer pessoa solicite a retirada do conteúdo, abrindo margens para eventuais abusos.

134 http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=621575

- PL 2712/2015[135] - Este projeto de lei se encontra apensado ao PL 1676/2015, descrito abaixo. Busca-se criar mais um direito para os usuários da internet, inseridos no artigo 7 do Marco Civil da Internet.

  "XIV – remoção, por solicitação do interessado, de referências a registros sobre sua pessoa em sítios de busca, redes sociais ou outras fontes de informação na internet, desde que não haja interesse público atual na divulgação da informação e que a informação não se refira a fatos genuinamente históricos."

  O direito ao esquecimento previsto, de forma implícita, na lei se reservaria apenas para os dados presentes na rede. A condição da retirada de conteúdo se dá por duas negativas: qualquer informação pode ser removida, desde que não haja interesse público atual e nem relevância histórica.

- PL 1.676/2015[136] – O projeto de lei não se reserva ao direito esquecimento, seus primeiros capítulos tratam de uma nova tipificação penal: fotografar, filmar ou obter gravação sonora de um indivíduo sem autorização ou fim legal. A pena seria de 1 a 2 anos de reclusão, aumento para entre 2 a 4 se ela for divulgada e entre 4 a 6 se ela for divulgada na internet. Após a tipificação das condutas apontadas acima, o artigo 3 da lei apresenta um conceito de direito ao esquecimento:

  "Art. 3º O direito ao esquecimento é expressão da dignidade da pessoa humana, representando a garantia de desvinculação do nome, da imagem e demais aspectos da personalidade relativamente a fatos que, ainda que verídicos, não possuem, ou não possuem mais, interesse público".

  Além disso, a lei afirma que o indivíduo pode solicitar o "esquecimento" para qualquer comunicador social, provedor de conteúdo e sites de busca, independente de medida judicial.
  Por fim, a lei obriga que os comunicadores sociais e as empresas de sites de buscas, provedores de conteúdo e redes sociais criem um departamento especializado para tratar dos casos de direito ao esquecimento, de forma que a própria empresa julgue se incide ou não o instituto.

- PL 1589/2015[137] - A autora do projeto procura agravar a pena de crimes como calunia e difamação que usem a rede como meio e também, inserir novos dispositivos no Marco Civil da Internet. Esses novos dispositivos procuram facilitar o acesso dos dados pessoais dos internautas pelo

135 http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1672348
136 http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1295741
137 http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1279451

Ministério Público. No que interessa o direito ao esquecimento, o projeto procura alterar o art. 19 da lei que trata da responsabilidade dos provedores de aplicações. Segue um dos parágrafos do artigo sugerido pela deputada:

"§ 3º-A O indivíduo ou seu representante legal poderá requerer judicialmente, a qualquer momento, a indisponibilização de conteúdo que ligue seu nome ou sua imagem a crime de que tenha sido absolvido, com trânsito em julgado, ou a fato calunioso, difamatório ou injurioso.

O texto é extremamente aberto e não considera a natureza dos assuntos que poderia ser objetos de esquecimento e também permite não somente a retirada do link, mas sim a remoção do conteúdo da rede. Um outro ponto importante da lei é a alta multa para o provedor de aplicação que não acatar a sentença judicial de retirada de conteúdo. Atinge o montante de R$ 50.000,00 (cinquenta mil reais) a multa pelo descumprimento de sentença, podendo ser sobrada em caso de reincidência do provedor. Atualmente o projeto se encontra apensado ao PL 215/15.

- PL 215/2015 - Já mais recentemente, na Comissão de Constituição, Justiça e Cidadania da Câmara dos Deputados (CCJC), foi discutido e aprovado o PL 215, que continha apensado o PL 1589/2015 e foi modificado nas negociações dentro da comissão. Por fim, o texto pretende adicionar ao artigo 19, parágrafo 3º do Marco Civil da Internet a possibilidade de "indisponibilização de conteúdo que associe seu nome ou imagem a crime de que tenha sido absolvido, com trânsito em julgado, ou a fato calunioso, difamatório ou injurioso"[138]. Tal projeto criaria, portanto, a possibilidade do "direito ao esquecimento". Tal redação, que embora obrigue as decisões a serem tomadas em processos judiciais e não apenas por Juizados Especiais onde o processo é mais acelerado, pode representar graves violações à liberdade de expressão e direito à memória e representaria um retrocesso significativo ao texto do Marco Civil da Internet. É importante ressaltar que o projeto vai além da desindexação de mecanismos de busca, já que propõe a retirada definitiva de conteúdos. O projeto encontra-se nas mãos da presidência da Casa e pode entrar na pauta do Congresso Nacional a qualquer momento.

1.2 Jurisprudencia

No Brasil, os primeiros casos emblemáticos envolvendo direito ao esquecimento envolvem conteúdos veiculados nos meios de radiodifusão e tratam de casos

138 http://olhardigital.uol.com.br/noticia/camara-aprova-lei-que-institui-direito-ao-esquecimento-na-web-brasileira/51963

criminais que aconteceram no passado, mas os quais a mídia retomou anos após os fatos. O judiciário reconhece o direito ao esquecimento, contudo apenas o caso prático revela em que medida ele será aplicado. Nessa linha, o judiciário Brasileiro procura afastar dogmáticas e aplicações imediatas.

(i) Recurso Especial nº 1.335.153 - RJ (2011/0057428-0)

Em 1958 o caso Aída Curi, torturada e assassinada, teve uma grande repercussão pública devido a crueldade do crime. Passadas muitas décadas, um programa de televisão resolveu fazer uma matéria sobre o caso, o que incomodou a família da vítima, que ingressou no Judiciário contra a emissora argumentando com base no direito ao esquecimento.

Pela primeira vez o direito ao esquecimento foi discutido no Superior Tribunal de Justiça (STJ). A decisão ponderou o embate entre o direito ao esquecimento e a liberdade de imprensa. Como o direito ao esquecimento está atrelado à dignidade da pessoa humana e aos direitos da personalidade, ele limita a liberdade de imprensa, segundo o julgado.

Contudo, apesar do juízo reconhecer a incidência do direito ao esquecimento no caso posto, ele não poderia ser utilizado para responsabilizar a emissora. Segundo, o desembargador, apesar do passar do tempo criar o direito ao esquecimento, o abalo moral gerado pela notícia também vai diminuindo de intensidade. De sorte que, após 50 anos do crime, a dor sofrida pelo familiares se resuma à somente a um desconforto. Além disso, afirma que em crimes marcantes, como o do presente caso, não há como desassociar a vítima. Assim, apesar de extensa e construtiva apresentação do direito ao esquecimento presente no julgado, ele não é aplicado.

Em recurso extraordinário[139] dos irmãos de Aída, ocaso foi considerado de grande relevância pelo Supremo Tribunal Federal , tendo em vista o argumento de que o direito ao esquecimento é um aspecto de proteção da dignidade da pessoa humana que ainda não teve apreciação pela corte. Na análise de admissibilidade, o relator, ministro Toffoli, reconhece que há um embate entre os direitos de expressão e acesso à informação contra a vida privada.

(ii) Recurso Especial nº 1.334.097 - RJ (2012/0144910-7)

Em 1993, policiais atiraram contra crianças e adolescentes que dormiam na escada de uma igreja. O caso conhecido como Chacina da Candelária ficou bastante famoso e o processo penal contra os policiais foram exaustivamente cobertos pela mídia.

---

139 http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?numero=833248&classe=ARE&origem=AP&recurso=0&tipoJulgamento=M

No presente caso, uma emissora de televisão noticiou o nome de um policial como se fosse participe do crime. O policial afirmou em sua inicial que o reavivamento do crime pelo jornal, com seu nome atrelado ao caso, ofendeu-lhe a honra e a vida intima. Já o jornal alegou que a participação do policial era peça fundamental para o episódio e que a chacina já integrava o patrimonio histórico brasileiro. O direito ao esquecimento se faz presente, pois apesar de ter sido indiciado para responder o processo, o autor foi absolvido. O relator da ação entendeu que o direito ao esquecimento encontra respaldo quando inexiste interesse público na matéria divulgada, porém, no caso, o envolvimento do policial absolvido não tinha nenhuma relação com o crime ou seu histórico já que foi absolvido posteriormente. Além disso, o tribunal entendeu que os absolvidos tem o direito ao esquecimento garantido em relação ao crime de que foram acusados. A condenação pecuniária também foi acompanhada da proibição de vincular o nome do policial ao caso, como se depreende do seguinte trecho "*No caso, permitir nova veiculação do fato com a indicação precisa do nome e imagem do autor, significaria a permissão de uma segunda ofensa à sua dignidade...*".

O Brasil ainda passa por uma construção jurídica e doutrinária para o desenvolvimento do direito ao esquecimento. A matéria ainda é bastante recente, mas com a popularização da internet no país e o crescimento do acesso à justiça o número de casos envolvendo o instituto tende a aumentar.

Quanto ao direito ao esquecimento na internet, recentemente, um caso envolvendo a apresentadora de televisão Xuxa e a Google também tiveram bastante repercussão. [140] Na ação, a apresenta deseja desvincular sua imagem das pesquisas em sites de busca contendo as expressões "Xuxa sexo" e "Xuxa pedofilia", os quais exibiam imagens de filme onde aparece em cenas de nudez com personagem menor de idade. Os tribunais superiores negaram o pedido da apresentadora, reafirmando a prevalência da circulação de informação no presente caso. Argumenta-se que um termo não pode ser retirado de uma ferramenta de busca, pois prejudica o acesso à informação. O provedor de pesquisa não poderia ser responsabilizado pela URLs que ele disponibiliza pelo seu serviço de busca, tendo tem vista que ele só mostra resultados de sites que existem na rede. A prevalencia do direito à informação se deu pela acusação equivocada que se deu contra o site de pesquisa.

Apesar da lei não ser específica quanto ao tratamento de dados pessoais ou do direito ao esquecimento propriamente dito, a jurisprudência brasileira já o reconhece como um direito da personalidade e, geralmente, encontra um embate entre a liberdade da circulação de informação e o direito ao esquecimento.

140 http://www.migalhas.com.br/arquivos/2014/9/art20140929-02.pdf

(iii) Casos emblemáticos na seara da remoção de conteúdo

Tais casos não configuram necessariamente a modalidade de direito ao esquecimento, mas são bastante relacionados e revelam algumas boas práticas, principalmente de análise técnica/tecnológica, nas cortes brasileiras relacionadas à remoção de conteúdo com o objetivo de omitir informações específicas de determinados atores na sociedade.

Um caso identificado acabou por ser revertido em instância superior, o que garantiu a não-penalização da plataforma Google. Neste caso, a reclamante ajuizou ação indenizatória contra o Google e o ex-namorado[141], pedindo que a plataforma retirasse seu nome do sistema de busca. O relator do caso, o desembargador Francisco Vildon José Valente, concluiu que não adiantaria o Google excluir palavras dos resultados da busca, pois qualquer outra combinação de palavras relacionadas que contenha o teor da pesquisa poderia gerar o mesmo resultado. Além disso, considerou também que o Google não é o único provedor de buscas da internet, e portanto tal limitação não levaria ao resultado supostamente esperado pela reclamante.

Decisão semelhante ocorreu no caso do senador Aécio Neves[142] durante o período eleitoral brasileiro de 2014. Ele solicitou a condenação dos sites de busca da internet Google, Bing e Yahoo, pedindo que as buscas realizadas nas ferramentas dessas plataformas fossem restringidas, e que o seu nome não pudesse ser relacionado a notícias de desvio de recursos públicos durante seu governo no estado de Minas Gerais. Entretanto, o juiz Rodrigo Garcia Martinez decidiu que o desrespeito ao direito da coletividade à informação, mesmo que a notícia fosse falsa, representaria "retrocesso à liberdade de manifestação e de informação sobre acontecimentos do mundo globalizado". Ainda adicionou que as ferramentas de busca apenas se limitam a indicar os links onde podem ser encontrados os termos procurados.

2. Argentina

2.1 Normativa

Na Argentina a Lei de dados - Lei 25.326[143] - procura tutelar juridicamente todos os dados pessoais que circulam nas mãos de pessoas jurídicas privadas e públicas. Em seu art. 2 ela define os verbetes que são utilizados na lei como dados sensíveis, dados pessoais, etc.

141 http://www.conjur.com.br/2015-fev-19/google-nao-obrigado-excluir-nomes-sistema-busca-tj-go
142 http://www.migalhas.com.br/Quentes/17,MI221104,71043-Aecio+Neves+nao+consegue+retirar+conteudo+desfavoravel+de+sites+de
143 http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

A ação jurídica que deve ser movida em função dos dados é a de *hab*e*as data*. O instituto é usado para acessar as informações presentes em qualquer banco de dados do país. Além disso, a ação também pode retificar alguma informação que esteja nesses bancos de dados. Não só modificações, com a ação os dados podem ser suprimidos. Aqui se insere o direito ao esquecimento, a proteção dos dados. Todo o procedimento jurídico é previsto no capítulo VII da lei.

Um projeto de lei para regulamentar o direito ao esquecimento foi proposto em 2014. O PL 8372-D[144] é bastante direto, afirmando que as pessoas podem notificar provedores de ferramentas de busca para a retirada de resultados que exponham dados pessoais, desde que tal retirada não afete terceiro ou fatos de interesse público. Dados esses que são definidos no artigo 2 da Lei 25.326.

Vale ressaltar que a lei não especifica o que seria uma retirada que afeta terceiro ou quais seriam os fatos de interesse público, deixando para os próprios provedores e, posteriormente, o judiciário a responsabilidade de julgar se o conteúdo deve ou não ser esquecido.

Além disso, obriga os provedores a criarem uma plataforma gratuita e de fácil acesso em seus sites para que os indivíduos enviem as notificações. Então, os provedores teriam 30 dias para deferir ou não o pedido feito pelo pessoa. Em caso de negativa, o caso seria enviado para conciliação no juizado especial de consumidor.

2.2 Jurisprudencia

A jurisprudência é bastante divergente quanto ao direito ao esquecimento no país. O caso mais emblemático, que foi, inclusive, o primeiro a ser julgado pela suprema corte, teve um posicionamento desfavorável ao direito ao esquecimento.

A ex-modelo Bélen Rodríguez tinha seu nome associado à sites de pornografia quando era pesquisa em plataformas de busca. Então, ela ingressou com ação contra o Google e o Yahoo! para que as plataformas de busca desvinculassem o seu nome dos site de entretenimento adulto, além de danos morais. O primeiro e o segundo grau de jurisdição deram procedência ao pedido da modelo, afirmando que o dano realmente aconteceu e que os buscadores deveriam retificar suas pesquisas sobre a modelo. Contudo, a suprema corte entendeu que essa desvinculação seria uma ofensa à liberdade de imprensa. A decisão comparou os sites de busca à imprensa e afirmou que só caberia a responsabilidade deles em casos excepcionais nos quais seriam vinculadas informações ilegais[145].

144 http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=8372-D-2014
145 http://www.rlpdp.com/wp-content/uploads/2014/10/CSJn-Google.pdf

Em linha contrária, o primeiro e o segundo grau de jurisdição no país sentenciam de maneira mais favorável ao direito esquecimento. Além da procedência do caso da modelo demonstrado acima, um caso envolvendo o secretário da Universidade de la Matanza[146] denota esse caráter pró esquecimento.

Havia vários sites criticando o comportamento do secretário frente aos estudantes, apresentando um histórico de autoritarismo e truculência. Assim, ele ingressou com uma ação contra o Google para desvincular seu nome desses sites na plataforma. O tribunal reconheceu o direito do secretário ao esquecimento, afirmando que as informações disponibilizadas nesses sites atingiam a honra do autor. As informações envolvendo o secretário deveriam ser estritamente profissionais.

Portanto, a jurisprudência ao direito ao esquecimento no país apresenta alguma controvérsias. Apesar da lei de proteção de dados indicar o habeas data como ferramenta processual para a supressão de dados pessoais, as soluções frente aos casos concretos são bastante divergentes quando se observam casos parecidos.. Dois indivíduos que tiveram seus nomes vinculados à fatos que maculavam a sua honra obtiveram decisões opostas frente ao judiciário. Contudo, as decisões são do final de 2014, o que revela que o debate sobre o direito ao esquecimento chegou recentemente aos grandes tribunais.

Por fim, temos que o país ainda se encontra em uma incipiente discussão de direito ao esquecimento em seus tribunais. Apesar da lei de dados datar de 2000, o debate sobre este instituto ganhou vigor recentemente, de forma que este direito ainda deve ser desenvolvido na área. O tramite do projeto de lei que trata especificamente do direito ao esquecimento no país pode trazer esse amadurecimento necessário.

3. Chile

3.1 Normativa

A lei de proteção da vida privada do Chile - Lei 19.628/99 [147] trata, fundamentalmente, do gerenciamento, segurança e responsabilidade acerca dos dados pessoais. O primeira capítulo da lei afirma, de antemão, que as matérias de liberdade e difusão da informação não são reguladas neste lei, mas no art. 19, inciso 12, da sua Constituição.

A lei afirma que os dados pessoais devem ser eliminados dos bancos de dados quando carecem de justificação jurídica para a sua retenção ou quando caducaram. A lei permite que os dados sejam retificados quando eles se apresentam de forma

146 http://www.lanacion.com.ar/1725758-fallan-contra-google-debe-dejar-de-listar-paginas-sobre-el-secretario-general-de-la-universidad-de-la-matanza

147 http://investigacion.uc.cl/images/pdf/Etica/Ley_19.628_Sobre_Protecci%C3%B3n_de_la_Vida_Privada.pdf

errônea ou incompleta.

Os artigos de 12 a 16 da lei tratam mais especificamente do processo de modificação e exclusão dos dados pessoais em posse de órgãos públicos e privados. A norma afirma que nenhuma convenção pode impedir o indivíduo de apagar, modificar ou acessar os seus dados pessoais. Todos os ônus decorrentes dessas modificações ou acesso cabem ao órgão possuidor dos dados. O art. 15 da lei apresenta as limitações para esse direito, por exemplo: a segurança nacional, o trabalho de órgão fiscalizadores, o interesse público não podem ser prejudicadas pela demanda acerca dos dados pessoais. Por fim, o art. 16 apresenta toda a cadeia processual pela qual o processo envolvendo dados pessoais percorre.

Apesar do direito ao esquecimento não estar claramente previsto na lei, todo o procedimento para a supressão de dados esta previsto nesta lei de dados pessoais. Um grupo de senadores visam modificar a lei, afirmando que toda pessoa tem o direito de exigir que os sites de busca removam qualquer dado pessoal seguindo o rito do art. 16. O projeto foi bastante criticado, pois não estabelece nenhum critério objetivo, podendo, inclusive, ser utilizado para prejudicar a liberdade de expressão.[148]

Proposta para novas normas também estão em discussão no Legislativo:

- PL 9388-03[149] – Este é o projeto de lei que tem maior visibilidade dentro do debate de direito ao esquecimento no país. Ele insere um inciso no primeiro artigo na lei de proteção de dados pessoais. Nele, estaria previsto que todos tem o direito de solicitar a remoção de dados pessoais em provedores de busca ou qualquer outro site. O inciso não estipula um prazo, mas caso os detentores dos dados não tomem providências ou se manifestem, o titular dos dados pessoais pode ingressar com ação judicial para a remoção como contra no art. 16 da lei de proteção de dados pessoais chilena.
- PL 9917-03 [150] – Este projeto de lei, apesar de tratar do direito ao esquecimento em suas justificativas, não prevê o instituto, de maneira explicita, em seu texto. Além disso, o projeto tem um enfoque mais comercial e financeiro do direito ao esquecimento. Fica vedado aos bancos de dados utilizarem e transferirem os dados pessoais transcorridos 5 anos após o cumprimento da função que aqueles dados tinham. O caráter econômico começa a ficar mais claro na pretendida modificação do art. 17 da lei de

148 https://www.fayerwayer.com/2014/06/senadores-chilenos-presentan-proyecto-de-ley-para-instaurar-el-derecho-al-olvido/

149 https://www.camara.cl/pley/pley_detalle.aspx?prmID=9800&prmBoletin=9388-03

150 http://www.retailfinanciero.org/wp-content/uploads/2014/11/Proyecto-de-Ley-Derecho-al-Olvido-Senador-Harboe-.pdf

proteção de dados pessoais. Esse artigo prevê como se dará o tratamento de dados pessoais que estão ligados à algumas atividades financeiras. Este projeto de lei veda o uso, tratamento, transferência, e comunicação de dados pessoais decorrentes de obrigações de caráter econômico, financeiro, bancário ou comercial, devendo proceder de forma como esses dados jamais tivessem existido. Em caso contrário, o projeto afirma que cabe ação judicial com pedido de indenização por danos morais e patrimoniais caso o titular constate a existência desses dados pessoais.

3.2 Jurisprudencia

Não há casos relevantes sobre o tema no Chile. Existem, inclusive, alguma críticas feitas pela mídia pela falta de aplicação e visibilidade que a lei de dados tem no pais. Apesar de não existir um direito ao esquecimento expresso no ordenamento chileno, a preocupação com o instituto começa a despontar no Poder Legislativo do país. Contudo, a lei de proteção de dados pessoais, que seria a ferramenta em vigor mais adequada para o direito ao esquecimento, não parece ter aplicação no país. Diferente de outros países, a lei não é utilizada para o esquecimento.

4. Uruguai

4.1 Normativa

A lei de dados pessoas uruguaia - Lei 18.331/08[151] possui uma peculiaridade em seu artigo 2: ela estende a proteção ás pessoas jurídicas. Além disso, cada artigo é redigido em forma de verbete, apresentando os princípios e os direitos seguidos da sua explicação e consequências legais. Nessa linha, o artigo 15 apresenta o direito de retificar, atualizar, adicionar e suprimir informações. O direito esquecimento, apesar de não estar evidentemente expresso, se dá pelo direito a supressão desses dados. As limitações impostas para as possíveis modificações são prejuízos ao interesse legitimo de terceiros, notório erro ou falsidade e contravenção imposta por obrigação legal. Os órgãos que detêm os dados tem 5 dias para cumprir o requerimento do art. 15.

Outro destaque da lei uruguaia é que ela distingui o regime dos bancos de dados públicos e privados, no entanto as duas obedecem as mesmas regras de registro. Os públicos podem restringir o direito de acesso, supressão e modificação. Além disso, os dados podem ser obtidos sem o seu consentimento, mas seu uso deve ser necessário para a segurança nacional. Enquanto que os bancos de dados privados devem seguir todos os princípios e direitos sem exceções.

Os arts. 37 a 45 regulam a ação de habeas data que pode ser impetrada para

151 http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331&Anchor=reg

proteger os dados pessoais. A medida processual é o instrumento para a efetivação dos direitos de adição, modificação, retificação e supressão dos dados pessoais. Ele informa as medidas processuais de forma bastante simplificada, inclusive, afirmando o conteúdo que a sentença de habeas data deve ter como a especificação do banco de dados, a identificação do que dever ser retirado e o prazo para tal.

Cabe também ressaltar que a lei de dado uruguaia institui a criação de uma agência reguladora (Agesic) formada por diferentes membros do poder público para penalizar bancos de dados que estejam violando a lei, auxiliar os indivíduos em suas demandas de proteção de informação, entre outras funções que tem como objetivo fazer vigorar a lei. Sobre direito ao esquecimento, o órgão emitiu um parecer que aproxima o direito ao esquecimento do ordenamento uruguaio[152].

4.2 Jurisprudencia

Apesar da criação da Agesic e de sua postura pró proteção de dados pessoais os números de decisões judiciárias são ínfimas para que se trace um panorama jurisprudencial no país. Mesmo o país não sendo populoso, 60% dos seus habitantes tem acesso ás redes. Ainda não há nenhum caso paradigmático que posa indicar o direcionamento do judiciários uruguaio quanto o direito ao esquecimento.

5. México

5.1 Normativa

A Lei de proteção de dados pessoais possuídos por particulares[153] , como sugere o título, tem sua aplicação limitada aos responsáveis particulares pelos dados. Assim, a aplicação do direito ao esquecimento por meio dessa lei não se enquadra aos bancos de dados públicos.

Outro diferencial da lei é que ela prevê, em seu art. 15, o aviso de privacidade. Além de informar a coleta de dado em si, o responsável deve informar ao titular dos dados sobre a finalidade, a limitação de divulgação e, principalmente, os meios para exercer o direito de retificação ou cancelamento dos dados.

A lei mexicana também não traz o direito ao esquecimento expresso em sua legislação. Contudo, o direito de retificar ou cancelar os dados esta presente no art. 22 da lei. Ainda, o art. 25 afirma que o direito de cancelamento do dado pode ser feito em qualquer tempo, contudo existem limitações para o direito ao cancelamento. Os dados serem objeto de contrato privado entre o titular e o responsável, se os dados tem um tratamento legal específico, a supressão resultar em empecilho para

152 http://www.agesic.gub.uy/innovaportal/file/3549/1/derecho_al_olvido.pdf
153 http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

as obrigações de fiscalizar e de investigar do Estado são alguns dos impeditivos do cancelamento previstos no art. 26.

O capítulo IV da lei trata do exercício processual do direito de cancelar e retificar os dados. Ao ter o cancelamento solicitado, o responsável tem 20 dias para comunicar ao titular o tratamento dos dados requisitados. Depois, o responsável terá 15 dias para efetivar o que foi comunicado. Além disso, todos os responsáveis privados pelos dados pessoais devem ter um departamento em suas empresas, exclusivos, para a análise dessas demandas.

5.2 Jurisprudencia

A jurisprudência mexicana tem procurado se afirmar por meio do Instituto Federal de Acesso à Informação e Proteção de Dados. A agencia criada em 2011 teve vários pedidos de retirada de dados pessoais, contudo quase nenhum chegou ao judiciário.

O primeiro desafio do direito ao esquecimento no país se deu em janeiro de 2015, quando a Google negou o pedido de um cidadão mexicano de desvincular o seu nome das pesquisas do buscador. A empresa argumenta que os dados utilizados são tratados nos Estados Unidos e não no México, de sorte que não poderia se submeter as leis mexicanas. O processo ainda esta sendo apreciado pela corte, podendo ser o primeiro grande precedente jurídico do direito ao esquecimento no país.

Por fim, cabe lembrar que a ausência de jurisprudência de peso no México sobre o direito ao esquecimento não se dá pela ausência de casos, mas pelo fato de que sua grande maioria é solucionado em esfera administrativa. Já é claro que o direito ao esquecimento no país tem força, mesmo sem a sua previsão expressa. Contudo, o caso envolvendo uma empresa de grande porte, como a Google, vai indicar o posicionamento do judiciário sobre o tema.

6. Colômbia

6.1 Normativa

A lei de proteção de dados colombiana - Lei 1581/2012[154] - segue o padrão latino americano em alguns aspectos: define princípios gerais no tratamento de dados, prevê o dever de notificação do detentor de dados pessoais aos seus titulares e coloca o habeas data como instrumento para modificar, retificar ou suprimir os dados, previsto no art. 8 da lei.

Os artigos 19 ao 24 regulam a atividade de uma agencia pública no que compete a

154 http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

proteção de dados. Sendo uma delegação da Superintendência da Industria e Comércio a responsável por fiscalizar o tratamento dos dados pessoais e os casos judiciários decorrentes deles. Mais uma vez observamos o direito ao esquecimento sendo retratado de forma indireta, sem qualquer referencia específica dentro do ordenamento jurídico colombiano.

O Decreto 1377/2013[155] procura retificar e complementar a lei de dados pessoais colombiana. Ela também traz o requisito de aviso de privacidade para a coleta de dados, previsto nos arts. 14 e 15 da lei. O art. 22 da lei trata de forma mais incisiva dos direitos à atualização, retificação e supressão dos dados. Afirma-se que os dados devem ser verídicos e condizentes com o fim do seu tratamento e coleta. Além disso,o pedido deve ser atendido, caso os dados não se enquadrem nos princípios citados.

6.2 Jurisprudencia

A Suprema Corte colombiana, recentemente, julgou um caso de direito ao esquecimento bastante relevante[156]. O jornal El Tiempo havia feito uma reportagem sobre uma quadrilha que estava sendo indiciada pelo crime de tráfico de pessoas. Entre os indiciados, estava Glória que trabalhava com a venda de passagens aéreas. No decorrer do processo, Glória foi inocentada pela justiça, contudo o jornal não atualizou a matéria. Assim, qualquer indivíduo que pesquisasse o nome da mulher nos sites de busca, encontraria seu nome na matéria do El Tiempo.

A decisão da Corte não tratou do direito ao esquecimento propriamente dito, mas fez importantes ponderações sobre a aplicação do direito na internet do país. Em um ponderamento entre o direito à honra e liberdade de expressão, os juízes concluíram que a notícia merecia ser retificada, contudo a liberdade de expressão seria afetada pela retirada da notícia da rede. Assim, conclui-se que a notícia seria retificada, mas não retirada. Além disso, o tribunal afirmou que o Google, ou qualquer empresa intermediária dos serviços de busca, não poderia ser responsabilizada por conteúdos gerados por terceiros. Portanto, a responsabilidade recairia sobre o jornal, que deveria desindexar a notícia dos resultados da Google quando pesquisassem pelo nome da mulher.

A saída dada pela corte colombiana parece bastante problemática. Primeiro, ela não trata do direito ao esquecimento, propriamente dito, que está em pauta de discussão do legislativo e do judiciário de vários países latinos. A não responsabilização da Google pela desindexação do conteúdo de suas pesquisas parece dificultar futuras ações que caminhem no sentido de suprimir o acesso à informações pessoais na

155 http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf
156 https://karisma.org.co/wp-content/uploads/2015/07/TUTELA-EL-TIEMPO.pdf

internet. Colocar o ônus no veículo de informação é inadequado, visto que os buscadores tem tecnologia de desindexação muito mais prática e aprimorada. Dessa forma, a jurisprudência colombiana mostra um primeiro passo mal dado no tema.

7. Costa Rica

7.1 Normativa

A Costa Rica não possui nenhuma legislação expressa sobre direito ao esquecimento. Contudo, o país apresenta uma construção jurisprudencial da Suprema Corte no tema. É um posicionamento bastante peculiar como se verá a seguir.

7.2 Jurisprudencia[157]

O direito ao esquecimento na Costa Rica foi uma construção da sua Suprema Corte que, na década de 90, entendeu que este direito era um desdobramento do direito a intimidade. Na prática, a Corte foi se posicionamento favoravelmente em casos contra o Arquivo Judicial, para que dados fossem retirados desse banco de dados. A Suprema Corte costarriquenha firmou entendimento de que o direito esquecimento, em esfera civil, pode se aplicar em matérias que tenham mais de 4 anos. Posicionamento esse que foi reafirmado no julgado do caso 160306-2006[158], no qual se definiu que o mesmo prazo se dá para dividas de impossível adimplemento e quando a divida se encontra cancelada por processo jurisdicional.

Ainda nessa linha, o julgado 1438-92 de 2 de junho de 1992 da Corte considerou inconstitucional diversos artigos do Código Penal e do Código de Processo Penal do país que aumentavam a pena dos reincidentes do sistema prisional. Dessa forma, o direito ao esquecimento começa a alcançar o direito penal. Além disso, os documentos relativos ao casos penais só teriam validade de 10 anos, buscando preservar o direito do detento a reintegração na sociedade. O julgado afirma que a manutenção contínua desses dados é como uma pena perpétua, pois trará danos às pessoas enquanto esses dados estiverem disponíveis.

8. Nicarágua

8.1 Normativa

157 Estudo sobre o tema em http://iij.ucr.ac.cr/sites/default/files/documentos/t12-el_derecho_al_olvido_en_la_internet.pdf

158 http://vlex.co.cr/vid/-499020190

A Lei 787 de 2012 - “Ley de Protección de Datos Personales”[159] - permite que o titular dos dados solicite a redes sociais, navegadores e servidores que removam e cancelem os dados pessoais armazenados em suas bases de dados. É considerada como sendo uma espécie de “direito ao esquecimento” digital, mas se limita a cuidar dos dados pessoais.

As regras servem tanto para serviços que recolhem dados de instituições públicas quanto privadas e que oferecem bens e serviços e, por razões contratuais, coletam dados pessoais. Nesses casos, uma vez que a relação contratual se encerre, o titular pode solicitar a exclusão e cancelar todas as informações pessoais registradas como sendo do usuário do serviço ou comprador de um determinado produto.

A definição de cancelamento já está prevista no Art. 3 da lei, que trata das definições. São tratados no item b os direitos dos titulares, que incluem o cancelamento mas também os direitos de acesso, retificação e oposição. Há uma seção exclusiva, a IV, para o “Direito de Cancelamento”. Ela diz respeito aos artigos 30, 31, 32 e 33 da lei de dados pessoais nicaraguense e discorrem sobre: Direito de Cancelamento; Exercício do Direito de Cancelamento; Bloqueio; e Propósitos do Bloqueio.

O bloqueio, no caso, tem o propósito de “(...) determinar possíveis responsabilidades relativas ao seu tratamento com o termo de limitações legais ou contratuais destes, e notificar o proprietário dos dados ou seu representante, em resposta ao pedido de cancelamento;”, de acordo com o item a do Art. 32.

8.2 Jurisprudencia

Não foi possível identificar jurisprudência para o caso de “direito ao esquecimento” na Nicarágua, para além de situações de uso da lei de proteção de dados pessoais.

9. Revisão das tendências e práticas na região

A análise das normas vigentes na America Latina, assim como as novas propostas de lei em debate, indicam que na região a aplicação do direito ao esquecimento tem se dado sem as devidas salvaguardas à liberdade de expressão.

O Brasil ainda passa por uma construção jurídica e doutrinária característica de toda a região, decorrente da expansão da internet nos países e o crescimento do acesso à justiça. Já na Argentina, nota-se que com relação aos casos mais bem difundidos

159 http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/7bf684022fc4a2b406257ab70059d10f?OpenDocument

ainda há contrastes significativos. O contexto Colombiano parece apontar mais claramente para avanços num sentido perigoso. No México, os casos tem sido tratados na esfera administrativa e ainda não foram verificados casos finalizados no âmbito judicial. No Uruguai e no Chile, tal aplicação ainda parece não ter emergido, também na Nicarágua não se identificou jurisprudencia. Na Costa Rica, o direito ao esquecimento tem se consolidado no âmbito penal. Não foi possível identificar praticas em outros países latinoamericanos.

Algumas das decisões judiciais identificadas, porém, dão boa margem para o estabelecimento de práticas positivas no âmbito do "direito ao esquecimento". Elementos interessantes identificados nessa jurisprudência reconhecem ou ressaltam:

- A ideia de que informações de relevante interesse público não podem ser retiradas de uma ferramenta de busca, por prejudicar o acesso à informação;

- A noção de que um provedor de pesquisa não pode ser responsabilizado pelo conteúdo de páginas para as quais disponibiliza links como resultado de buscas. Isso porque, tal serviço apenas realiza uma indexação de termos específicos, caracterizando-se como mero intermediário;

- A improbabilidade e impossibilidade de determinados conteúdos serem completamente removidos da rede;

- Que o controle de conteúdo não deve ser passado aos provedores intermediários que, pelo receio de intervenções judiciais, tenderiam a censurar previamente diversos tipos de conteúdo legitimo.

10. Conclusão

Observando-se o atual contexto regional, fica claro que estamos em um momento crucial de definição e modulação do direito ao esquecimento na America Latina. Nesse sentido, reconhecemos as preocupações relacionadas a proteção de dados e da privacidade em face da coleta massiva de nossos dados pessoais por atores públicos e privados. Também entendemos que é vital que a privacidade seja protegida na era digital. No entanto, alguns outros aspectos devem ser levados em consideração:

- **Indivíduos não tem e não deveriam ter um direito absoluto de controle sobre as informações que lhe dizem respeito.** O fato de uma informação dizer respeito a um individuo não implica que esse individuo tem domínio total sobre tal informação, em um sentido patrimonial. Indivíduos nao deveriam poder restringir acesso a informações sobre sua pessoa, que tenham sido publicadas por terceiros, exceto quando tal informação for privada ou sua publicação não tenha qualquer tipo

de justificativa legítima. Em outras palavras, informação sobre um individuo pode igualmente pertencer ao publico, que não pode ser impedido de acessá-la. A idéia de que um indivíduo pode ter controle total sobre uma informação ignora o fato de que existe um direito coletivo a acessar, receber e disseminar material que esteja legitimamente em domínio publico.

- A liberdade de expressão é pautada pelo interesse publico. Em geral, nenhuma justificativa deve ser exigida para a publicação de informações que não sejam de natureza privada. O que muitos consideram como informação trivial, pode fornecer insumos de grande valor para historiadores e outros pesquisadores. A partir do momento que uma informação já seja publica, existe grande interesse em sua preservação e na manutenção de sua acessibilidade para estudos, arquivamento e analises. A coleta de dados culturais e históricos – que podem incluir dados pessoais – deve ser tratada como forma válida de retenção de dados para além de sua validade para 'fins operacionais'.

- **Mesmo a publicação de informação obtida ilegalmente pode ser de interesse publico**. É o caso, por exemplo, de informações vazadas por denunciantes (whistleblowers).

- As pessoas deveriam ter a oportunidade de perdoar. Muitas vezes, permitir que indivíduos façam a desindexação de certos links associados ao seu nome acaba por permitir que eles apresentem um retrato também distorcido sobre quem são. Indivíduos que buscam informações sobre uma pessoa deveriam poder formar suas próprias opiniões sobre elas. Indivíduos deveriam ter a oportunidade de perdoar ou ignorar erros passados ao invés de ter tais erros 'apagados' por aqueles que os cometeram.

- Derivar o "direito ao esquecimento" de leis de proteção de dados é problemático. Dados pessoais podem ser privados ou públicos. Leis de proteção de dados permitem que se apague informações sobre indivíduos simplesmente porque tais pessoas consideram que tais informações já nao são relevantes. Essas normas nao levam em consideração conceitos próprios da proteção da liberdade de expressão, como a idéia de uma "expectativa razoável de privacidade", a verificação de dano real significativo, ou a noção de domínio publico (que serão detalhados abaixo). A aplicação de leis de proteção de dados para tratar o direito ao esquecimento pode levar ao resultado de que muitas informações perfeitamente legais poderiam ser tornadas de difícil acesso simplesmente porque indivíduos querem ocultar informações embaraçosas. Alem disso, leis de proteção de dados colocam as ferramentas de busca em posição desconfortável, pois elas passam a ter que determinar quando um dado é "inadequado, irrelevante ou nao mais relevante", devendo ser, portanto, desindexado. Ferramentas de busca, no entanto,

nao possuem independência e imparcialidade para tomar decisões que impactem sobre o direito a privacidade e/ou liberdade de expressão.

Sem tentar apontar soluções prontas, indicamos a seguir algumas recomendações que visam facilitar o uso de elementos importantes do direito ao esquecimento, ao mesmo tempo que reconhecendo suas limitações e assegurando a proteção à liberdade de expressão.

1. Remédios já existentes devem ser privilegiados

Embora seja legitimo que indivíduos busquem a remoção do acesso a informações sobre eles que seja de natureza privada ou difamatória, normas já existentes nessas áreas (como leis de privacidade e difamação) podem embasar tal demanda, sem a necessidade de criação de nova legislação especifica que se proponha a criação de um direito ao esquecimento. Soluções com base em contratos de serviço de intermediários (provedores) também podem ser usadas como alternativa.

2. Qualquer direito ao esquecimento eventualmente reconhecido deve ser de natureza restritiva

Tendo em vista a tendência à adoção de um direito ao esquecimento por legisladores e cortes na região, sugerimos abaixo alguns padrões para adoção de um conceito restritivo de direito ao esquecimento. Importante reconhecer também que provedores de busca podem considerar oferecer soluções nessa área através da auto-regulacao.

- Direito individual: qualquer reconhecimento deveria limitar o direito ao esquecimento a pessoas jurídicas naturais, não permitindo seu uso por empresas ou outras instituições, uma vez que sua justificativa é a proteção da dignidade individual.
- Causa para ações contra ferramentas de busca: qualquer direito ao esquecimento deveria ser exercido primariamente contra ferramentas de busca enquanto controladores de dados, para desindexação de resultados de busca, e não contra serviços de hospedagem ou provedores de conteúdo.
- Proteção da liberdade de expressão: normas estabelecendo um direito ao esquecimento deveriam fazer referencia explicita ao direito à liberdade de expressão como direito igualmente fundamental, e em relação ao qual deve ser balanceado o direito ao esquecimento nos casos concretos.
- As cortes devem decidir: embora provedores de serviços de busca sejam a porta de entrada natural para demandas de “esquecimento”, acreditamos que como principio, as cortes deveriam decidir sobre a pertinência dos pedidos

elaborados.

3. Nos casos concretos, alguns critérios podem ser utilizados para balancear a liberdade de expressão e o direito ao esquecimento

Em algumas circunstancias, quando fica claro que a informação reclamada nunca deveria ter sido tornada publica, dada sua natureza privada, e sua publicação nunca tenha sido justificada, o direito ao esquecimento pode ser considerado incontroverso e uma alternativa importante para uma solução eficiente do caso. Por exemplo, casos de vingança pornográfica são melhor solucionados pela desindexação de resultados de busca. Alem disso, a desindexação pode ser vista como solução mais interessante do que a remoção de conteúdo, por ter impacto menos negativo sobre a liberdade de expressão.

No entanto, outros casos tocam em aspectos mais controversos do direito ao esquecimento, como nos casos em que a informação reclamada é parte de um registro publico ou refere-se a uma pessoa publica. Entendemos que, como principio, informações desse tipo devem ser mantidas em domínio publico e ser facilmente acessadas através de ferramentas de busca. No entanto, em casos excepcionais, pode ocorrer que o interesse publico nesse tipo de divulgação seja sobreposto por outros interesses importantes, por exemplo, reabilitação de adolescentes em conflito com a lei. Nesses casos, alguns critérios podem orientar as decisões na análise dos casos concretos:

- Verificar se a informação é efetivamente de natureza privada. Indivíduos pressupõem que algumas informações suas sejam mantidas na privacidade, como detalhes sobre sua vida íntima e sexual, informações sobre sua saúde, informações bancarias ou detalhes de cartões de credito, informações de contato ou identificação (como senhas, números de contribuinte, etc), assim como outras informações de conteúdo sensível, como associação a grupos específicos, origem étnica ou racial; opiniões políticas, religiosas ou filosóficas também podem ser consideradas de natureza privada.
- Verificar se o individuo tinha uma expectativa razoável de privacidade em relação à informação reclamada. Por exemplo, verificar se ele nunca consentiu ou autorizou sua liberação publica, ou verificar se a informação já não é de conhecimento amplo e geral.
- Verificar se a informação questionada é de interesse publico. O interesse publico deve ser compreendido extensivamente e engloba informações que tenham impacto em assuntos de preocupação social, tais como: política, segurança e saúde publica, administração da justiça e cumprimento da lei, direitos e interesses dos consumidores, temas ambientais, assuntos

econômicos, exercício de poder, arte e cultura.

- Verificar se a informação questionada refere-se a uma pessoa publica. O direito internacional dos direitos humanos tem entendido que figuras publicas, em especial aqueles que exercem funções publicas, devem ter uma menor expectativa de privacidade. Figuras publicas estão mais sujeitas ao escrutínio publico e devem ser mais tolerantes a tal escrutínio, em razão de suas atividades. Mesmo alguns fatos sobe a vida privada de figuras publicas podem ser de interesse, por exemplo, do publico votante.
- Verificar se a informação é parte de um registro publico. Ou seja, ao analisar pedidos de direito ao esquecimento, deve-se verificar a natureza e origem da informação. É importante a preservação de material jornalístico, artístico e acadêmico, assim como informação de cunho estatal.
- Verificar se o demandante demonstrou dano significativo decorrente da disponibilidade da informação questionada.
- Verificar quão recente é a informação e se ela ainda possui valor por ser de interesse publico.

Vigilancia estatal de las comunicaciones (Fundación Karisma[160])

Una mirada a la retención de datos en América Latina y algunos retos del uso de herramientas de hacking

Carolina Botero[161] y Juan Carlos Castañeda[162]-

Introducción

Las preocupaciones por seguridad nacional y por la creciente actividad criminal en línea justifican la vigilancia de las autoridades a las tecnologías de la información y las comunicaciones (TIC), sin embargo, no cualquier actividad de inteligencia por los Estados es legal, ni legítima. Es necesario analizar las nuevas técnicas de vigilancia y revisar los marcos juŕidicos de los países para asegurarnos de que estén en línea con los derechos humanos.

La vigilancia estatal de las comunicaciones busca recaudar datos para la investigación de inteligencia o criminal. En ese proceso, las actividades se ocupan de la recolección, almacenamiento, procesamiento y circulación de datos y comprende diferentes técnicas. Entre las técnicas que más se habla están la interceptación de comunicaciones, la retención de datos y el uso de herramientas de hackeo (pruebas de penetración y explotación de vulnerabilidades de seguridad).

[160]Organización de la sociedad civil dedicada a apoyar y difundir el buen uso de las tecnologías en los entornos digitales, en procesos sociales y en las políticas públicas colombianas y de la región, desde una perspectiva de protección y promoción de los derechos humanos. Durante nuestra trayectoria hemos mantenido un interés constante en la convergencia de las TIC y el derecho, y en la promoción y participación ciudadana en relación a estos temas. En la actualidad, desarrollamos nuestra labor a través de los grupos de trabajo “Derecho, Internet y Sociedad” (DIS) y “El Laboratorio de Innovación y Tecnologías Sociales” (Lab. ITS). Fue fundada en el año 2003 y está localizada en Bogotá, Colombia. https://karisma.org.co/

[161] Investigadora, abogada, conferencista, escritora y consultora en temas relacionados con el derecho y la tecnología. Es directora de la Fundación Karisma.

[162] Abogado e investigador de la Fundación Karisma

Sin embargo, la falta de un proceso democrático en la creación de capacidades de vigilancia y el establecimiento de fuertes controles y medidas de transparencia hacen que estas capacidades se ubiquen fácilmente en el campo de la ilegalidad, y signifiquen el desarrollo de acciones altamente lesivas de derechos fundamentales, que puedan incluso llegar a comprometer las bases de la democracia.[163]

El presente documento analiza, en primer lugar, los marcos legales de Perú, México, Brasil, Colombia y Argentina sobre la forma como enfrentan los riesgos contra los derechos humanos en la retención de datos. El segundo capítulo se ocupa de hacer una mirada regional al uso de herramientas de hackeo como parte del sistema de vigilancia de las comunicaciones que, progresivamente, se han establecido en esta parte del mundo. Se aprovecha el reciente escándalo de Hacking Team para establecer cómo esta técnica es un nuevo reto de la región y se analizan los riesgos de esta práctica frente a un inexistente marco legal.

El propósito central es llamar la atención sobre la falta de garantías que existen en estos países para la protección de derechos humanos en desarrollo de la retención de datos y del uso de herramientas de hackeo. La base para establecer los estándares relevantes dentro del Sistema Interamericano de Derechos Humanos fue principalmente el Informe del año 2013 de la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA.

La investigación de los marcos legislativos en cada país tuvo como insumo de base los informes coordinados por Katitza Rodríguez de la Electronic Frontier Foundation para Perú[164], México[165], Brasil[166], Colombia[167] y Argentina[168].

Legitimidad de las restricciones

Según la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, las medidas que afectan las comunicaciones, en tanto restricciones a derechos fundamentales, deben ser acordes con estándares y

[163] CIDH (2013). *Libertad de expresión e internet*. OEA/Ser.L/V/II.149 Doc.50, Capítulo IV, párr. 154.
[164] Perú: Morachimo, M. Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú (Octubre, 2015). Electronic Frontier Foundation e Hiperderecho. Recuperado de: https://www.eff.org/files/2015/11/24/peru-es-final.pdf
[165] García, L. Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México (Octubre, 2015). Electronic Frontier Foundation y Red en Defensa de los Derechos Digitales. Recuperado de: https://www.eff.org/files/2015/11/24/mexico-es-final.pdf
[166] Antonialli, D. y de Souza Abreu, J. State Surveillance of Communications in Brazil and the Protection of Fundamental Rights (Septiembre, 2015). Recuperado de https://en.necessaryandproportionate.org/files/2015/12/03/brazil-en-dec2015.pdf
[167] Rivera, J. y Rodríguez, K. Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia (Mayo, 2015) Recuperado de: https://www.eff.org/files/2015/05/19/colombia-principios-may-14.pdf
[168] Ferrari, V. y Schnidrig, D. Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina (Octubre, 2015) Recuperado de: https://en.necessaryandproportionate.org/files/2015/12/04/argentina-sp-dec2015.pdf

principios planteados en distintos documentos internacionales y los Estados deben revisar y armonizar sus normas según ellos.

Por ejemplo, según el Informe sobre terrorismo y derechos humanos de la Comisión IDH, la Convención Interamericana sobre el Terrorismo, en últimas, busca defender el régimen democrático y, por tanto, obliga a los Estados a respetar el estado de derecho y los derechos y libertades fundamentales en la toma de medidas contra el terrorismo. De acuerdo con la Declaración Conjunta sobre programas de vigilancia y su impacto en la libertad de expresión, los Estados deben mantener bajo consideraciones de necesidad y proporcionalidad los programas de vigilancia de las comunicaciones para conseguir una limitación efectiva de su afectación a derechos humanos. Otros documentos a tener en cuenta son la Declaración Conjunta sobre Wikileaks y la Declaración Conjunta sobre Libertad de Expresión e Internet.

Dado que la retención de datos y el uso de herramientas de hackeo no solo afectan la libertad de expresión, sino también el derecho a la intimidad, es necesario tener en cuenta otros documentos internacionales. Según el Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la Libertad de Opinión y Expresión, se entiende que a pesar de que el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos no especifica las condiciones que debe seguir las limitaciones al derecho a la intimidad, es claro que toda limitación a este derecho debe cumplir con las garantías establecidas para otros derechos. Así pues, las limitaciones admisibles a la intimidad (a) deben ser legales, (b) no deben comprometer la esencia del derecho humano, (c) deben ser necesarias en democracia, (d) no deben ser discrecionales, (e) deben ser necesarias para un objetivo legítimo, y (f) deben ser proporcionales, adecuadas, las menos lesivas y deben guardar proporción con el interés protegido.

Por su parte, para la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, la legitimidad de las medidas de vigilancia de las comunicaciones deriva entonces del cumplimiento de ciertas condiciones decantadas de los distintos documentos del Sistema Interamericano de Derechos Humanos:[169]

1. Consagración legal
2. Búsqueda de una finalidad imperativa
3. Necesidad, idoneidad y proporcionalidad de la medida para alcanzar la finalidad perseguida
4. Debido proceso y reserva judicial

[169] *Supra*, Capítulo IV, párr. 55.

El Relator para libertad de expresión de la OEA, a propósito de las revelaciones sobre el uso de productos y servicios de la empresa italiana Hacking Team por parte de gobiernos alrededor del mundo,[170] expresó que:

> de acuerdo con los estándares internacionales, el uso de programas o sistemas de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en la ley, ser verdaderamente excepcional y selectivo, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos como la investigación de delitos graves definidos en la legislación.[171]

La intrusión en los dispositivos de las personas es una violación a su intimidad, pero también afecta su derecho a la libre expresión y opinión. Como afirma el Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, en la era digital, el ejercicio de estos derechos no se limita al fuero interno de las personas, también se ejerce en el uso de buscadores o en el almacenamiento de archivos que se encuentran en los dispositivos o en la nube.[172] De ahí que la falta de discusión democrática sobre el uso de herramientas de hackeo sea una urgencia.

Finalmente, distintas organizaciones de la sociedad civil lideraron un proceso en el que participaron también representantes de la industria y expertos en la materia para desarrollar los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones,* a partir de las conceptualizaciones que se han realizado en torno al derecho internacional de los derechos humanos en el entorno digital.[173] Los principios que deben regir la aplicación de medidas de vigilancia de las comunicaciones son: legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, autorización judicial competente, debido proceso, notificación del usuario, transparencia, supervisión pública, integridad de las comunicaciones y los sistemas, garantías para la cooperación internacional y garantías contra el acceso ilegítimo, y derecho a un recurso efectivo.

---

[170] *Infra*. Herramientas de hackeo.

[171] Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA (2015, 21 de julio). Comunicado de prensa sobre la adquisición e implementación de programas de vigilancia por parte de Estados del hemisferio. Recuperado de http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&IID=2.

[172] Kaye, D (2015). Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/29/32, párr. 20. Recuperado de: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

[173] *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*. Recuperado de https://es.necessaryandproportionate.org/text.

Retención de datos

Todo lo que se puede saber sobre una persona superó hace mucho tiempo su círculo social. Ahora la información personal se encuentra en bases de datos, que tiene diversos fines y son administradas por entidades públicas o privadas. Esas bases de datos están siendo alimentadas por flujos de información constantes. Su conjunto conforma un archivo sobre cada individuo, un "dossier personal".[174] Las tecnologías digitales de las que la vida moderna depende, como computadores personales, teléfonos celulares y demás, producen y registran datos constantemente. Los computadores registran a qué horas están encendidos, qué aplicaciones se usan, las páginas web que se visitan, el lugar donde se encuentran. Los celulares están todo el tiempo atentos a su ubicación geográfica, contienen registros de llamadas entrantes y salientes, mensajes de texto y fotos. La fuerza de cada uno de estos datos por separado no es mayor, pero su combinación puede llegar a revelar tanto sobre una persona que puede convertirse en una seria violación de sus derechos. Sin embargo, todo esto hace parte de una suerte de concesión que hacen las personas usuarias a cambio de recibir el servicio. El resultado, en términos del tipo de datos que producimos y quienes los administran, es que somos un "libro abierto para los gobiernos y las corporaciones".[175] De ahí que se necesite garantizar el respeto a los derechos humanos que pueden afectarse por estos flujos y usos de la información.

La provisión de servicios de telecomunicaciones es uno de los ámbitos donde se producen más datos y, gradualmente, más gobiernos obligan a estos proveedores a retenerlos y entregarlos para diversos propósitos. El interés de los gobiernos en este punto radica, principalmente, en que las personas usuarios tienen una relación de dependencia con las empresas de telecomunicaciones en dos niveles: (1) el de la provisión del servicio en sí misma, y (2) el de la salvaguarda de los datos que fluyen a través de la conexión.[176] Las obligaciones de retención buscan la conservación de los datos que generan las conexiones de telefonía fija, celulares o de Internet, estableciendo el tipo de datos a conservar por los operadores, el tiempo de retención y las condiciones, y los facultados para el acceso a esos datos.

Los datos que se recogen son, por ejemplo, el número que recibe una llamada, el tiempo de la llamada, la ubicación geográfica del dispositivo o sus identificadores únicos (IMEI e IMSI) en telefonía móvil o fija, y las direcciones IP en internet. Esto es, en un nivel simple, diferente de la recolección de las comunicaciones en sí

[174] Solove, D.J. (2004). *The digital person technology and privacy in the information age*. New York, U.S.: New York University Press.
[175] Schneier, B. (2015). Data and Goliath: the hidden battles to collect your data and control your world. New York, U.S.: W. W. Norton.
[176] Kerr, I.R., Gilbert, D. & McGill, J. (2006). The medium and the message: personal privacy and the forced marriage of police and telecommunications providers.*Criminal Law Quarterly*, 51(4).

mismas y, por tanto, han sido llamados “metadatos”, es decir, datos acerca de las comunicaciones. Esta clasificación puede llevar a concluir erróneamente sobre que los metadatos o los datos de identificación del suscriptor merecen una protección menor a la que está establecida para las comunicaciones en sí mismas.[177] La agregación de datos, en realidad, es más reveladora que el contenido de las comunicaciones.[178] Por esta razón, se ha establecido que la retención de datos es una medida que restringe y afecta los derechos a la intimidad y a la libertad de expresión.[179]

A continuación se desagregan los requisitos establecidos para la legitimidad de las restricciones a los derechos humanos y se analizan por separado respecto a los regímenes de retención de datos en Perú, México, Brasil y Colombia. Se menciona Argentina, cuando hay lugar a ello.

Legalidad

Una restricción a los derechos a la intimidad o a libertad de expresión como la que comporta la retención obligatoria de datos de telecomunicaciones debe (1) estar consignada en una ley en sentido formal y material, y (2) debe ser clara y precisa.[180]

Ley en sentido formal y material

Sobre el primer punto, está claro que solo se cumple el requisito cuando la restricción se impone a través de una norma adoptada por el órgano legislativo democráticamente elegido y según el procedimiento previsto en la constitución respectiva. Una disposición administrativa no satisfacería el requisito.

En los ordenamientos analizados, se encuentra una mezcla de regulaciones y leyes en sentido material que aplican distintos aspectos de la retención de datos.

Perú

La Ley No. 27.336 (2002) regula la conservación de registros fuentes del detalle de las llamas y facturación de los servicios. El Decreto Legislativo No. 1182 (2015) regula la retención de datos de tráfico y de identificación y localización de terminales. El Código Procesal Penal (Decreto Legislativo No. 957 de 2004) regula el acceso a la geolocalización de dispositivos por parte del organismo investigador.

---

[177] Electronic Frontier Foundation & American Civil Liberties Union Brief *Amicus Curiae* en Kalyman v. Obama,20 de agosto de 2014. Disponible en https://www.eff.org/document/eff-and-aclu-amicus-brief-klayman.

[178] Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2014). *El derecho a la privacidad en la era digital*. A/HRC/27/37, parr. 19.

[179] Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40, párr. 148

[180] *Supra* (nota 1), Capítulo IV, párr. 58.

México

El régimen de retención está enteramente consagrado en leyes en sentido formal y material a través de la Ley Federal de Telecomunicaciones y Radiodifusión (2014) y del Código Nacional de Procedimientos Penales (CNPP), que sustituye al Código Federal de Procedimientos Penales (CFPP).

Brasil

Se encuentran dos resoluciones administrativas que regulan la retención de datos de telefonía fija (Resolución No. 426/05 de ANATEL) y móvil (Resolución No. 477/07 de la misma entidad), la Ley No. 12.850 sobre retención y acceso a datos en ambas modalidades de telefonía, y la Ley No. 12.965 o Marco Civil de Internet, sobre retención y acceso a datos de tráfico de Internet.

Colombia

El Decreto No. 1704 de 2012 trata de la retención de datos para efectos de investigación criminal, mientras que la Ley No. 1621 de 2013 lo hace para efectos de actividades de inteligencia.

Argentina

Precisamente la diferencia entre este país y el resto es que en Argentina no hay consagración legal expresa de la retención de datos. Sin embargo, se encuentra vigente el Reglamento de calidad de los servicios de telecomunicaciones de la Secretaría de Comunicaciones (ahora Autoridad Federal de las Tecnologías de la Información y las Comunicaciones), que obliga a los prestadores a garantizar a la autoridad toda la información que estime pertinente para hacer las evaluaciones de calidad del servicio.[181] Así mismo, su artículo 8 obliga directamente a la conservación de los datos que recojan sus sistemas y que puedan servir para determinar la calidad del servicio.

La Ley No. 25.873 y su decreto reglamentario No. 1563 de 2004 obligaban a los prestadores de servicios de telecomunicaciones a "registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos" por el plazo de 10 años y para acceso del Poder Judicial o del Ministerio Público. Estas normas fueron declaradas como inconstitucionales por la Corte Suprema de Justicia por violar los requisitos de legalidad y necesidad y proporcionalidad.

El Tribunal consideró que resulta inadmisible la vaguedad de la invocación del interés general para sustentar las normas en cuestión, en vista de la afectación que comportan a los intereses de la ciudadanía.[182] Respecto al requisito de legalidad,

[181] Ministerio de Planificación Federal, Inversión Pública y Servicios (2013, 1 de julio). Resolución No. 5. Recuperado de http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm.

[182] Corte Suprema de Justicia (2009, 24 de Febrero). Halabi v. Estado Nacional.

opinó que no está claro qué son datos de tráfico, por tanto, podría confundirse con el contenido de la comunicación. Además, determinó que no había claridad sobre las condiciones y las autoridades que tendrían acceso a los datos. Dejó claro que, en todo caso, el acceso a los datos requeriría autorización judicial.

También se pronunció respecto a la proporcionalidad de la medida y dijo que "no es dudoso que la norma en cuestión pone bajo sospecha a todos los usuarios de los servicios de telecomunicaciones por el amplísimo término de 10 años", lo que se agrava en el ámbito de las comunicaciones digitales porque allí "todos los movimientos quedan registrados". Señaló, además, que la medida no era admisible porque, aunque no todos los procedimientos podrían ameritar su uso, no está claro para qué procedimientos judiciales estaba autorizada.

Claridad

Los regímenes de retención de datos deberían ser claros respecto al tipo de datos afectados por la medida y al tiempo por el que deben ser retenidos. En lo que se refiere al acceso a datos de localización, debido a que buscan ubicar un equipo, solo se habla de la posibilidad de su consulta en tiempo real, siendo México la única excepción, pues exige que estos datos también sean conservados.

Perú

En general, la Ley No. 27.336 ordena a los prestadores del servicio de telecomunicaciones la conservación por 3 años de "los registros fuentes del detalle de las llamadas y facturación de los servicios que explota".[183] La Resolución de OSIPTEL usa términos similares y obliga a una conservación mínima de 2 meses.[184] El Código Procesal Penal, por su parte, se refiere simplemente a la "geolocalización de teléfonos móviles".[185]

El Decreto Legislativo No. 1182 no hace ninguna descripción de lo que se entiende por "datos derivados de las telecomunicaciones", ni tampoco sobre qué comprende los datos de localización.[186] Los plazos que señala para la conservación de los datos de tráfico son 12 meses en un sistema que permita consulta y entrega en línea y en tiempo real, y 24 meses en sistema de almacenamiento.

México

La LFTR hace una lista exhaustiva de los datos materia de retención que va desde los datos del suscriptor hasta el registro de la hora de inicio y finalización de la

[183] Ley No. 27.336, artículo 16, literal e.
[184] Resolución de Consejo Directivo No. 138-2012-CD-OSIPTEL, artículo 65.
[185] Código Procesal Penal, artículo 230, numeral 4.
[186] Decreto Legislativo No.1182, primera y segunda disposición final complementaria.

comunicación y los números involucrados.[187] En este caso sí es clara la obligación de registrar la ubicación geográfica de los dispositivos. Por su parte, el CFPP establece que los prestadores entregarán "la localización geográfica, en tiempo real".[188] El Código Nacional de Procedimientos Penales, que reemplazará al CFPP, establece la misma obligación en términos similares.[189]

La LFTR ordena la conservación de los mencionados datos por 12 meses a través de acceso a un sistema de consulta y entrega en tiempo real.[190] Pasado este tiempo, los datos deben conservarse otros 12 meses en archivo.

Brasil

Las telecomunicaciones afectadas por la medida de retención son claramente la telefonía fija y móvil, e internet. Sobre los tipos de datos, para telefonía fija, se exige vagamente la retención de "todos los datos relativos a la prestación del servicio, incluidos los de facturación".[191] Para el servicio de telefonía móvil, deben retenerse la información del suscriptor, los registros de llamadas entrantes y salientes, las fechas de las llamadas y la duración de estas.[192]

La Ley sobre organizaciones criminales ordena a las concesionarias de telefonía fija y móvil, la conservación del "registro de identificación de los números de las terminales de origen y destino de conexiones telefónicas internacionales, interurbanas y locales".[193] En todos los casos anteriores, el tiempo de la retención es de 5 años.

Respecto a Internet, el Marco Civil ordena varios tipos de retención.[194] Por un lado, quien provea conexión a Internet debe conservar los datos de conexión, que incluye la fecha y hora de inicio y finalización de la misma y la dirección IP de la terminal usada para la conexión por 1 año.[195] Por otro, los proveedores de aplicaciones de Internet con personería jurídica y con ánimo de lucro deben conservar los registros

[187] El artículo 190 III ordena la retención de: nombre o denominación del suscriptor, el tipo de comunicación (voz, buzón, conferencia o datos), los servicios suplementarios (como reenvío o transferencia de llamada) o servicios de mensajería o multimedia, los necesarios para rastrear e identificar el origen y destino de la comunicación móvil: número de destino y modalidad de contrato, los necesarios para determinar fecha, hora y duración de la comunicación o mensaje, fecha y hora de la primera activación del servicio y "etiqueta de localización (identificador de celda)" desde la que se activó, "[e]n su caso identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor", y la "[u]bicación digital del posicionamiento geográfico de las líneas telefónicas".
[188] Código Federal de Procedimiento Penal, artículo 133 Quáter.
[189] Código Nacional de Procedimientos Penales, artículo 303.
[190] Ley Federal de Telecomunicaciones y Radiodifusión, artículo 190 III.
[191] Resolución No. 426 de 2005, artículo 22.
[192] Resolución No. 477 de 2007, artículo 10 XXII.
[193] Ley No. 12.850 de 2013.
[194] Ley No. 12.965 de 2014 (Marco Civil), artículo 13; Resolución 614 de 2013, artículo 53.
[195] *Supra*, artículo 5-IV.

de acceso a aplicaciones de Internet, fecha, hora y la dirección IP de uso por 6 meses.[196] Adicionalmente, deben conservar la información de suscripción.[197]

Colombia

Para efectos de investigación criminal, se obliga a los proveedores de servicios de telecomunicaciones a conservar "los datos del suscriptor, tales como identidad, dirección de facturación y tipo de conexión" y datos que permitan saber la localización de terminales en tiempo real "tal como sectores, coordenadas geográficas y potencia, entre otras".[198] Para efectos de actividades de inteligencia, se habla del "historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recae la operación" y de "la localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización".[199] No está claro qué significa "historial de comunicaciones" ni el alcance de las cláusulas generales empleadas en estas normas (p. ej "entre otras" o "cualquier otra información"). Sobre el tiempo, en ambos casos los datos deben ser retenidos por el término de 5 años, aunque no está claro si los datos de localización deben ser registrados para posterior consulta.

Por otro lado, no está claro si la obligación de retención aplica también a los datos de tráfico de Internet, pues, aunque los artículos relevantes, tanto del Decreto 1704 como de la Ley 1621, se dirigen a los "proveedores de redes y servicios de telecomunicaciones" u "operadores de servicios de telecomunicaciones", los datos que obliga aplican a la telefonía móvil o fija.

Hechos y autoridades

Lo que se busca con este criterio es que la retención de datos sea clara respecto a las circunstancias que ameritan la recolección o el acceso a los datos, sobre las autoridades facultadas para acceder, las condiciones que deben comprobarse para realizar el acceso y las autoridades a quienes corresponde el control de la medida.

Perú

La Ley No. 27.336, en su artículo 15, establece que OSIPTEL podrá acceder a los datos retenidos en uso de sus facultades de supervisión. Por su parte, la Segunda disposición complementaria final del Decreto Legislativo No. 1182 adolece de claridad respecto a las autoridades que pueden acceder a los datos, aunque se puede interpretar que se trata de la Policía Nacional, pues una de las motivaciones del Decreto es aumentar la capacidad operativa de este organismo. Tampoco hay

[196] *Supra*, artículos 15 y 15-VIII.
[197] *Supra*, artículo 10(3); Resolución No. 614 de 2013, artículo 53.
[198] Decreto No. 1704 de 2012, artículos 4 y 5.
[199] Ley No. 1621 de 2013, artículo 44.

una determinación de las condiciones de acceso a estos datos como sí la hay para los datos de geolocalización.

Respecto a los datos de geolocalización, el artículo 4 del Decreto Legislativo No. 1182 determina que una unidad especializada de la Policía para la petición de datos podrá acceder cuando concurran las siguientes condiciones, recogida en el artículo 3: (1) cuando se trate de flagrancia, (2) cuando el delito investigado sea sancionado con pena superior a los cuatro años de privación de libertad, y (3) cuando el acceso a los datos constituya un medio necesario para la investigación. La Fiscalía, por su parte, podrá acceder a los datos de geolocalización cuando investigue la posible comisión de una conducta sancionada con una pena privativa de la libertad mayor a 4 años y bajo la convicción de su absoluta necesidad.[200]

El Proyecto de Ley No. 4809/2015-CR, que busca derogar el Decreto Legislativo No. 1182, establece que el Ministerio Público es el único que puede pedir los datos al Juez Penal.

En cualquier caso, vale la pena anotar que puede haber una cláusula general de acceso a esa información en el artículo 42.1 del Decreto Legislativo No. 1141 sobre fortalecimiento del sistema de inteligencia cuando establece que cualquier entidad de la administración pública debe entregar información que sea requerida por las autoridades de inteligencia. En el mismo decreto, en su artículo 42.5, está establecido que la información protegida por la intimidad o el secreto profesional, personal o familiar está exenta de ese deber de colaboración. En todo caso, no es claro si los datos de tráfico que se retienen en virtud de la Ley No. 27.336 estén cobijados por la excepción del artículo 42.5.

México

La Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) trae una cláusula general, en su artículo 189, según la cual los "proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes". Tanto los datos de tráfico como los de localización deben ser entregados según la LFTR, de forma vaga, a "las autoridades competentes", lo que incluye las "instancias de seguridad y procuración de justicia", por remisión al artículo 189 (fracción III del artículo 190, inciso primero).

Específicamente, el Código Federal de Procedimientos Penales (Art 133 Quáter) determina que la Procuraduría General de la República puede solicitar el acceso a datos de geolocalización en tiempo real cuando se investiguen hechos de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas.

[200] Código Procesal Penal, artículo 230, numerales 1 y 4.

Sin embargo, el artículo 291 Código Nacional de Procedimientos Penales, que reemplazará al CFNP, deja abierta la posibilidad a que cualquier investigación haga uso del acceso a datos de localización.

Brasil

En general, ANATEL, en tanto autoridad de telecomunicaciones, puede acceder a los datos de telefonía fija y móvil.[201] Igualmente puede hacerlo la autoridad de impuestos y aduanas –Secretaria da Receita Federal do Brasil.[202]

La Ley 12.850/13, aunque se refiere al crimen organizado, no especifica que sea éste tipo de investigación la única que amerita el acceso a datos retenidos. Las autoridades que pueden acceder a estos datos son la Policía y el ente de investigación criminal –Ministerio Público (Art. 15). Las Comisiones Parlamentarias de Investigación también pueden acceder a los datos retenidos.[203]

El Marco Civil de Internet no especifica las autoridades que pueden acceder a la información retenida. Por una parte, establece en su artículo 10, párrafo 3, que las "autoridades administrativas que tengan competencia legal" podrán acceder a la información del suscriptor. De otra, el artículo 22 establece que el acceso a registros de conexión y acceso a aplicaciones de Internet serán autorizados a "la parte interesada" en la recolección de material probatorio en investigaciones civiles o penales.

Colombia

En cuanto a investigación penal, no hay una restricción respecto a los delitos cuya investigación amerita el acceso a los datos retenidos. Por otro lado, la orden de entrega debe provenir de la Fiscalía General de la Nación, que es titular de la acción penal y encargado de la investigación). La ejecución de la orden está en manos del "grupo de Policía Judicial" designado.[204] En cuanto a las actividades de inteligencia, la única restricción que impone la norma es la existencia de una "operación autorizada", aunque no hay forma de determinar qué hechos ameritan el desarrollo de una operación de inteligencia ni quién puede autorizarla. Además, con una norma tan ambigua, hay un buen número de autoridades que podrían legítimamente solicitar esta información por ser parte de la comunidad de inteligencia.[205]

---

[201] Ley No. 9472 de 1997, artículo 8.
[202] Ley No. 8218 de 1991, artículo 11.
[203] Supremo Tribunal Federal. Mandado de Segurança 23452/RJ.
[204] Decreto No. 1704 de 2012, artículos 4 y 5.
[205] En Colombia, son agencias de inteligencia: la Dirección Nacional de Inteligencia, la Unidad de Información y Análisis Financiero, la Dirección de Inteligencia de la Policía y las correspondientes jefaturas dentro del Comando General de las Fuerzas Militares, el Ejército Nacional, la Armada Nacional y la Fuerza Aérea. *Véase* el Decreto No. 857 de 2014.

Objetivos imperativos

Solo se puede restringir derechos para alcanzar ciertos objetivos imperativos autorizados por la Convención Americana. Estos objetivos son (1) protección de los derechos de los demás, (2) seguridad nacional, (3) orden público, (4) salud pública, y (5) moral pública. La interpretación de estos objetivos debe estar de acuerdo con los principios de una sociedad democrática. Es decir, los Estados no pueden interpretarlos libremente.[206]

La protección de los derechos de los demás requiere que la amenaza sea clara y que la medida no se imponga para proteger los mismos derechos que afecta. Asimismo, debe recurrirse a medidas menos restrictivas antes de afectar derechos.[207]

El mantenimiento del orden público, en tanto "condiciones que aseguran el funcionamiento armónico y normal de las instituciones sobre la base de un sistema coherente de valores y principios", requiere la demostración de "causas reales y objetivamente verificables, que planteen una amenaza cierta y creíble de una perturbación potencialmente grave de las condiciones básicas para el funcionamiento de las instituciones democráticas". No valen, entonces, la justificación sobre hechos o situaciones hipotéticas o amenazas sin el adecuado nivel de gravedad.[208]

La seguridad nacional, por su parte, no debe definirse en términos incompatibles con una sociedad democrática. Por ejemplo, justificando ataques a disidentes políticos, periodistas o defensores de derechos humanos con objetivos políticos o para entorpecer su trabajo. Los criterios para considerar que un caso amerita aplicación de la medida deben estar claramente definidos.[209]

Como se puede deducir del análisis del requisito de legalidad, las legislaciones estudiadas no obedecen completamente el requisito de la persecución de objetivos imperativos para la imposición de la medida de retención de datos. Por ejemplo, las regulaciones de Brasil (resoluciones no. 426/05 y 477/07) y Perú (Ley No. 27.336) ordenan la medida para efectos de control de las empresas de prestación de servicios de telecomunicaciones, a la vez que garantizan el acceso a esos datos a organismos de seguridad. La legislación mexicana simplemente ordena la retención de datos en el marco de una ley que regula de manera general el sector de las telecomunicaciones, sin hacer una referencia expresa a los motivos de la retención.

---

[206] CIDH, *op. cit.* (nota 1), Capítulo IV, párr. 157; CIDH (2009). *Informe anual de la Relatoría Especial para la Libertad de Expresión.* OEA/Ser.L/V/II Doc.51, Capítulo III, párr. 76.
[207] *Supra*, Capítulo III, párr.77-80.
[208] *Supra*, Capítulo III, párr. 81-83.
[209] *Supra* (nota 1), Capítulo IV, párr. 60 y 157.

La legislación colombiana, aunque impone la retención y garantiza el acceso a datos solo en el marco de una investigación criminal o las actividades de inteligencia, está muy lejos de determinar con claridad la amenaza a la seguridad nacional o al orden público que la medida puede llegar a minimizar. Se observa que las agencias de inteligencia pueden tener acceso a los datos retenidos a través de cláusulas generales, lo que efectivamente implica la imposición de medidas de restricción con objetivos que no son imperativos ni urgentes y la violación del principio de legalidad. Por tanto, no hay ninguna certeza sobre el alcance y los hechos que justifican la medida. México se destaca por tener en la Ley de Seguridad Nacional una lista de qué se considera que son amenazas a la seguridad nacional (Art.5).

El siguiente requisito trata de la necesidad, idoneidad y proporcionalidad de una medida para alcanzar los objetivos imperativos. De ahí que, si la conexión entre la medida y los objetivos no es suficiente, como es el caso de las legislaciones analizadas, la posibilidad de demostrar satisfactoriamente la necesidad, idoneidad y proporcionalidad de una medida es muy reducida.

Necesidad, Idoneidad y Proporcionalidad

La necesidad de una medida de restricción de derechos debe ser cierta e imperiosa, lo que, además, impone una demostración más allá de lo simplemente útil, razonable u oportuno para alcanzar los objetivos imperativos. Además, la medida debe estar limitada a lo indispensable para alcanzar el objetivo por lo cual debe considerarse la imposición de medidas menos restrictivas. Por tanto, la medida debe estar autorizada solo para casos excepcionales.[210]

La retención de datos, por naturaleza, y tal como aparece en las legislaciones analizadas, es una medida que afecta los derechos a la intimidad y a la libertad de expresión, entre otros, y opera de manera constante sobre los datos de las personas usuarias de servicios de comunicaciones. Esa pasividad de la medida excluye por completo el requisito de necesidad, pues no opera solo en casos excepcionales. Por otro lado, la vaguedad con la que está consagrado en las normas el acceso a los datos retenidos tampoco permite hablar de excepcionalidad en el uso de la medida. En Colombia, se puede acceder a todos los datos que se debe retener para la investigación de cualquier delito o para cualquier situación que los organismos de inteligencia consideren necesaria. Lo mismo sucederá en México cuando entre a regir el Código Nacional Procesal Penal. En Perú y Brasil, las cláusulas generales de colaboración con los organismos de inteligencia impiden determinar cuáles son los casos excepcionales en los que se usará la medida.

[210] *Supra* (nota 39), Capítulo III, párr. 85-87 & *Supra* (nota 1), Capítulo IV, párr. 64, 160 y 162.

El requisito de idoneidad busca que la medida sea "efectivamente conducente para obtener los objetivos legítimos e imperiosos que mediante ella se persiguen".[211] Como queda claro del análisis, la falta de precisión en los términos de la medida y la ausencia de conexión fuerte entre ella y los objetivos imperativos impide determinar su idoneidad.

La proporcionalidad de una medida se establece a partir de la evaluación de (1) el grado de afectación a derechos que supone la medida, (2) la importancia de satisfacer el derecho protegido por la medida, y (3) si tal satisfacción de ese derecho justifica la restricción de los otros.[212] La aplicación de medidas de vigilancia de las comunicaciones deberá autorizarse solo ante la presencia de riesgo cierto contra los derechos protegidos (seguridad, por ejemplo), y cuando el interés de la sociedad en mantener esos derechos sea superior al de mantener los derechos que afecta.[213]

Establecer la proporcionalidad de la medida en cada legislación de forma abstracta es difícil, ya que requiere de la evaluación de sus contextos sociales, culturales y legales particulares. Sin embargo, debe tenerse en cuenta en este punto que estas legislaciones implican la retención de todos o de algunos de estos datos: información de la persona suscrita al servicio, datos de tráfico de comunicaciones fijas, móviles y de Internet, y la localización de las terminales; que el número de autoridades que pueden acceder a ellos es amplio y que los motivos que justifican el acceso tampoco son claros. Además, el tiempo de retención parece ser arbitrario. En Colombia, la única mención es a 5 años, lo que obligaría a pensar que se refiere a cualquier tipo de datos. En Perú, se establecen 3 años, mientras que en México son 2 años. En Brasil, los datos de telefonía móvil o fija deben retenerse por 5 años y los de Internet por 1 año.

Por el momento, solo en Brasil se está discutiendo ante las Cortes la legalidad y proporcionalidad de la medida de retención impuesta en la Ley No. 12.850 sobre crimen organizado, pues, a juicio de las personas accionantes, no hay claridad respecto a la necesidad de autorización judicial para el acceso a datos de tráfico, situación que aprovechan las autoridades para exigir toda clase de datos retenidos por los operadores.

Los argumentos con los que el Tribunal de Justicia de la Unión Europea declaró la invalidez de la Directiva 2006/24/EC sobre retención de datos son relevantes, pues apuntan a muchos de los problemas que tienen los regímenes de retención de datos

---

[211] *Supra* (nota 39), Capítulo III, párr. 88.
[212] *Supra* (nota 1), Capítulo IV, párr. 90.
[213] Relator Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de opinión y de expresión & Relatora Especial para la libertad de expresión de la CIDH de la OEA (2013, 21 de junio). *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*. Punto 9.

analizados en este documento.[214] Sobre la proporcionalidad de la medida, señala el fallo que su población objetivo resulta ser cualquier persona que haga uso de medios de comunicación, es decir, toda la población europea. En ese contexto, el Tribunal no encuentra que haya límites a la aplicación de la medida en función del objetivo que persigue. En particular, no hay límites a las zonas geográficas, personas o tipos de comunicaciones sujetas a la medida en relación con el objetivo que persigue o la gravedad de los hechos que se investigan.

Descontando la legitimidad de la retención de datos para efectos de control de los prestadores del servicio de telecomunicaciones (Perú y Brasil) o para efectos indeterminados (México), no se encuentran límites adecuados a la medida cuando se emplea para investigación criminal y para suministrar información a los organismos de inteligencia. No existe ningún tipo de límite respecto a las personas ni al tiempo que pueden ser afectadas. En Colombia ni siquiera hay una limitación respecto al tipo de delitos cuya investigación puede servirse de datos retenidos.

En estas condiciones, la proporcionalidad de la retención de datos queda claramente cuestionada, pues los intereses de la sociedad en la investigación de los delitos, por sí mismos, no justifican una afectación de semejante magnitud en los derechos a la intimidad y a la libertad de expresión de las personas donde esta se encuentra vigente. A esto debe sumarse que la efectividad de la retención de datos radica, si acaso, en la facilitación de la investigación de hechos pasados, aunque poco pueda hacer para prevenir la comisión de crímenes en el futuro.[215]

Debido proceso y reserva judicial

Una medida de restricción de derechos, para ser legítima, debe respetar "las garantías vinculadas al debido proceso y a la reserva judicial".[216] Esto comprende, en general, la posibilidad de autorización y control judicial, la notificación a la persona usuaria afectada por la medida y la presentación de informes de transparencia sobre el empleo de la medida.

Reserva judicial

Las normas sobre retención de datos deberían ser claras respecto a las condiciones que admiten el acceso a los datos retenidos y las autoridades que pueden hacerlo. Cuando existen estos requisitos, son las autoridades judiciales las llamadas a decidir si la medida es: idónea para alcanzar el objetivo, suficientemente restringida para no vulnerar derechos más de lo necesario, y proporcional respecto al interés

[214] Tribunal de Justicia de la Unión Europea (2014, 8 de abril). *Sentencia Digital Rights Ireland*, párr. 56, 57, 59 y 63.
[215] Breyer, P. (2005). Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR. *European Law Journal*, 11(3).
[216] *Supra* (nota 1), Capítulo IV, párr. 65.

defendido.[217] En pocas palabras, son las autoridades judiciales quienes deben velar por la aplicación de las medidas que restringen derechos en el marco constitucional y democrático.

A diferencia de la interceptación de comunicaciones, la retención de datos es automática y abarca a toda la población. Por tanto, la actividad misma de recolección de datos no está mediada por una valoración judicial de su necesidad y proporcionalidad. Por su parte, el control judicial del acceso a los datos retenidos o a los datos de geolocalización varía de país a país.

Perú

Los datos de tráfico no requieren ningún tipo de autorización judicial cuando son usados por OSIPTEL dentro de sus facultades de supervisión de acuerdo a la Ley No. 27.336. En cambio, cuando la policía solicite acceso a los datos de tráfico retenidos, según la Segunda disposición complementaria final del Decreto No. 1182, se requiere autorización judicial previa.

El acceso a la geolocalización de terminales cuando lo solicita la Policía Nacional en el marco del Decreto Legislativo No. 1182 requiere convalidación ante un juez (Art.5). Cuando la geolocalización directamente la solicita el Ministerio Público, debe haber autorización judicial previa.[218]

El Proyecto de Ley No. 4809/2015-CR, que busca derogar el Decreto No. 1182, establece que para obtener los datos de geolocalización se requiere autorización judicial previa.

En cuanto al acceso a datos retenidos por parte de los organismos de inteligencia, el artículo 32 del Decreto No. 1141 impone la autorización judicial previa para los "procedimientos especiales de obtención de información". En caso de peligro contra la seguridad nacional y circunstancias urgentes, el Director de Inteligencia Nacional podrá autorizar la medida de obtención de información y convalidarla ante el juez competente dentro de las 24 horas siguientes (Art. 33.5).

México

El acceso a datos de tráfico retenidos en virtud de la Ley Federal de Telecomunicaciones y Radiodifusión no requiere autorización judicial.

El acceso a datos de geolocalización en medio de investigaciones relacionadas con delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas no requiere autorización judicial según el artículo 133 Quáter del Código Federal de Procedimientos Penales. El Código Nacional de Procedimientos Penales,

[217] *Supra* (nota 1), Capítulo IV, párr. 165.
[218] Código Procesal Penal, artículo 230, numeral 4.

especialmente sus artículo 291 y 303, representa un avance en este sentido, pues impone la necesidad de autorización judicial previa.

Brasil

Según la Ley No. 12.850 no es necesaria la autorización judicial para obtener la información del suscriptor. No es suficientemente claro que el acceso a datos de tráfico requiera autorización judicial. Este argumento es parte de la Acción Directa de Inconstitucionalidad 5063/DF que está pendiente de decisión.

El acceso a los registros de conexión y aplicaciones de Internet será autorizado por un juez solo para investigaciones penales o civiles cuando haya (1) indicio fuerte de culpabilidad, (2) justificación de la utilidad de los registros en la investigación, y (3) se especifique el período por el cual se solicitan los registros.[219]

Colombia

El acceso a los datos retenidos o a la geolocalización de dispositivos no requiere ningún tipo de autorización judicial. Tampoco está sometida a control judicial posterior ni en el contexto de la investigación criminal ni en el de las actividades de inteligencia.

Notificación a la persona usuaria

Este requisito también incluye las garantías procesales para que las personas afectadas por la medida puedan defenderse adecuadamente.[220] Por tanto, notificar a la persona usuaria es parte esencial de su defensa, ya que o de otra manera no podría saber si ha sido vigilado y presentar los recursos adecuados para mitigar los efectos de la vigilancia.

El único país que prevé la notificación a la persona usuaria en un caso es Perú, en específico, para los casos de acceso a datos de localización a través del procedimiento del artículo 230 del Código Procesal Penal. Tal notificación está contemplada para realizarse posteriormente a la puesta en marcha de la medida y solo "si el objeto de la investigación lo permitiere y en tanto no pusiere en peligro la vida o la integridad corporal de terceras personas", asunto que determinará el juez correspondiente (Art. 231). Sin embargo, este procedimiento no está establecido en el Decreto No. 1182 ni en la Ley No. 27.336.

Transparencia

Para efectos de que las actividades de vigilancia de los Estados sean transparentes y que la ciudadanía pueda ejercer el debido control, se requiere que los Estados publiquen "información global sobre el número de solicitudes de intercepción y

[219] *Marc Civil*. Ley No.12.965 de 2014, artículos 10(3), 13(5), 15(3) y 22.
[220] *Supra* (nota 1), Capítulo IV, párr. 164.

vigilancia aprobadas y rechazadas, incluyendo la mayor cantidad de información posible como – por ejemplo – un desglose de solicitudes por proveedor de servicios, tipo de investigación, tiempo durante el cual se extienden las investigaciones, etcétera". [221] Asimismo, los proveedores de servicios de telecomunicaciones deberían publicar informes donde especifiquen qué procedimientos siguen cuando reciben una solicitud de las autoridades, el tipo de solicitudes y su cantidad.[222]

México es el único país que dispone sobre la publicación de informes de transparencia. EL Artículo Art 70 XLVIII de la La Ley General de Transparencia y Acceso a la Información Pública obliga a las autoridades a publicar el listado de solicitudes que han hecho a concesionarios y proveedores de servicios y aplicaciones de Internet respecto a intervención de comunicaciones y registros de datos y geolocalización. El informe debe contener, a saber,: el objeto de la intervención, el alcance temporal, sus fundamentos legales y la existencia de autorización judicial, cuando sea el caso.

Los prestadores de servicios de telecomunicaciones podrían estar obligados a presentar un informe semestral sobre las solicitudes de acceso a datos de tráfico y de geolocalización, especificando el número de solicitudes recibidas, aceptadas y rechazadas. Esto sería así si queda en firme el lineamiento décimo cuarto del Borrador de "Lineamientos de colaboración en materia de seguridad y justicia", que presentó el Instituto Federal de Telecomunicaciones a partir de la facultad que le otorga el artículo 190 I de la LFTR.

Herramientas de hackeo: retos del futuro en la protección de los derechos humanos

Internet está siendo afectado por todo tipo de medidas de control que determinan hasta qué punto es un medio libre, abierto y seguro. Ron Deibert clasifica los controles de la siguiente forma.[223] Existen, por un lado, sistemas de corte defensivo de filtrado o bloqueo de contenidos (primera generación. Posteriormente, se han creado controles que implican una profundización de sus capacidades al interior de la sociedad a través de la colaboración de los gobiernos con el sector privado, imponiendo o solicitando acceso a "puertas traseras" en el hardware o software, estableciendo mayores requisitos para el acceso a Internet, como el registro con datos biométricos, o como la prohibición de herramientas de seguridad y cifrado (segunda generación).

Actualmente, los controles también son ofensivos e incluyen el uso de ataques dirigidos por parte de los gobiernos, a través de capacidades propias o empleando

[221] *Supra* (nota 1), Capítulo IV, párr. 168.
[222] *Supra* (nota 1), Capítulo IV, párr. 168 y 169.
[223] Deibert, R. (2015). Cyberspace under siege. J*ournal of Democracy*, 26(3).

tecnologías del sector privado como las que ofrece Hacking Team. Los Estados, entonces, han estado adquiriendo capacidades tecnológicas para acceder subrepticiamente a dispositivos electrónicos y obtener información de ellos, e incluso encender las cámaras o los micrófonos y registrar lo que ellos perciben[224], con propósitos que van desde la investigación criminal hasta la supresión de la disidencia, pasando por la recopilación de información para inteligencia.[225]

Aunque en la región estas herramientas han hecho presencia, no ha habido un debate sobre su legitimidad ni sobre los retos que estas actividades suponen para los marcos legales de derechos humanos en nuestros países.

De otra parte, se afirma que el uso de estas herramientas por parte de las autoridades de vigilancia es una necesidad para la lucha contra el crimen y el terrorismo, pues iguala las capacidades de la delincuencia con las de la autoridad.[226] Incluso, hay quienes sostienen que el uso de herramientas de hackeo puede ser legítimo en la medida que exista una orden judicial para aprovechar vulnerabilidades de sistemas informáticos. La legalización y aplicación de controles judiciales a esta actividad podría tener el efecto de poner límites a esta actividad, así como minimizar sus efectos negativos. Esta alternativa evitaría la creación de nuevas vulnerabilidades, pues solo explota las que ya existen y aliviaría la presión sobre fabricantes o prestadores de servicios para colaborar con los gobiernos.[227]

Hacking Team en América Latina

En América Latina, solo hasta el 2015, la ciudadanía estableció que las herramientas de hackeo forman parte del portafolio de actividades de las autoridades de vigilancia de la región.

---

[224] LaRue, F. (2013). *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión*. A/HRC/23/40,p. 37.

[225] *Véase*, por ejemplo, McCullagh, D. (2007). *Feds use keylogger to thwart PGP, Hushmail. CNET*. Recuperado de http://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail/; Nagaraja, S., & Anderson, R. (2009). T*he snooping dragon: social-malware surveillance of the Tibetan movement. University of Cambridge Computer Laboratory;* Glance, D. (2011, 11 de octubre). Ein spy: is the German government using a trojan to watch its citizens? *The Conversation*. Recuperado de https://theconversation.com/ein-spy-is-the-german-government-using-a-trojan-to-watch-its-citizens-3765-.

[226] Vincenzetti, D. (2015, 29 de julio). Terrorists and criminals have a lot less to worry about since we were hacked. *International Business Times*. Recurperado de: http://www.ibtimes.co.uk/hacking-team-ceo-terrorists-criminals-have-lot-less-worry-about-since-we-were-hacked-1513148. Vicenzetti es el CEO de la compañía italiana Hacking Team.

[227] Bellovin S.M., et al. (2014). Lawful hacking: using existing vulnerabilities for wiretapping on the internet. *Northwestern Journal of Technology and Intellectual Property*. 12, p. 1. Recuperado de http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1.

En marzo de 2013, un informe del CitizenLab documenta por primera vez el uso software Finfisher en México.[228] Poco después, en abril del mismo año, un nuevo informe de esa organización mostraba la ampliación de su uso a Panamá.[229] En el último reporte de octubre de 2015, el CitizenLab muestra como Finfisher está siendo utilizada también por Venezuela y Paraguay.[230] De otra parte, desde febrero de 2014, gracias a otra investigación del CitizenLab, se conoce del uso de un malware comercializado por Hacking Team en por los menos tres países de la región: México, Panamá y Colombia.[231] Las revelaciones de 2015 sobre las filtraciones a la empresa italiana Hacking Team confirmaron esa investigación, e incluso se estableció que la extensión del uso de esta herramienta en la región era mucho mayor de lo reportado inicialmente.[232] Se supo también que Ecuador, Chile y Honduras, en algún momento, habían adquirido o utilizado este software,[233] que Brasil había conseguido las autorizaciones correspondientes para usarlo y pensaba utilizarlo como mecanismo de vigilancia en las próximas olimpiadas,[234] que en Perú se realizaron demostraciones,[235] y que en Argentina también se estaban haciendo acercamientos.[236]

La reacción de los gobiernos de la región ante estas revelaciones ha sido diversa. En Colombia, la Policía Nacional, en un comunicado a medios de comunicación, no negó su uso pero rechazó tener relaciones con Hacking Team. La policía colombiana afirmó que no ha sostenido vínculo comercial con la firma Hacking Team, aunque admitió que "adquirió una herramienta tecnológica con la empresa Robotec Colombia S.A.S, que ofrece equipos para la seguridad. El propósito de esta

---

[228] Marquis-Boire, M. et al. (2013). *For their eyes only: the commercialization of digital spying*. Toronto: Canadá: Citizen Lab. Recuperado de https://citizenlab.org/2013/04/for-their-eyes-only-2/.

[229] Marquis-Boire, M. et al. . (2013). *You only click twice: FinFisher's global proliferation*. Toronto, Canadá: University of Toronto. Recuperado de https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

[230] Marczak, B. et al. (2015, 15 de octubre). *Pay no attention to the server behind the proxy: mapping FinFisher's continuing proliferation*. Toronto, Canadá: CitizenLab. Recuperado de https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/.

[231] Marczak, B. et al. (2014). Mapping Hacking Team's "untraceable" spyware. Toronto, Canadá: Citizen Lab, p. 17. Recuperado de https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

[232] Cuando hackean a los hackers (2015, 11 de julio). *Revista Semana*. Recuperado de http://www.semana.com/nacion/articulo/los-lios-de-hacking-team-por-informacion-hackeada/434391-3

[233] Fundación Karisma (2015, 7 de julio). *Sociedad civil de América Latina rechaza software espía de Hacking Team*. Recuperado de https://karisma.org.co/sociedad-civil-de-america-latina-rechaza-software-espia-de-hacking-team/.

[234] Viana, N. (2015, 27 de julio). Hackeando o Brasil. *Agencia Pública*. Recuperado de http://apublica.org/2015/07/hackeando-o-brasil/.

[235] Vinculan a entidades del Estado con empresa de espionaje Hacking Team (2015, 12 de julio). *RPP noticias*. Recuperado de http://rpp.pe/politica/actualidad/vinculan-a-entidades-del-estado-con-empresa-de-espionaje-hacking-team-noticia-816283.

[236] Dubove, A (2015, 13 de julio). Hacking Team hizo contactos en Argentina para vender software espía. *Panam Post*. Recuperado de http://es.panampost.com/adam-dubove/2015/07/13/hacking-team-hizo-contactos-en-argentina-para-vender-software-espia/.

compra –dijo– fue potencializar la capacidad de detección de amenazas del terrorismo y la criminalidad organizada en el ciberespacio colombiano".[237]

La Secretaría Nacional de Inteligencia de Ecuador también negó su relación con Hacking Team.[238] No obstante, existen pruebas que sugieren el uso de su software contra personas y grupos opositores.[239]

En Chile, la Policía de Investigaciones admitió la adquisición del software de Hacking Team y justificó la compra como parte de los proyectos de modernización "cuyo objetivo era incrementar sus capacidades operativas en la investigación de crimen organizado, terrorismo internacional y narcotráfico a gran escala".[240]

Finalmente, en México, tras las filtraciones, se comprobó que 14 autoridades, tanto federales como estatales, eran clientes de la firma italiana y se cuestionó la legalidad de estas actividades.[241] Según los documentos filtrados, el país realizó el mayor pago que se haya hecho de alguna corporación pública o privada en la historia de la compañía, al adquirir 600 licencias para realizar monitoreos simultáneos.[242]

Como se mencionó anteriormente, en ninguno de los países analizados hay una consagración legal de la actividad de intrusión o 'hackeo' de dispositivos.[243] Por tanto, el primer requisito de legalidad como garantía de legitimidad de una medida de restricción de derechos no está satisfecho. En esas condiciones, puede decirse que tampoco están cumplidos los demás requisitos.

---

[237] Policía Nacional niega vínculo con la firma Hacking Team (2015, 8 de julio). *W Radio*. Recuperado de http://www.wradio.com.co/noticias/actualidad/policia-nacional-niega-vinculo-con-la-firma-hacking-team/20150708/nota/2841301.aspx.

[238] Secretaría Nacional de Inteligencia niega contratos con empresa que ofrece servicios de espionaje (2015, 10 de julio). *El Universo*. Recuperado de http://www.eluniverso.com/noticias/2015/07/10/nota/5011474/secretaria-inteligencia-niega-contratos-empresa-que-ofrece.

[239] APNewsBreak: leaked Hacking Team emails suggest Ecuador illegally spied on opposition (2015, 6 de agosto). *US New*. Recuperado de http://www.usnews.com/news/business/articles/2015/08/06/apnewsbreak-email-leak-suggests-ecuador-spied-on-opposition.

[240] PDI confirma compra de software creado por empresa italiana que fue hackeada (2015, 6 de julio).. *El Mercurio*. Recuperado de http://www.emol.com/noticias/Tecnologia/2015/07/06/724738/PDI-confirma-compra-de-software-creado-por-empresa-italiana-que-fue-hackeada.html.

[241] Sánchez, J. (2015, 6 de julio).Vulneración a Hacking Team confirma abuso de espionaje en México. *El Economista*. Recuperado de http://eleconomista.com.mx/tecnociencia/2015/07/06/vulneracion-hacking-team-confirma-abuso-espionaje-mexico.

[242] Ángel, A. (2015, 21 de julio). Sedena negoció compra de software a Hacking Team en 2015 para espiar a 600 personas. *Animal Político*. Recuperado de http://www.animalpolitico.com/2015/07/sedena-negocio-compra-de-software-a-hacking-team-en-2015-para-espiar-a-600-personas/.

[243] *Supra* (nota 75), Legitimidad de las restricciones.

La ausencia de un debate democrático sobre el uso de herramientas de hackeo es más notoria si se tiene en cuenta que todos los países analizados penalizan la intrusión abusiva a sistemas informáticos. En Perú, la Ley No. 300096 (2013) penaliza, en su artículo 2, el acceso ilícito a sistemas informáticos y, en su artículo 7, la interceptación de comunicaciones privadas. El Código Penal Federal mexicano tipifica en al artículo 177 la intervención de comunicaciones privadas. Brasil, por su parte, castiga la invasión de dispositivos informáticos en el artículo 154A del Código Penal. Finalmente, en Colombia, según el Código Penal es delito la violación ilícita de comunicaciones (Art. 192) y el acceso abusivo un sistema informático (Art. 195).

A pesar de la aparente ilegalidad de las actividades que denunciaron los escándalos de Hacking Team, no hay investigaciones en contra de las personas o entidades responsables.

Conclusiones

La retención de datos debe ser una de las técnicas de vigilancia más usada en la región, o al menos de las primeras herramientas utilizadas por las autoridades, a juzgar por la forma como las legislaciones se han esparcido para legalizarla. De los 5 países que analizamos, 4 de ellos han legislado esta técnica y no son las únicas legislaciones de este tipo en la región. Países como Honduras y Chile también cuentan con normas de retención de datos y con un análisis detallado, seguramente, emergerán muchas más.

Sin embargo, que exista legislación que reglamente el uso de la retención de datos, por sí solo, no es garantía de protección a los derechos humanos. Una legislación de ese tipo debe cumplir con una serie de condiciones para que la práctica sea legítima. Ninguna de las 4 legislaciones pasa el análisis. Las leyes sobre retención de datos de Perú, Colombia, México y Brasil son demasiado permisivas, amplias y tan poco garantes que no es posible confiar en ellas para tener un marco legal protector y respetuoso de los derechos humanos de su ciudadanía, como quedó demostrado en este documento. De otra parte, la legislación que hubo en Argentina fue declarada inconstitucional, precisamente, después de que se estableciera que no era una norma clara ni proporcional.

Es preocupante que, en materia de técnicas de vigilancia, se esté privilegiando una mirada esencialmente instrumental de la tecnología, que no cuestiona su verdadera utilidad. Si se hiciera una evaluación de este tipo, el carácter residual de la retención de datos frente a otras técnicas dirigidas y menos invasivas sería evidente. El marco jurídico que ofrece la CIDH y otros análisis como el que articulan los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* deben servir para promover legislaciones que ofrezcan verdaderas

garantías para la ciudadanía y mejoren la seguridad jurídica sobre la que se deben soportar las autoridades para hacer su trabajo.

De otra parte, debemos hablar de los retos que tiene nuestra región para debatir amplia y democráticamente el uso de herramientas de hackeo por las autoridades de vigilancia. Muchas de las herramientas con las que hoy cuentan las autoridades tienen, de alguna manera, un alcance limitado. La interceptación de llamadas o correos electrónicos extrae solo la información que cursa por esos medios y que la persona afectada ha decidido compartir con otras. En cambio, el acceso a un sistema informático, bien sea un computador personal o un teléfono móvil, puede implicar la recolección de toda clase de información personal como fotos, documentos de trabajo o personales, historial de navegación, acceso a micrófonos y cámaras web, e incluso al control mismo el dispositivo. Todo esto, sin que la persona se entere o sin que pueda establecerse un límite temporal a la ejecución de la intrusión. El hackeo, claramente, entrega mucha más información que la que se obtendría, por ejemplo, en el allanamiento de la casa de la persona afectada, aunque, por contraste, para esta última medida existan muchos más controles que para la primera.

Por tanto, el uso de herramientas de hackeo por autoridades de vigilancia plantea múltiples retos que deben ser abordados. La esquematización de los requisitos de legitimidad que se hizo anteriormente para evaluar la retención de datos de tráfico de telecomunicaciones debería dar una idea de lo que hay que evaluar en el uso de estas herramientas.

La normatividad que autorice el hackeo debe ser clara respecto a los tipos de herramienta que se pueden usar y las funciones del equipo que puede afectar, por ejemplo, el acceso a archivos guardados dentro del dispositivo, a registrar los que se teclea o a lo que perciben el micrófono o la cámara web. Asimismo, debe ser clara respecto a cuánto tiempo puede emplearse una herramienta semejante, qué autoridades y bajo qué condiciones puede hacerlo (p. ej. investigaciones de ciertos crímenes).

También debe analizarse hasta qué punto está limitada la medida en cuanto a los medios sobre los que operaría (redes, computadores personales, teléfonos móviles, cámaras de seguridad, tráfico de internet, etc.), sobre los datos a los que accedería, y el tiempo máximo por el cual podría implementarse.

La falta de precisión en alguno de estos puede ser un cheque en blanco en favor de la autoridad que pueda desplegar la medida, de donde puede fallarse el requisito de objetivo legítimo, pues se permitiría una restricción de derechos por razones vagas y poco fundamentadas, y el requisito de necesidad y proporcionalidad.

Es claro que el hackeo requeriría autorización judicial, por tanto, debe establecerse un procedimiento de solicitud en el que se pueda comprobar la satisfacción de los requisitos que exigiría la ley para el uso de la medida y que, además, impida su abuso. También debe contener provisiones respecto a la observación de la cadena de custodia, la notificación de la persona afectada para que pueda ejercer el derecho a la defensa, y la presentación de informes de transparencia por parte de las autoridades sobre la frecuencia de uso y la efectividad de la medida.

Finalmente, hay que tener en cuenta que la medida de hackeo como una forma legítima de vigilancia de las comunicaciones puede contener una contradicción respecto a otros deberes del Estado. Por un lado, este tipo de medidas se basan en la existencia de vulnerabilidades informáticas, es decir, en fallas de seguridad. Por el otro, los Estados desarrollan actualmente políticas de ciberseguridad, siguiendo el deber que tienen de garantizar la seguridad de la ciudadanía. Si el Estado no reporta las vulnerabilidades que encuentra, mantiene condiciones de inseguridad contraviniendo sus obligaciones. Si las reporta, en cambio, reduce las oportunidades para usarlas, desperdiciando el tiempo y los recursos que empleó para explotarlas. La superación de esta contradicción es un tema que debe ser parte necesaria de la discusión pública sobre la legalización del hackeo.

Criminalización del Discurso Crítico en Internet (CELE)

Por Verónica Ferrari y Daniela Schnidrig[244*]
Centro de Estudios en Libertad de Expresión y Acceso a la Información.[245]

Introducción

El Sistema Interamericano de Derechos Humanos (SIDH) otorga especial protección al derecho a la libertad de expresión, y esa protección ha sido extendida a las expresiones difundidas a través de internet. Sin embargo, en América Latina se observa una incipiente tendencia a criminalizar discurso crítico vertido en línea.

Si bien no son comunes los tipos penales que criminalicen expresiones en internet específicamente, se observan casos en los que se han aplicado normas tradicionales, como delitos contra el honor, contra la seguridad nacional, normativa sobre terrorismo, entre otras, para perseguir discurso difundido por internet.

Este informe busca señalar algunas de estas normas utilizadas en países de América Latina para acallar voces en internet, ejemplificando con casos concretos

244 * Verónica Ferrari es licenciada en Ciencias de la Comunicación de la Facultad de Ciencias Sociales (UBA). Es investigadora en los proyectos de la Iniciativa por la Libertad de Expresión en Internet (iLEI) y coordina la comunicación del Centro de Estudios en Libertad de Expresión y Acceso a la información (CELE) de la Universidad de Palermo.

Daniela Schnidrig es abogada graduada de la Universidad Torcuato Di Tella y diplomada en Derechos Humanos de las Mujeres por la Universidad de Chile. Es investigadora en la Iniciativa por la Libertad de Expresión en Internet (iLEI) del CELE.

245 El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo tiene como objetivo realizar investigaciones que se constituyan en herramientas útiles para periodistas, instituciones gubernamentales, sectores privados y de la sociedad civil dedicados a la defensa y promoción de estos derechos, especialmente en América Latina. Dentro del CELE, funciona la Iniciativa por la Libertad de Expresión en Internet (iLEI), un programa especial que busca proporcionar asesoramiento y apoyo a los promotores de regulación y políticas de internet. Este trabajo contó con los aportes y la supervisión de Eduardo Bertoni, director del CELE. Las autoras agradecen la colaboración de Ricardo Rosales Roa, pasante del CELE. Y a las organizaciones Hiperderecho, Artigo 19, Derechos Digitales y *Contingente Mx por los aportes.* http://www.palermo.edu/cele/

su uso, contrario a los estándares interamericanos, para perseguir expresiones legítimas.

Estándares del Sistema Interamericano de Derechos Humanos respecto de libertad de expresión y protección de discursos críticos

La importancia de la libertad de expresión en una sociedad democrática

El derecho a la libertad de expresión es, como lo entendió la Corte Interamericana de Derechos Humanos en 1985, "la piedra angular de cualquier sociedad democrática" [246] . La Convención Americana de Derechos Humanos (CADH) contempla el derecho a la libertad de pensamiento y expresión en su artículo 13[247].

Sin embargo, como han expresado la Comisión y la Corte Interamericana de Derechos Humanos, el derecho a la libertad de expresión no es un derecho absoluto[248]. Hay situaciones excepcionales en las que podría limitarse el derecho a

---

[246] Corte I.D.H., La Colegiación Obligatoria de Periodistas, Opinión Consultiva OC-5/85, 13 de noviembre de 1985, párrafo 70.

[247] Artículo 13. Libertad de Pensamiento y de Expresión. 1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a) el respeto a los derechos o a la reputación de los demás, o

b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

[248] Corte I.D.H., *Caso Eduardo Kimel VS. Argentina*. Sentencia de 2 de mayo de 2008. Serie C No. 177, párr. 54; Corte I.D.H., *Caso Palamara Iribarne*. Sentencia de 22 de noviembre de 2005. Serie C No.135, párr. 79; Corte I.D.H., *Caso Herrera Ulloa Vs. Costa Rica*. Sentencia de 2 de julio de 2004. Serie C No. 107, párr. 120; Corte I.D.H., *Caso Tristán Donoso Vs. Panamá*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia del 27 de enero de 2009 Serie C No. 193, párr.

la libertad de expresión para proteger otros derechos. El artículo 13 de la CADH establece aquellas restricciones válidas que pueden limitar el derecho a la libertad de expresión, y establece las condiciones que dichas limitaciones deben cumplir para ser legítimas[249]. Estas condiciones se conocen como "test tripartito" y su alcance ha sido interpretado por la Comisión y la Corte Interamericana de Derechos Humanos.

Del artículo 13 de la CADH se desprende que la regla en el Sistema Interamericano es la prohibición de la censura previa. Sin embargo, el artículo admite, excepcionalmente, la restricción previa de aquellos espectáculos públicos que puedan afectar a la moral de la infancia y la adolescencia, y la propaganda a favor de la guerra, o el discurso que haga incitación a la violencia.

A su vez, sólo podrán aplicarse responsabilidades ulteriores cuando éstas cumplan con tres requisitos. En primer lugar, las restricciones ulteriores deben cumplir con el requisito de legalidad — es decir, deben estar previstas de forma expresa en una ley —. En segundo lugar, las limitaciones deben ser necesarias para proteger derechos de terceros, la seguridad nacional, el orden público o la salud o moral públicas.

La Corte Interamericana de Derechos Humanos ha interpretado estos requisitos. Según la Corte, para que las restricciones a la libertad de expresión sean legales, deben ser necesarias para satisfacer un interés público imperativo. El medio utilizado para perseguir dicho objetivo debe ser proporcional, y deberá utilizarse la opción que restrinja en menor medida el derecho a la libertad de expresión[250].

110; Corte I.D.H., *Caso Ríos y otros Vs. Venezuela*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 28 de enero de 2009. Serie C No. 194, párr. 106; Corte I.D.H., *Caso Perozo y otros Vs. Venezuela*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 28 de enero de 2009. Serie C No. 195, párr. 117; CIDH. Informe Anual 1994. Capítulo V: Informe sobre la Compatibilidad entre las Leyes de Desacato y la Convención Americana sobre Derechos Humanos. Título IV. OEA/Ser. L/V/II.88. doc. 9 rev. 17 de febrero de 1995.

[249] Corte I.D.H., *Caso Herrera Ulloa Vs. Costa Rica*. Sentencia del 2 de julio de 2004. Serie C No. 107, párr. 120; Corte I.D.H*., La Colegiación Obligatoria de Periodistas* (Arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985, Serie A No. 5, párr. 35; CIDH. Informe No. 11/96, Caso No. 11.230. Francisco Martorell. Chile. 3 de mayo de 1996, párr. 55; CIDH. Alegatos ante la Corte Interamericana en el caso Ricardo Canese Vs. Paraguay. Transcritos en: Corte I.D.H., *Caso Ricardo Canese Vs. Paraguay*. Sentencia de 31 de agosto de 2004. Serie C No. 111, párr. 72.a).

[250] *Véase*, Corte I.D.H., *La Colegiación Obligatoria de Periodistas* (arts. 13 y 29 Convención Americana sobre Derechos Humanos), párrafo 42.Sobre proporcionalidad, *véase*,Declaración Conjunta sobre Libertad de Expresión e Internet, op. Cit, puntos 1, b) y d).

La protección a la libertad de expresión extendida a internet

Durante los últimos años, varios órganos de derechos humanos han expresado que la protección a la libertad de expresión debe extenderse también a las expresiones difundidas en internet. Por ejemplo, el Comité de Derechos Humanos de las Naciones Unidas se expresó sobre el alcance de la protección a la libertad de expresión en internet en su Observación general N° 34, en interpretación al artículo 19 del Pacto Internacional de Derechos Civiles y Políticos —en adelante, PIDCP— [251]. Allí, se estableció que:

> El párrafo 2 [del artículo 19 del PIDCP] protege todas las formas de expresión y los medios para su difusión. Estas formas comprenden la palabra oral y escrita y el lenguaje de signos, y expresiones no verbales tales como las imágenes y los objetos artísticos[252]. Los medios de expresión comprenden los libros, los periódicos[253], los folletos[254], los carteles, las pancartas[255], las prendas de vestir y los alegatos judiciales[256], así como modos de expresión audiovisuales, electrónicos o de Internet, en todas sus formas. (El resaltado es nuestro).

El Consejo de Derechos Humanos de las Naciones Unidas también se expresó en su Resolución A/HRC/20/L.13[257] sobre el alcance de la protección de libertad de expresión en Internet, y estableció 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…". (El subrayado es propio).

En la misma línea se encuentra la *Declaración conjunta sobre libertad de expresión e Internet* de 2011, en la que los relatores aclaran que:

---

[251] Comité de Derechos Humanos de Naciones Unidas, Observación General N° 34. CCPR/C/GC/34. 12 de septiembre de 2011.

[252] *Véase*, comunicación Nº 926/2000, *Shin c. la República de Corea*.

[253] *Véase*, comunicación Nº 1341/2005, *Zundel c. el Canadá*, dictamen aprobado el 20 de marzo de 2007.

[254] *Véase*, comunicación Nº 1009/2001, *Shchetoko y otros c. Belarús*, dictamen aprobado el 11 de julio de 2006.

[255] *Véase,* comunicación Nº 412/1990,*Kivenmaa c. Finlandia*, dictamen aprobado el 31 de marzo de 1994.

[256] *Véase*, comunicación Nº 1189/2003,*Fernandoc. Sri Lanka*.

[257] ONU, Resolución A/HRC/20/L.13, disponible en:http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/13/PDF/G1214713.pdf?OpenElement

> La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad (la prueba 'tripartita')."(El resaltado es nuestro).

En definitiva, esto quiere decir que las normas que restrinjan la libertad de expresión en internet deberán analizarse bajo el mismo estándar estricto que las normas tradicionales sobre libertad de expresión.

¿Qué significa que el medio utilizado sea "proporcional"? Al ser un criterio dinámico, no hay una interpretación fija, sino que deberá analizarse caso por caso. Al respecto, los relatores en su la declaración conjunta de 2011 sostuvieron que:

> (…)al evaluar la proporcionalidad de una restricción a la libertad de expresión en Internet, se debe ponderar el impacto que dicha restricción podría tener en la capacidad de Internet para garantizar y promover la libertad de expresión respecto de los beneficios que la restricción reportaría para la protección de otros intereses[258].

Creemos que, en principio, una norma que criminalice discursos difundidos a través de internet difícilmente pueda ser considerada proporcional. En las secciones siguientes desarrollaremos esta sobre esto.

Criminalización de discurso crítico en general

> Los órganos del SIDH desalientan la utilización del derecho penal para criminalizar el discurso crítico. Por ejemplo, la Relatoría Especial para la Libertad de Expresión expresó en su informe de 2009 que: Las autoridades de los Estados no deben hacer uso del derecho penal para sancionar a quienes hacen investigaciones o emiten opiniones personales sobre asuntos de interés público, sobre funcionarios públicos, personas públicas o particulares involucrados voluntariamente en asuntos de interés público[259].

[258] Declaración Conjunta sobre Libertad de Expresión e Internet, junio de 2011, disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=848

[259] Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. OEA/Ser.L/V/II. Diciembre de 2009. Párrafo 217.

Y que:

> Las expresiones, informaciones y opiniones críticas sobre asuntos de interés público, sobre el funcionamiento del Estado y sus instituciones, o sobre los funcionarios públicos, gozan de una mayor protección bajo la Convención Americana, lo cual implica que el Estado debe abstenerse, con mayor rigor, de establecer limitaciones a estas formas de expresión. En efecto, como ya se ha indicado, la legitimidad y fortaleza de las instituciones se construye gracias al debate público y no como efecto de su supresión[260].

El Sistema Interamericano denomina "protección dual del honor" al principio según el cual los funcionarios públicos deban ser más tolerantes a las críticas. Y agrega que:

> Este principio adopta, además, el estándar de la doctrina de la real malicia (actual malice), que considera que las sanciones a las expresiones sobre funcionarios públicos han de ser civiles, y únicamente en los casos en los que se difunda información falsa a sabiendas de ese carácter, con la intención expresa de causar daño o con un grosero menosprecio por la verdad[261]. De ahí que, a la luz de este principio y de los preceptos que lo sustentan, la imposición de las sanciones penales a las ofensas contra funcionarios públicos relacionadas con el ejercicio de sus funciones sería contraria a los criterios de necesidad y proporcionalidad en el marco de una sociedad democrática"[262].(El resaltado es nuestro).

La Relatoría Especial para la Libertad de Expresión de la OEA se ha expresado sobre la incompatibilidad de las normas de desacato y aquellas figuras que penalizan las ofensas a funcionarios públicos en ejercicio de sus funciones, lo que, ha sostenido "es a todas luces contrario al principio democrático del control de quienes ejercen los poderes del Estado"[263].

---

260 Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. OEA/Ser.L/V/II. Diciembre de 2009. Párrafo 556.

261 (Cfr). CIDH, Informe Anual 2000. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo II, Apend. B.

262 Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. 2004. Capítulo VI. Punto 11. Disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=459&lID=2

263 Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. 2004. Capítulo VI. Punto 12. Disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=459&lID=2

Este criterio sostenido por la Relatoría ha sido ratificado recientemente respecto de las normas penales que restringen la libertad de expresión "y que permiten la imposición de medidas desproporcionadas que pueden tener un efecto silenciador incompatible con una sociedad democrática"[264].

La Relatoría pone como ejemplo de uso del derecho penal para silenciar voces, a figuras penales vagas e imprecisas como terrorismo, subversión e incitación a la violencia —figuras que analizaremos más adelante en este informe— para sancionar expresiones críticas o de protesta. Por último, destaca que los sistemas democráticos no sólo no deben criminalizar expresiones, sino que deben fomentar la deliberación pública y garantizar una mayor apertura ante expresiones de ciudadanos en ejercicio del control democrático[265].

La Corte IDH, a su vez, se expresó sobre el tema en el caso Kimel[266], en el que ordenó al Estado argentino reformar sus leyes penales sobre calumnias e injurias. La Corte entendió que "el Derecho Penal es el medio más restrictivo y severo para establecer responsabilidades respecto de una conducta ilícita" [267] y que "la tipificación amplia de delitos de calumnia e injurias puede resultar contraria al principio de intervención mínima y de última ratio del derecho penal"[268].

Posteriormente, en el caso Usón Ramírez[269], la Corte entendió que el delito de "injuria contra la Fuerza Armada Nacional" no cumplía con el principio de legalidad por ser un tipo penal ambiguo, y que, en el caso, la aplicación del derecho penal al caso no era idónea, necesaria y proporcional.

La Corte sostuvo, además, que cuando las restricciones a la libertad de expresión estén impuestas por normas penales, deberá cumplirse las exigencias propias del principio de estricta legalidad, es decir "utilizar términos estrictos y unívocos, que acoten claramente las conductas punibles"[270]. Eso significa que el tipo penal debe

---

[264] Organización de los Estados Americanos, Relatoría Especial para la Libertad, Comunicado de prensa 44/15.

[265] *Ibíd.*

[266] Corte I.D.H., *Caso Kimel Vs. Argentina.* Sentencia de 2 de mayo de 2008. Serie C No. 177

[267] Corte I.D.H., *Caso Kimel Vs. Argentina.* Sentencia de 2 de mayo de 2008. Serie C No. 177, párr. 76.

[268] Corte I.D.H., *Caso Kimel Vs. Argentina.* Sentencia de 2 de mayo de 2008. Serie C No. 177, párrafo 76.

[269] Corte I.D.H., *Caso Usón Ramírez Vs Venezuela.* Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 20 de noviembre de 2009. Serie C No. 207

[270] Corte I.D.H., *Caso Usón Ramírez Vs Venezuela.* Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 20 de noviembre de 2009. Serie C No. 207, párrafo 55.

contar con "una clara definición de la conducta incriminada, la fijación de sus elementos y el deslinde de comportamientos no punibles o conductas ilícitas sancionables con medidas no penales"[271].

Criminalización de discurso crítico difundido por internet

Como mencionamos anteriormente, de acuerdo con los estándares internacionales de derechos humanos, la protección de la libertad de expresión debe extenderse también a aquellas expresiones difundidas por internet. Por lo tanto, no podría aceptarse la criminalización o el agravamiento de penas en casos de discursos simplemente por haber sido difundidos a través de internet.

La Relatoría Especial para la Libertad de Expresión de la OEA se ha pronunciado al respecto en el informe "Libertad de expresión e Internet"[272], en el que deja en claro que:

> (…) no sería aceptable una ley que penalice, específicamente, los delitos contra el honor en línea e imponga penas más rigurosas que para los perpetrados en el mundo offline"[273], en tanto "ello significaría una restricción desproporcionada para la expresión en Internet, bajo un paradigma que considera a ese medio más riesgoso que otros. Ese tipo de medidas tendría el efecto de restringir y limitar a Internet como espacio para el libre intercambio de ideas, informaciones y opiniones.[274][275].

---

[271] Corte I.D.H., *Caso Usón Ramírez Vs Venezuela.* Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 20 de noviembre de 2009. Serie C No. 207, párrafo 55.

[272] Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. 31 de diciembre de 2013.

[273] Article 19, *El derecho a bloguear*, 2013, pp. 33-34. En Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. 31 de diciembre de 2013.

[274] Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. A/HRC/17/27. 16 de mayo de 2011. Párr. 72. Disponible para consulta en:http://ap.ohchr.org/documents/dpage_s.aspx?m=85 En Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. 31 de diciembre de 2013.

[275] Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. 31 de diciembre de 2013. Párrafo 74.

Normativa que criminaliza discurso crítico

En esta sección del informe analizaremos distintos tipos de normativa que han sido utilizados para criminalizar discurso crítico difundido a través de internet.

Normas tradicionales que se utilizan para criminalizar discurso online

Si bien son escasas las normas que penalizan específicamente aquellos discursos difundidos a través de internet, una práctica observada es la de utilizar tipos penales tradicionales para perseguir discurso online. En esta sección describiremos algunos tipos penales tradicionales que se han utilizado para perseguir penalmente la difusión de discurso a través de internet, ilustrando con algunos casos concretos.

Delitos contra el honor

El marco de protección de derechos del Sistema Interamericano señala que la honra, la dignidad y la reputación también son derechos humanos consagrados en el artículo 11 de la Convención Americana. Y agrega:

> Según el artículo 13.2 de la Convención Americana, la protección de la honra y reputación de los demás puede ser un motivo para establecer restricciones a la libertad de expresión, es decir, puede ser un motivo para fijar responsabilidades ulteriores por el ejercicio abusivo de dicha libertad. Sin embargo, es claro—como se mencionó anteriormente—que el ejercicio del derecho a la honra, dignidad y reputación debe armonizarse con el de la libertad de expresión, puesto que no ocupa una jerarquía o nivel superior[276].

Sin embargo, el SIDH también señala que:

> El honor de los individuos debe ser protegido sin perjudicar el ejercicio de la libertad de expresión ni el derecho a recibir información. Cuando se presenta en un Estado una tendencia o patrón en el sentido de preferir el derecho a la honra sobre la libertad de expresión y restringir esta última cuando existe tensión, en todo caso, se violenta el principio de armonización concreta que surge de la obligación de respetar y garantizar el conjunto de derechos humanos reconocidos en la Convención Americana[277].

---

[276] Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, *Marco jurídico interamericano sobre el derecho a la libertad de expresión*, punto 103, disponible en: https://www.oas.org/es/cidh/expresion/docs/cd/sistema_interamericano_de_derechos_humanos/index_MJIAS.html

[277] *Ibíd.*

A continuación, describiremos algunos casos en los que se han criminalizado expresiones en internet a raíz de "delitos contra el honor", que han resuelto esta tensión a contramano de los estándares interamericanos.

Colombia. Caso "Blanco porcelana": retiro de contenidos por injuria

En Colombia, un colectivo de artistas elaboró la obra Blanco porcelana. En la obra, se utilizaban anécdotas familiares y fotografías con el objetivo de reflexionar sobre el racismo en Colombia producto de la herencia colonial[278]. A través de estas memorias, las artistas daban cuenta de lo enraizada que estaba la idea de que "lo bonito" y "lo bueno" estaba asociado a lo blanco

Familiares de una de las integrantes del colectivo, Margarita Ariza, al ver la obra, denunciaron penalmente a las artistas por los delitos de injuria y calumnia, tipificados en el Código Penal colombiano[279]. Asimismo, los familiares interpusieron una acción de tutela porque, a su juicio, se estaban vulnerando sus derechos a la intimidad y al buen nombre.

En Colombia, al igual que en el resto de los países de América Latina con excepción de México, se penalizan los delitos contra el honor a contramano de los estándares del SIDH:

> Artículo 220. Injuria. El que haga a otra persona imputaciones deshonrosas, incurrirá en prisión de dieciséis (16) a cincuenta y cuatro (54) meses y multa de trece punto treinta y tres (13.33) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes[280].

Los juzgados penales Treinta y Seis Municipal de Bogotá y Veinte de Bogotá accedieron a la solicitud de la acción de tutela[281] ya que, para estos juzgados, se

---

278 Botero, Carolina, "'Blanco Porcelana', la obra de arte que ganó la batalla por la libertad de expresión en Colombia", *Digital Rights LAC,* 12 de junio de 2015, disponible en: http://www.digitalrightslac.net/es/blanco-porcelana-la-obra-de-arte-que-gano-la-batalla-por-la-libertad-de-expresion-en-colombia/

279 Arts. 220 y 221, Cód. Pen. de Colombia, disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

280 *Ibíd.*

281 Juzgado 36 penal municipal, acción de tutela, 26 de abril de 2012, disponible en: https://www.scribd.com/fullscreen/92403013?access_key=key-2xndmg6kb3soo1102uc&allow_share=true&escape=false&view_mode=scroll

estaba vulnerando estos derechos en tanto en la obra se utilizaron sus nombres y fotos familiares sin su autorización[282].

Estas sentencias limitaron la exhibición de las piezas del proyecto Blanco porcelana y exigieron el retiro de esos contenidos del sitio web de la obra (www.blancoporcelana.com) y de su página en Facebook en un plazo de 48 horas. La autora, en línea con la decisión, retiró las fotos y textos objetados por sus familiares porque en ellos aparecían sus nombres.

El caso fue revisado finalmente por la Corte Constitucional colombiana que, en su decisión[283] protegió el derecho a la libertad de expresión artística de las tres artistas. Para la Corte, "la protección de la libertad de expresión y creación artística plasmada en el proyecto 'Blanco Porcelana' exige una limitación del derecho a la intimidad de los familiares de la artista demandada"[284].

Funcionarios públicos que emprenden acciones penales a raíz de comentarios críticos publicados en internet

Las expresiones de interés público son un tipo de discurso especialmente protegido por la CADH. Al respecto, la Corte Interamericana ha establecido en su jurisprudencia que esta especial protección de las expresiones referidas a funcionarios o a asuntos de interés público encuentra su justificación, entre otras cosas, en la importancia de un marco jurídico que fomente la deliberación pública y en que los funcionarios se exponen voluntariamente a un mayor escrutinio social, y tienen mayor acceso a los medios de comunicación para responder sobre hechos que los involucren[285].

Al respecto, tanto la CIDH como la Corte Interamericana han considerado, en todos los casos concretos que han sido objeto de su estudio y decisión, que la protección de la honra o reputación de funcionarios públicos (o candidatos a ejercer cargos)

---

[282] "¿Censura judicial al arte?", *La Silla Vacía*, 05 de febrero de 2012, disponible en:http://lasillavacia.com/queridodiario/33030/censura-judicial-al-arte?utm_source=twitterfeed&utm_medium=twitter y Botero, Carolina, "Blanco porcelana", *El Espectador*, 3 de mayo de 2012, disponible en: http://www.elespectador.com/opinion/blanco-porcelana

[283] Corte Constitucional de Colombia, Sentencia T-015/15, disponible en:http://www.corteconstitucional.gov.co/relatoria/2015/T-015-15.htm

[284] *Ibíd*.

[285] *Supra* nota 32, punto 105.

mediante el procesamiento o la condena penal de quien se expresa, resultaba desproporcionada e innecesaria en sociedades democráticas[286].

Sin embargo, como se ejemplificará a continuación, funcionarias y funcionarios de la región siguen recurriendo al derecho penal y a las figuras de calumnias e injurias para acallar voces críticas. Y, como veremos a continuación, esta tendencia se extiende a las expresiones vertidas en internet.

Costa Rica - Presidenta demanda por difamación por un posteo en Facebook

La ahora ex presidenta de Costa Rica, Laura Chinchilla, demandó a un ciudadano por difamación en junio de 2013 ante el Tribunal Penal de San José, a raíz de un comentario publicado en Facebook [287]. En el posteo, el demandado, Alberto Rodríguez Baldí, se había referido a la ex mandataria como "la presidenta millonaria"[288].

Según el Código Penal costarricense, será reprimido "con veinte a sesenta días multa el que deshonrare a otro o propalare especies idóneas para afectar su reputación"[289]. De acuerdo con esta normativa, quien injurie, calumnie o difame; o quien reprodujera dichos ofensivos en contra de alguien, aun cuando se trate de funcionarios públicos, no puede ser encarcelado, pero sí puede ser multado o incluido en una lista de condenados penales.

En primer término, el tribunal de justicia absolvió al demandado. El tribunal estableció que la publicación realizada por Rodríguez Baldí no habría constituido una ofensa explícita hacia la ex presidenta debido a que el texto se prestaría a distintas interpretaciones[290] y que "el umbral de tolerancia que se espera de la persona que detenta la Presidencia es muy alto"[291].

---

286 *Ibíd.*, punto 111.

287 "Presidenta Chinchilla demanda a empresario por comentario en Facebook", *CRHoy*, 26 de junio de 2013, disponible en: http://www.crhoy.com/presidenta-chinchilla-demanda-a-empresario-por-comentario-en-facebook/

288 "Empresario afirma que Laura Chinchilla lo demanda para distraer discusión de OAS", *Nación*, 26 de junio de 2013, disponible en: http://www.nacion.com/nacional/Empresario-Chinchilla-distraer-discusion-OAS_0_1350065096.html

289 Art. 146, Cód. Pen. de Costa Rica, disponible en: https://www.oas.org/juridico/spanish/cr_res4.htm

290 Arguedas, Carlos, "Tribunal absuelve a empresario del delito de difamación en perjuicio de expresidenta Chinchilla", *Nación*, 21 de julio de 2014, disponible en:

En febrero de este año, el Tribunal de Apelaciones del II Circuito Judicial de San José, dio lugar al recurso de apelación presentado por Chinchilla y anuló la sentencia que absolvía a Rodríguez Baldí y ordenó volver a realizar el juicio, pero con una conformación distinta del tribunal[292].

En primer término, este caso da cuenta de una tendencia que persiste en la región: el uso de las figuras penales para criminalizar el discurso. Y, en particular, este caso va a contramano de los estándares interamericanos en tanto las expresiones y opiniones críticas sobre los funcionarios y las funcionarias gozan de una mayor protección bajo la Convención Americana. Este tipo de tipificaciones tiene, de acuerdo al marco de derechos del Sistema Interamericano, el efecto de desincentivar el debate público[293].

En este sentido, la Relatoría Especial para la Libertad de Expresión ha señalado en 2010 que:

> (...) los funcionarios acceden a sus cargos de manera voluntaria y a sabiendas de que, por el enorme poder que administran, estarán sometidos a un escrutinio mucho más intenso. Esta tesis se sustenta, además, en el hecho de que los funcionarios públicos tienen una gran capacidad de incidencia en el debate público, no sólo por el respaldo ciudadano y la credibilidad de la cual gozan, sino porque suelen contar con posibilidades reales y efectivas de participación en el proceso de comunicación de masas que, en general, no tienen los ciudadanos y ciudadanas que no ocupan dichas posiciones. En este sentido, se ha sostenido que las críticas, incluso ofensivas, radicales o perturbadoras, deben recibirse con más y no con menos debate, y que es el ciudadano y no las propias autoridades criticadas, quien debe decidir si una idea o información es merecedora de atención y respeto o si, simplemente, debe ser descartada[294].

---

http://www.nacion.com/sucesos/Tribunal-empresario-difamacion-expresidenta-Chinchilla_0_1428057294.html

[291] Murillo, Álvaro, "La justicia costarricense absuelve a un usuario de redes que criticó a Chinchilla", *El País*, 22 de julio de 2014, disponible en: http://internacional.elpais.com/internacional/2014/07/22/actualidad/1406043678_303543.html

[292] *Ibíd.*, nota 46.

[293] Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. OEA/Ser.L/V/II. Diciembre de 2009. Párrafo 556.

[294] Organización de los Estados Americanos, Relatoría Especial para la Libertad de Expresión, *Una agenda hemisférica para la defensa de la libertad de expresión*, 2010, disponible en:

Ecuador – Caso de tuitero encarcelado por expresiones de descrédito y deshonra

Otro ejemplo de funcionarios públicos que acuden al derecho penal para acallar voces críticas es el caso de Sebastián Cevallos. Cevallos, subdirector nacional del movimiento Unidad Popular, publicó mensajes en su cuenta de Twitter donde denunciaba actos de nepotismo en el Gobierno. Específicamente, hizo alusión a Paula Rodas, funcionaria pública sobrina del Ministro de Trabajo, Carlos Marx Carrasco.[295]

Rodas demandó a Cevallos por proferir "expresiones en franco descrédito y deshonra", y un tribunal de Cuenca lo sentenció a 15 días de prisión.[296] El tribunal condenó a Cevallos sobre la base del artículo 396 del Código Orgánico Integral Penal de Ecuador, que prevé la siguiente contravención "Será sancionada con pena privativa de libertad de quince a treinta días: 1. La persona que, por cualquier medio, profiera expresiones en descrédito o deshonra en contra de otra. Esta contravención no será punible si las expresiones son recíprocas en el mismo acto. …"[297]

La CIDH, así como la Corte Interamericana, han expresado previamente que proteger la honra o reputación de funcionarios públicos (o candidatos a ejercer cargos) mediante el procesamiento o la condena penal de quien se expresa, es una medida desproporcionada e innecesaria en sociedades democráticas[298].

---

https://www.oas.org/es/cidh/expresion/docs/cd/sistema_interamericano_de_derechos_humanos/index_AHDLE.html

[295] Fundamedios, "Tuitero es condenado a 15 días de prisión por denuncias de nepotismo", 12 de noviembre de 2015. Disponible en http://www.fundamedios.org/alertas/tuitero-es-condenado-15-dias-de-prision-por-denuncias-de-nepotismo/ ; Ecuador noticias, "Carlos Marx Carrasco tiene a varios familiares en puestos públicos", 22 de julio de 2015. Disponible en http://www.ecuadornoticias.com/2015/07/carlos-marx-carrasco-tiene-varios.html

[296] Fundamedios, "Tuitero es condenado a 15 días de prisión por denuncias de nepotismo", 12 de noviembre de 2015. Disponible en http://www.fundamedios.org/alertas/tuitero-es-condenado-15-dias-de-prision-por-denuncias-de-nepotismo/ ; Panam Post, "Ecuador envía a prisión a tuitero por denunciar nepotismo gubernamental", 17 de noviembre de 2015. Disponible en http://es.panampost.com/belen-marty/2015/11/17/ecuador-envia-a-prision-a-tuitero-por-denunciar-nepotismo-gubernamental/

[297] Artículo 396.I) del Código Orgánico Integral Penal de Ecuador, disponible en http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

[298] Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, *Marco jurídico interamericano sobre el derecho a la libertad de expresión*, punto 103, disponible en:

En su Declaración Conjunta de 2002, el Relator Especial de la ONU sobre la Libertad de Opinión y Expresión, el Representante de la OSCE sobre la Libertad de Prensa y el Relator Especial de la OEA sobre Libertad de Expresión expresaron de forma muy clara, respecto de la difamación penal, que "La difamación penal no es una restricción justificable de la libertad de expresión; debe derogarse la legislación penal sobre difamación y sustituirse, conforme sea necesario, por leyes civiles de difamación apropiadas."[299]

La figura contravencional y la decisión en el presente caso son, a todas luces, contrarias a los estándares del Sistema Interamericano respecto de libertad de expresión y, específicamente, respecto de los estándares en casos de funcionarios públicos.

Ecuador - Caso de bloguero encarcelado por "ofensas a la autoridad"

En 2011, Víctor Vizcaíno Luzuriaga fue acusado de cometer el delito de ofensas contra el, por entonces, Fiscal General del Estado, Washington Pesántez, por comentarios realizados en su blog (www.laplegariadeunpagano.com)[300]. El 19 de abril de 2011, el juzgado Vigésimo Cuarto de Garantías Penales de Pichincha, a pedido del fiscal de la Unidad Especializada de la Administración Pública de ese estado, emitió una orden de detención contra el bloguero.

Vizcaíno fue detenido días más tarde y liberado al día siguiente, después de que un juez de Garantías Penales reemplazara la orden de prisión por otras medidas cautelares[301] como el impedimento para acercarse al fiscal y a su familia, el no iniciar actos de intimidación y la obligación de presentarse cada diez días ante la

---

https://www.oas.org/es/cidh/expresion/docs/cd/sistema_interamericano_de_derechos_humanos/index_MJIAS.html , punto 111.

[299] Declaración Conjunta. Relator Especial de la ONU sobre la Libertad de Opinión y Expresión, Representante de la OSCE sobre la Libertad de Prensa y Relator Especial de la OEA sobre Libertad de Expresión. Diciembre de 2002. Disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=87&lID=2

[300] Aguilera Muñoz, Paulina, "Ecuador: Bloguero detenido por ofensas al Fiscal General", *Global Voices*, 7 de mayo de 2011, disponible en:http://es.globalvoicesonline.org/2011/05/07/ecuador-bloguero-detenido-por-ofensas-al-fiscal-general/

[301] "Juez ordena la prisión contra bloguero acusado de ofender a exfiscal", *El Universo,* 11 de enero de 2012, disponible en: http://www.eluniverso.com/2012/01/11/1/1355/juez-ordena-prision-contra-bloguero-acusado-ofender-exfiscal.html

fiscalía[302]. Al no cumplir con las medidas cautelares, meses después, el 30 de noviembre de 2011, el juzgado 24 de Garantías Penales del Guayas dictó el auto de llamamiento a juicio contra el bloguero y su prisión preventiva[303] .

Vizcaíno fue acusado de haber cometido un delito contra la administración pública que estaba contemplado en el antiguo Código Penal de Ecuador. El delito por el que se lo acusó, tipificado en el artículo 231 del código, señalaba que "la persona que con amenazas, injurias, amagos o violencias, ofendiere a cualquiera de los funcionarios públicos (...) cuando éstos se hallen ejerciendo sus funciones, o por razón de tal ejercicio, será reprimido con prisión de quince días a tres meses y multa de cincuenta a trescientos sucres"[304].

Este artículo ubicado en la sección dedicada a los "delitos contra la administración pública", incluía esto dentro de "la rebelión y atentados contra los funcionarios".

Como señalan la Corte Interamericana de Derechos Humanos y la Declaración de Principios sobre libertad de expresión de la CIDH, los funcionarios públicos están sujetos a un mayor escrutinio por parte de la sociedad. En este sentido, de acuerdo al Sistema Interamericano de protección de derechos, leyes como ésta de Ecuador que penalizan la expresión ofensiva dirigida a funcionarios públicos, atentan contra los derechos de libertad de expresión y acceso a la información[305].

El Código Orgánico Integral Penal (COIP) de Ecuador, aprobado en 2014, eliminó esta figura despenalizando la injuria no calumniosa. En términos de la Relatoría Especial para la Libertad de Expresión de la OEA, esto representó un importante avance[306].

---

[302] Fundamedios, Alerta No. 300, disponible en: https://twitter.com/fundamedios/status/68007537810735105

[303] "Código eliminó delitos catalogados 'absurdos'", *El Universal*, 13 de agosto de 2014, disponible en: http://www.eluniverso.com/noticias/2014/08/13/nota/3395286/codigo-elimino-delitos-catalogados-absurdos

[304] Art. 231, Cód. Pen. de Ecuador, disponible en:http://www.cepal.org/oig/doc/ecuart5511codigopenal.pdf

[305] Comisión Interamericana de Derechos Humanos, *Declaración de principios sobre libertad de expresión*, disponible en: https://www.cidh.oas.org/basicos/basicos13.htm

[306] Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión de 2013, p. 130, disponible en:https://www.oas.org/es/cidh/expresion/docs/informes/anuales/2014_04_22_IA_2013_ESP_FINAL_WEB.pdf

Sin embargo, el COIP mantiene la figura de calumnias, cuya pena es de seis meses a dos años de cárcel para "la persona que por cualquier medio, realice falsa imputación de un delito en contra de otra"[307].

El principio 10 de la Declaración de Principios sobre Libertad de Expresión introduce el llamado sistema de protección dual del honor, según el cual los funcionarios públicos y las personas públicas se han expuesto voluntariamente a un mayor escrutinio por parte de la sociedad, y en aras del control social necesario para un eficiente y adecuado ejercicio de los poderes del Estado, han de ser más tolerantes a la crítica. El SIDH establece que "la protección al honor en estos casos ha de darse en sede civil, en virtud de que la sanción penal podría inhibir el control de la función pública necesario en una sociedad democrática"[308].

Chile – Caso del Alcalde de Nogales que querelló por injurias en redes sociales

Otro caso que se suma a los anteriores es el del Alcalde Oscar Cortés que inició una querella contra alrededor de veinte personas por considerar que lo habían injuriado en Facebook.[309]
Una sentencia de julio de 2015 condenó a Andrés Santiago Marín Nieto a 250 días de prisión sobre la base del artículo 417 del Código Penal chileno, que reza "Son injurias graves: 1°. La imputación de un crimen o simple delito de los que no dan lugar a procedimiento de oficio. 2°. La imputación de un crimen o simple delito penado o prescrito. 3°. La de un vicio o falta de moralidad cuyas consecuencias puedan perjudicar considerablemente la fama, crédito o intereses del agraviado. 4°. Las injurias que por su naturaleza, ocasión o circunstancias fueren tenidas en el concepto público por afrentosas. 5°. Las que racionalmente merezcan la calificación de graves atendido el estado, dignidad y circunstancias del ofendido y del ofensor."[310]

---

[307] Art. 182, COIP, disponible en:http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

[308] Comisión Interamericana de Derechos Humanos, *supra* nota 56.

[309] Soy Chile.cl, "Alcalde Cortés se aburrió del bullying y los memes en las redes sociales y presentó querella", 26 de junio de 2014. Disponible en http://www.soychile.cl/Quillota/Sociedad/2014/06/23/257300/Alcalde-Cortes-se-aburrio-del-bullying-y-los-memes-en-las-redes-sociales-y-presento-querella.aspx ; Impacto Digital, "Nogales: Alcalde se querelló por delito de injurias y calumnias emitidas en redes sociales", 20 de junio de 2014, disponible en http://www.impactodigital.cl/nogales-alcalde-se-querello-por-delito-de-injurias-y-calumnias-emitidas-en-redes-sociales/#sthash.a3RNwqVr.dpuf

[310] Disponible en http://www.leychile.cl/Navegar?idNorma=1984

Como se señaló en los casos anteriores, la aplicación de delitos contra el honor para acallar discurso crítico, especialmente cuando se trata de funcionarios públicos, es contraria a los estándares del Sistema Interamericano de Derechos Humanos.

Delitos financieros

Guatemala: tuiteros y pánico financiero

Jean Ramses Anléu Fernández fue arrestado en la ciudad de Guatemala por instar en un tuit a retirar depósitos del banco Banrural, una entidad que en ese entonces se encontraba envuelta en un escándalo vinculado con un crimen [311]. Anleu Fernández fue acusado de generar "pánico financiero".

Según el Código Penal de Guatemala:

> Comete delito de pánico financiero quien elabore, divulgue o reproduzca por cualquier medio o sistema de comunicación información falsa o inexacta que menoscabe la confianza de los clientes, usuarios, depositantes o inversionistas de una institución sujeta a la vigilancia e inspección de la Superintendencia de Bancos. Se entenderá que se menoscaba la confianza de los clientes, usuarios, depositantes o inversionistas de una institución cuando, como consecuencia de los referidos actos, se atente contra su reputación o prestigio financiero o que de la misma sea objeto de retiro masivo de depósitos o inversiones, mayores o superiores a su flujo normal u ordinario.
> El responsable de la comisión de este delito será sancionado con prisión de uno a tres años y con multa de cinco mil a cincuenta mil Quetzales.
>
> Si el delito fuere cometido conociendo o previendo los daños o perjuicios a causar a la institución, el responsable será sancionado con prisión de cinco a diez años inconmutable y con una multa de cien mil a ochocientos mil Quetzales. En este caso, no se podrá otorgar cualquiera de las medidas sustitutivas contempladas en el Código Procesal Penal[312].

[311]"Guatemala police arrest Twitter user for 'inciting financial panic'", *The Guardian*, 15 de mayo de 2009, disponible en: http://www.theguardian.com/world/2009/may/15/guatemala-twitter-jean-anleu-fernandez
[312]Artículo 342 b, Cód. Pen. de Guatemala, disponible en: http://leydeguatemala.com/codigo-penal/monopolio/3163/

Venezuela. Caso Acosta Oxford y Nares Castro[313]

El 8 de julio de 2010, Luis Enrique Acosta Oxford y Carmen Cecilia Nares Castro fueron arrestados por el Cuerpo de Investigaciones Penales y Criminalísticas (CICPC) en el estado de Bolívar en Venezuela. Días antes, Acosta había difundido en cuenta de Twitter (@leaoxford) un mensaje que decía, haciendo alusión a un banco, "Señores para que no digan que no se les dijo retiren hoy de [nombre del banco]quedan pocos días, se les dijo"[314].

Posteriormente, Acosta y Nares Castro fueron puestos en libertad condicional, con el deber de presentarse ante el tribunal cada quince días y no difundir mensajes relacionados con los bancos[315].

La normativa utilizada en este caso fue la Ley General de Bancos y Otras Instituciones Financieras y su artículo 448 dedicado a la "Difusión de Información Falsa". El artículo señala que "Las personas naturales o jurídicas que difundan noticias falsas o empleen otros medios fraudulentos capaces de causar distorsiones al sistema bancario nacional que afecten las condiciones económicas del país, serán penados con prisión de nueve (9) a once (11) años"[316].

El Director del CICPC declaró:

> Los falsos rumores en las redes sociales están claramente sancionados en el artículo 448 de la Ley de Bancos, en este sentido cualquier persona que propague rumores mal intencionados por cualquier medio, correos electrónicos, mensajes de texto en celulares (sms), la red twitter, facebook, o cualquier otra herramienta tecnológica, a viva voz o por cualquier otro medio

313 Human Rights Foundation, "HRF in Washington Times: Venezuelans Charged for Twitter Statements", disponible en: http://humanrightsfoundation.org/news/hrf-in-washington-times-venezuelans-charged-for-twitter-statements-00100

Véase, Espacio Público, "Arrestan a usuarios de Twitter por "desestabilizar" sistema bancario", 9 de julio de 2010, disponible en: http://espaciopublico.org/index.php/noticias/1-libertad-de-expresi/818-arrestan-a-usuarios-de-twitter-por-desestabilizarsistema-bancario-

314 Reporteros sin Fronteras, "Internet en libertad vigilada. Venezuela", disponible en: http://es.rsf.org/surveillance-venezuela%2c39771.html y

"Dos twitteros detenidos por difundir falsos rumores sobre sistema bancario", *Correo del Orinoco*, 8 de julio de 2010, http://www.correodelorinoco.gob.ve/judiciales-seguridad/dos-twitteros-detenidos-difundir-falsos-rumores-sobre-sistema-bancario/

315 Reporteros sin Fronteras, *supra* nota 63.

316 Ley general de bancos y otras instituciones financieras, disponible en http://www.bcv.org.ve/c3/leybancos.pdf

de comunicación está cometiendo un delito y debe responder por ello ante las autoridades competentes[317].

La Relatoría Especial para la Libertad de Expresión de la OEA pone ejemplos de figuras penales vagas e imprecisas que pueden ser utilizadas para sancionar expresiones críticas o de protesta[318]. "Menoscabar la confianza de los clientes" y "atentar contra la reputación o el prestigio financiero" de una entidad bancaria pueden caer dentro de esta categoría. Además, merece una especial llamada de atención la idea de que una empresa puede tener honor y reputación.

La jurisprudencia interamericana ha definido la libertad de expresión como "el derecho del individuo y de toda la comunidad a participar en debates activos, firmes y desafiantes respecto de todos los aspectos vinculados al funcionamiento normal y armónico de la sociedad" y ha señalado en reiteradas ocasiones que, en el debate sobre asuntos de interés público, se protege tanto la emisión de expresiones inofensivas y bien recibidas por la opinión pública, como aquellas que chocan, irritan o inquietan a un sector cualquiera de la población[319].

Ninguno de estos dos ejemplos de criminalización de actividades relacionadas con "pánico financiero" se subsumen en los discursos no protegidos por la libertad de expresión según el SIDH. Tampoco se ajustan al test tripartito, en tanto estas limitaciones a la libertad de expresión no se encuentran establecidas en forma taxativa, precisa y clara y esto no provee seguridad jurídica a los ciudadanos.

Como señalan los estándares interamericanos en la materia, la normativa que penaliza discurso bajo figuras vagas o ambiguas como éstas "otorgan facultades discrecionales muy amplias a las autoridades son incompatibles con la Convención Americana, porque pueden sustentar potenciales actos de arbitrariedad que

---

317 *Correo del Orinoco*, *supra* nota 63.

318 CIDH, Comunicado de prensa R 44/15, 2011, "En el día mundial de la libertad de prensa, la relatoría especial llama a los Estadosa abstenerse de usar el derecho penal para silenciar las voces críticas", disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=986&lID=2

319 Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, *Marco jurídico interamericano sobre el derecho a la libertad de expresión*, 2009, Discursos especialmente protegidos, Discurso político y sobre asuntos de interés público, punto 34, disponible en: https://www.oas.org/es/cidh/expresion/docs/cd/sistema_interamericano_de_derechos_humanos/index_MJIAS.html

equivalgan a censura previa o que impongan responsabilidades desproporcionadas por la expresión de discursos protegidos"[320].

Asimismo, el marco jurídico señala que "Los Estados no son libres de interpretar de cualquier forma el contenido de estos objetivos para efectos de justificar una limitación de la libertad de expresión en casos concretos. La jurisprudencia interamericana se ha detenido en la interpretación de algunos de ellos, concretamente, en la noción de "protección de los derechos de los demás", y de la noción de 'orden público'"[321].

En este sentido, la Corte Interamericana señala que para garantizar el "orden público" es necesaria la mayor circulación de información posible. Y que "…no resulta suficiente invocar meras conjeturas sobre eventuales afectaciones del orden, ni circunstancias hipotéticas derivadas de interpretaciones de las autoridades frente a hechos que no planteen claramente un riesgo razonable de disturbios graves" y agrega que "Una interpretación más amplia o indeterminada abriría un campo inadmisible a la arbitrariedad y restringiría de raíz la libertad de expresión que forma parte integral del orden público protegido por la Convención Americana"[322].

En la región, encontramos tipificaciones similares en normativas penales y en legislación sobre delitos financieros[323] que podrían derivar en decisiones judiciales similares a estas que acabamos de analizar. Esto podría representar una tendencia a tener en cuenta por el impacto que puede tener en la libertad de expresión en línea.

Terrorismo

México. Caso tuiteros de Veracruz. Terrorismo equiparado y sabotaje

Gilberto Martínez Vera y María de Jesús Bravo Pago fueron encarcelados en agosto de 2011 a raíz de mensajes publicados en Twitter y Facebook que daban cuenta de rumores sobre posibles ataques a escuelas locales[324]. Según las autoridades

---

320 *Ibíd.*, Condiciones que deben cumplir las limitaciones para ser legítimas según la Convención Americana, punto 70.

321 *Ibíd.*

322 *Ibíd.,* Limitaciones a la libertad de expresión, punto 82.

323 Figuras similares aparece, por ejemplo, en Ecuador (COIP, artículo 322), en Venezuela (decreto del Sector Bancario, artículo 226), Perú (CP, artículo 249), Colombia (CP, artículo 302) y en Panamá (CP, artículo 260).

324 *Véase también*, Robles Maloof, Jesús y García, Luis Fernando, "Internet surveillance technologies in Mexico", Internews. Disponible en: http://contingentemx.net/2014/11/05/internet-surveillance-technologies-in-mexico/

veracruzanas, esto ocasionó que muchos padres recogieran a niños y niñas varias escuelas cerraran temporalmente[325].

Estas acciones a través de redes sociales fueron enmarcadas dentro de los delitos de "terrorismo equiparado" y sabotaje en "contra de la seguridad del Estado"[326], previstos en el Código Penal del estado de Veracruz, en México.

Los acusados, en primer término, fueron encarcelados [327] por el delito de terrorismo[328]. Sin embargo, de acuerdo al pedido formal de prisión, el juzgado determinó que Martínez Vera y Bravo Pagolos no habían incurrido en este delito sino en el de "terrorismo equiparado"[329], que establece que se considera terrorista y se sancionará como tal a la persona que "dé voces de alarma o provoque estruendos por los medios idóneos, simulando la posible existencia de alguno de los actos considerados por el delito de terrorismo, con el fin de suscitar tumultos, desórdenes, alarma o zozobra aun cuando éstos no se produzcan"[330]. Este delito, según el Código Penal estadual, prevé una condena de tres a treinta años de prisión.

En el mismo auto de formal prisión, el juzgado también señaló que incurrieron en el delito de sabotaje, que establece penas de dos a veinte años de prisión al que "con el fin de trastornar gravemente la vida económica o cultural del Estado o alterar su capacidad de asegurar el orden público, dañe, destruya o entorpezca servicios

---

325 Amnistía Internacional – México, "Personas en riesgo de prisión en México tras publicaciones en Twitter y Facebook", disponible en: http://amnistia.org.mx/nuevo/2011/09/01/personas-en-riesgo-de-prision-en-mexico-tras-publicaciones-en-twitter-y-facebook/

326 Juzgado Tercero de Primera Instancia, Xalapa, Veracruz, Auto de formal prisión, disponible en: https://es.scribd.com/doc/63750611/Auto-de-formal-prision-a-tuiteros

327 "Veracruz: Arrestan a dos por difundir mensajes terroristas", *Animal Político*, 26 de agosto de 2011, disponible en: http://www.animalpolitico.com/2011/08/arrestan-en-veracruz-a-dos-por-difundir-mensajes-terroristas/

328 Según el código penal de Veracruz, se considera terrorista "(...) a quien utilizando explosivos, sustancias tóxicas, armas de fuego o por incendio, inundación o por cualquier otro medio realice actos en contra de personas, las cosas o servicios al público, que produzcan alarma, temor, terror en la población o en un grupo o sector de ella, para perturbar la paz pública o tratar de menoscabar la autoridad del Estado o presionar a ésta para que tome una determinación". Código Penal para el Estado Libre y Soberano de Veracruz de Ignacio de la Llave, Capítulo V, artículo 311, disponible en: http://www.legisver.gob.mx/leyes/LeyesPDF/PENAL0708152.pdf

329 "Los argumentos del juez para dar formal prisión a tuiteros", *Animal Político*, 2 de septiembre de 2011, http://www.animalpolitico.com/2011/09/los-argumentos-del-juez-para-dar-formal-prision-a-tuiteros/

330 Art. 313, Cód. Pen. para el Estado Libre y Soberano de Veracruz de Ignacio de la Llave.

públicos, centros de producción o distribución de bienes y servicios básicos; elementos fundamentales de instde instituciones de docencia o investigación o recursos esenciales que el Estado destine para mantenimiento del orden público"[331].

En el marco de esta causa, la organización Artículo 19 presentó un *amicus curiae* afirmando que estos delitos de "terrorismo equiparado" y "sabotaje", y los actos que derivaron de su aplicación, son incompatibles con los tratados sobre derechos humanos aprobados por el Estado mexicano[332].

Como consecuencia de este caso, el 13 de septiembre de 2011, desde el gobierno de Veracruz se presentó una propuesta para tipificar el delito de "perturbación del orden público". El argumento de los impulsores de esta norma era que, bajo este delito que no existía al momento de la acusación, Martínez Vera y Bravo Pagolos podrían salir bajo fianza.

El 21 de septiembre de 2011, se aprobó esta reforma conocida como #leyjavierduarte, por su impulsor, el gobernador de Veracruz, Javier Duarte. Esta ley modificó el artículo 343 del Código Penal de Veracruz tipificando el delito de "perturbación del orden público". La reforma establecía que:

> (…) a quien por cualquier medio, afirme falsamente la existencia de aparatos explosivos u otros; de ataques con armas de fuego o de sustancias químicas, biológicas o tóxicas que puedan causar daño a la salud, ocasionando la perturbación del orden público, se le impondrá prisión de uno a cuatro años y multa de quinientos a mil días de salario mínimo, atendiendo a la alarma o perturbación del orden efectivamente producida[333].

El mismo día en que se aprobó la norma y después de pasar un mes en la cárcel por los delitos de terrorismo equiparado y sabotaje, los tuiteros detenidos salieron en libertad[334].

---

331 *Ibíd.*, art. 314.

332 Artículo 19, "Article 19 presenta Amicus Curiae para Amparo en Veracruz por personas acusadas de terrorismo", 20 de septiembre de 2011, disponible en: http://www.articulo19.org/mexico-article-19-presenta-amicus-curiae-para-amparo-en-veracruz-por-personas-acusadas-de-terrorismo/#sthash.n1vm9wB9.dpuf

333 Juárez, Geraldine, "Ley anticonstitucional e ilegítima es aprobada por el Gobierno de Veracruz", *Hipertextual,* 21 de septiembre de 2011, disponible en: http://hipertextual.com/2011/09/ley-javier-duarte-inconstitucional-e-ilegitima-es-aprobada-por-el-gobierno-de-veracruz

334 "México: liberan a tuiteros, pero tipifican nuevo delito", *BBC Mundo*, 22 de septiembre de 2011, disponible en: http://www.animalpolitico.com/2011/09/procuraduria-de-veracruz-ya-no-ejercera-accion-penal-contra-twitterroristas/

El 20 de junio de 2013, la Suprema Corte de Justicia mexicana declaró inconstitucional la llamada Ley Duarte. En su decisión, el tribunal resolvió que el artículo 373 del Código veracruzano violaba garantías constitucionales de libertad de expresión, derecho a la información y exacta aplicación de la ley penal[335][336].

Venezuela. Caso Medina Ravell. Instigación al terrorismo

Otro caso relevante es el de Federico Medina Ravell, cuyo hogar fue allanado en enero de 2013 por entender que era el titular de @lucioquincioc, una cuenta de Twitter publicaba información sobre la salud del fallecido presidente Hugo Chávez Frías[337].

Luego, una fiscal del estado de Carabobo fue designada para iniciar una investigación sobre presunta "instigación al terrorismo a través de las redes sociales"[338].

No es claro qué tipo penal se utilizó ya que la "instigación al terrorismo" no está tipificada en la normativa penal venezolana[339]. No obstante, es preocupante que se haya realizado un allanamiento con sustento en el tipo penal de terrorismo.

---

335 "Corte tumba la Ley Duarte en Veracruz contra tuiteros", *Animal Político*, disponible en:http://www.animalpolitico.com/2013/06/corte-tumba-la-ley-duarte/

336 Corte Suprema de Justicia de la Nación, México, Acción de inconstitucionalidad, Expediente 29/2011, 20 de junio de 2013, disponible en: http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=132774

337 "Fotos exclusivas: Sebin allanó una vivienda buscando al tuitero @lucioquincioc", *Noticias 24*, 6 de enero de 2013, http://www.noticias24.com/venezuela/noticia/144376/comision-del-sebin-allano-casa-del-primo-de-alberto-federico-ravell-en-el-trigal-fotos/ y "Ministerio Público investiga presunta instigación al terrorismo a través de las redes sociales", *Venezolana de Televisión*, http://www.vtv.gob.ve/articulos/2013/01/08/ministerio-publico-investiga-presunta-instigacion-al-terrorismo-a-traves-de-las-redes-sociales-2930.html

338 Ministerio Público, República Bolivariana de Venezuela, "Ministerio Público investiga presunta instigación al terrorismo a través de las redes sociales", 8 de enero de 2013, http://www.mp.gob.ve/web/guest/buscador/-/journal_content/56/10136/1836394

339 Tampoco surge de las fuentes consultadas en qué estado se encuentra la investigación contra Medina Ravell. En una entrevista con *The Commentator*, reveló que estaba en proceso de solicitar asilo político en EE.UU. *Véase*, "El hombre que Chávez quiere muerto", *The Commentator*, 9 de enero de 2015, disponible en: http://www.thecommentator.com/article/2415/el_hombre_que_chavez_quiere_muerto [Consultado: 2015, septiembre].

Si bien la Relatoría Especial para la Libertad de Expresión de la OEA ha expresado que el terrorismo es una amenaza cierta a los derechos humanos y la democracia[340], recientemente advirtió sobre el uso de figuras penales vagas e imprecisas, como el terrorismo, para sancionar expresiones críticas o de protesta. La relatoría sostuvo que "Un sistema democrático pleno debe fomentar la deliberación pública y garantizar una mayor apertura frente a expresiones y apreciaciones realizadas por los ciudadanos en ejercicio del control democrático"[341].Es particularmente preocupante si se tiene en cuenta que varios países de la OEA cuentan con legislación contra el terrorismo[342].

---

340 Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. Informe "Libertad de Expresión e Internet". Diciembre de 2013. Párrafo 145.

341 Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. Comunicado de Prensa R 44/15. 3 de mayo de 2015.

342 Por ejemplo, Antigua y Barbuda (The Prevention of Terrorism Act. Aprobada en 2005, modificada en 2008 y 2010. http://ondcp.gov.ag/wp-content/uploads/2014/05/amended_pta-2010.pdf); Bolivia (Artículo 133 del Código Penal http://www.oas.org/juridico/spanish/gapeca_sp_docs_bol1.pdf), Canadá (Código Penal. PART II.1. TERRORISM http://laws-lois.justice.gc.ca/eng/acts/C-46/FullText.html); Chile (Ley 18314); Colombia (Código Penal. Artículo 343. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388); Costa Rica (Código Penal. Artículo 6 bis. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=98548&strTipM=TC); Cuba (Código Penal. Artículo 106 http://www.cepal.org/oig/doc/cub1987codigopenalley62.pdf); Ecuador (Código Penal. Artículo 366. http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf); El Salvador (Ley Especial contra Actos de Terrorismo. Decreto 108. http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-especial-contra-actos-de-terrorismo); Guatemala (Ley para prevenir y reprimir el financiamiento del terrorismo. Decreto 58/2005 http://old.congreso.gob.gt/archivos/decretos/2005/gtdcx58-2005.pdf); Honduras (Código Penal. Artículo 335. https://www.ccit.hn/wp-content/uploads/2013/12/Codigo-Pena-Honduras.pdf); Jamaica (Terrorism prevention Act. http://moj.gov.jm/laws/terrorism-prevention-act);México (Código Penal Federal. Artículo 139. http://www.diputados.gob.mx/LeyesBiblio/pdf/9_120315.pdf); Nicaragua (Código Penal. Artículo 394. http://www.poderjudicial.gob.ni/pjupload/noticia_reciente/CP_641.pdf);Panamá (Ley 62. Agrega el delito de terrorismo al Código Penal. 17 de septiembre de 2013. http://www.organojudicial.gob.pa/cendoj/wp-content/blogs.dir/cendoj/ley-62-de-17-de-septiembre-de-2013.pdf); Perú (Decreto Ley 25.475. http://www.oas.org/juridico/PDFs/mesicic5_per_6_dec_ley_25475.pdf); República Dominicana (Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología.

En la misma línea se encuentran las declaraciones de la Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de Naciones Unidas respecto de la tipificación como delito de expresiones legítimas. El ex relator, Frank La Rue, expresó su preocupación por legislación que "suele justificarse por motivos de protección de la reputación de una persona, seguridad nacional o lucha contra el terrorismo, pero, en la práctica, se utiliza para censurar contenidos que no son del gusto del Gobierno y otras entidades poderosas o con los que estas instancias no están de acuerdo"[343].

En su informe, el ex relator sostuvo que la restricción a la libertad de expresión en virtud de razones de seguridad nacional o terrorismo únicamente podría justificarse si "a) la expresión tiene por objetivo instigar a la violencia inmediata; b) es probable que instigue a ese tipo de violencia; y c) existe una relación directa e inmediata entre la expresión y la posibilidad de que se produzca ese tipo de violencia"[344][345],

En conclusión, si bien se reconoce que el terrorismo es un problema cierto, la utilización de ese tipo penal para acallar discursos críticos no se ajusta a los estándares internacionales de derecho a la libertad de expresión.

Incitación al pánico o publicación de mensajes desestabilizadores

Otro tipo de figuras penales que se han utilizado para acallar discurso crítico son aquellas variantes de instigación pública, incitación al pánico, al caos o la publicación de mensajes desestabilizadores.

---

http://www.oas.org/juridico/PDFs/repdom_ley5307.pdf); Venezuela (Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo, http://www.oas.org/juridico/PDFs/mesicic4_ven_ley_del_org_finan_terr.pdf)

343 ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. A/HRC/17/27. 16 de mayo de 2011. Párrafo 34.

344 Principios de Johannesburgo sobre seguridad nacional, libertad de expresión y acceso a la información, Principio 6, aprobado en el documento E/CN.4/1996/39.

345 ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. A/HRC/17/27. 16 de mayo de 2011. Párrafo 36.

Venezuela. Caso Ortega Pérez[346]

El 13 de marzo de 2013, pocos días después de que falleciera el ex presidente Hugo Chávez Frías, Lourdes Alicia Ortega Pérez fue detenida por el CICPC. El ministro de Relaciones Interiores y Justicia, Néstor Luis Reverol Torres, informó que Ortega había sido detenida por usurpar la identidad de una funcionaria del Servicio Autónomo de Registros y Notarías (SAREN), y por publicar en su cuenta de Twitter (@Ulilou) mensajes desestabilizadores para el país[347]. Reverol también declaró que "se siguen monitoreando los mensajes de las redes sociales que pretenden desestabilizar al país"[348].

Extraoficialmente, se reveló que el tuit que desencadenó la detención era un comentario sobre la muerte de Hugo Chávez[349].

Según fuentes periodísticas, Lourdes Ortega fue imputada por la presunta comisión del delito de difusión de "información falsa" en los términos del artículo 296-A del Código Penal venezolano[350]. Esta normativa señala que:

> Todo individuo que por medio de informaciones falsas difundidas por cualquier medio impreso, radial, televisivo, telefónico, **correos electrónicos** o escritos panfletarios, cause pánico en la colectividad o la mantenga en zozobra, será castigado con prisión de dos a cinco años.
>
> Si los hechos descritos en el aparte anterior fueren cometidos por un funcionario público, valiéndose del anonimato o usando para tal fin el nombre ajeno, la pena se incrementará en una tercera parte. Este artículo

---

346 Espacio Público. "Detenida por un mensaje en Twitter", disponible en:http://www.espaciopublico.org/index.php/noticias/1-libertad-de-expresi/2575-detenida-por-un-mensaje-en-twitter; "Detienen a una mujer que enviaba "mensajes desestabilizadores" por las redes sociales", *Noticias24*, disponible en:http://www.noticias24.com/venezuela/noticia/155978/detienen-a-una-mujer-que-enviaba-mensajes-desestabilizadores-por-las-redes-sociales/

347 "Detenida mujer por un mensaje de Twitter", *El Nacional*, disponible en:http://www.el-nacional.com/sucesos/Detenida-mujer-mensaje-Twitter_0_152987493.html

348 "MIJ detiene a ciudadana por generar rumores desestabilizadores en red social Twitter", *Aporrea*, 13 de marzo de 2013, http://www.aporrea.org/ddhh/n224943.html

349 "Detenida mujer por un mensaje de Twitter", *El Nacional*, disponible:http://www.el-nacional.com/sucesos/Detenida-mujer-mensaje-Twitter_0_152987493.html;*véase también*, CP de Venezuela, disponible en: http://www.mp.gob.ve/c/document_library/get_file?uuid=4d73d650-7f5c-4fb1-8206-b2355fcdef65&groupId=10136

350 "LARA: Dejan libre a Twitera que comentó sobre cadáver de Chávez", *Reportero24*, disponible en: http://www.reportero24.com/2013/03/lara-dejan-libre-a-twitera-que-comento-sobre-cadaver-de-chavez/ [Consultado: 2015, septiembre]

será aplicado sin perjuicio a lo establecido en la legislación especial sobre los delitos informáticos, telecomunicaciones, impresos y transmisión de mensajes de datos[351]. (El resaltado es nuestro).

Venezuela. Caso Marcano y Hernández

Otro caso de personas detenidas en Venezuela en virtud de sus publicaciones en Twitter[352] es el de Lessy Marcano, un supuesto vidente, y Ginette Hernández, su sobrina, quien —en teoría—manejaba la cuenta de su tío.

Hernández y Marcano fueron detenidos por presuntamente publicar en Twitter, a través de la cuenta @Hiipolita, dos tuits prediciendo que la Asamblea Nacional estaría de luto, pocos días antes de la muerte del diputado Robert Serra[353].

Ambos fueron imputados por los delitos de difusión de información falsa, agavillamiento —ambos tipos contenidos en el Código Penal—y oferta engañosa —previsto en la Ley Especial Contra los Delitos Informáticos—[354].

Tabasco, México. Incorporación de delito de alarma falsa al Código Penal

---

[351] Artículo 296-A, Cód. Pen. de Venezuela, disponible en: http://www.mp.gob.ve/c/document_library/get_file?uuid=4d73d650-7f5c-4fb1-8206-b2355fcdef65&groupId=10136

[352] Este caso se enmarca en una serie de arrestos a ciudadanos venezolanos por publicaciones en redes sociales. *Véase*, Instituto Prensa y Sociedad de Venezuela, "Siete twitteros fueron detenidos por agentes de seguridad del estado venezolano", disponible en: https://www.ifex.org/venezuela/2014/11/05/twitteros_detained/es/ [Consultado: 2015, septiembre], *véase*, Espacio Público. "Informe sobre la aplicación del Pacto de Derechos Civiles y Políticos en su artículo 19. (Respuestas a la Lista de Cuestiones - CCPR/C/VEN/Q/4) Caracas – Ginebra, junio de 2015)", en el marco del examen de informes del Estado Venezolano ante el Comité de Derecho Humanos, disponible en:http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/VEN/INT_CCPR_CSS_VEN_20709_S.pdf [Consultado: 2015, septiembre].

[353] "Venezuela está encarcelando a los adivinos que hacen 'predicciones' en Twitter", *Vice News*, disponible en: http://www.vice.com/es_co/read/venezuela-encarcelando-a-los-adivinos-que-hacen-predicciones-en-twitter [Consultado: 2015, septiembre] y "Callen al tuitero", *El Universal*, 16 de noviembre de 2014, disponible en: http://www.eluniversal.com/nacional-y-politica/141116/callen-al-tuitero

[354] "Temor a la palabra", *El Universal*, disponible en: http://www.eluniversal.com/nacional-y-politica/150726/temor-a-la-palabra [Consultado: 2015, septiembre].

El Congreso de Tabasco aprobó en septiembre de 2011 una ley que se propone castigar con hasta seis años de cárcel a quienes utilicen el servicio telefónico o "cualquier otro medio de comunicación masiva" para dar aviso de alarma falsa[355].

En esta modificación al Código Penal estadual, el artículo 312 bis dedicado a "De la veracidad de las comunicaciones a los servicios de emergencia", señala que:

> A quien utilice el servicio telefónico o cualquier medio de comunicación masiva para dar aviso de alarma o emergencia falsa, provocando con ello la movilización o presencia de los servicios de emergencia o cuerpos de seguridad pública, **o provoque caos o inseguridad social**, se le impondrá prisión de seis meses a dos años y de cincuenta a trescientos días multa[356]. (El subrayado es nuestro).

Según fuentes periodísticas, el legislador que impulsó la reforma aseguró en su momento que "se tendrá un equipo especial para detectar a quienes intenten crear pánico entre los ciudadanos" y que se incluiría a las redes sociales[357].

La ambigüedad y falta de precisión de términos como "caos", "pánico", "zozobra" o "inseguridad social" de los ejemplos descriptos en esta sección podría entenderse como contrario a los estándares interamericanos, que establecen que:

> Las leyes que establezcan responsabilidades ulteriores han de ser lo suficientemente explícitas para garantizar a los individuos un margen de certeza respecto de las posibles responsabilidades de sus expresiones. La ambigüedad o falta de claridad puede crear un margen de incertidumbre que podría inhibir a las personas de manifestar opiniones o informaciones y de participar activamente en el debate democrático.

Y, específicamente, cuando se utiliza el derecho penal, la CIDH insta a los Estados a "utilizar términos estrictos y unívocos, que acoten claramente las conductas punibles"[358].

---

355 "Modificaciones a Código Penal de Tabasco, atentan contra la libertad de expresión", *Animal Político*, 1 de septiembre de 2011, disponible en: http://www.animalpolitico.com/2011/09/aprueban-ley-contra-el-%E2%80%9Crumor%E2%80%9D-en-tabasco/

356 Artículo 312 Bis., Código de Procedimientos Penales del Estado de Tabasco, disponible en:http://cgaj.tabasco.gob.mx/leyes/estatales/leyes

357 Xicoténcatl, Fabiola, "Tabasco calla y castiga rumor; penaliza difusión de falsas alarmas", 1 de septiembre de 2011, disponible en: http://www.excelsior.com.mx/node/765346

358 CIDH, *supra* nota 32.

Venezuela. Casos de instigación pública

Caso Magaly Contreras

María Magaly Contreras, una mujer venezolana de 55 años con trastornos psíquicos, difundió mensajes en Twitter identificándose como vidente. Los mensajes advertían sobre la futura muerte de Fidel Castro ("Fidel castro te queda poco en este mundo, y también morirá la dictadura aquí en Venezuela y en otros países... veo a una mujer del Psuv, y de la revolución roja que se está hinchando por dentro..... quien originó y trajo la desgracias a nuestra Venezuela, va a morir pronto...Fidel Castro te vas a hacerle compañía a tu hijo Huguito… la muerte sigue y va por los rojos rojitos del Psuv, ay Jorge Rodríguez te veo gravemente enfermo... ay Jorge Rodríguez, la pelona te sigue las espaldas...y a Di Martino también… Dios cuida y protege a Venezuela...")[359].

Contreras fue detenida por el SEBIN en octubre de 2014, imputada con los delitos de "instigación pública"[360] e "intimidación pública por medio de información falsa"[361]. Finalmente, en abril de 2015 fue liberada, bajo medida de presentarse ante un tribunal cada quince días y acudir a consultas psicológicas y psiquiátricas dos veces por mes[362].

---

359 Espacio Público, "Informe sobre la aplicación del Pacto de Derechos Civiles y Políticos en su artículo 19. (Respuestas a la Lista de Cuestiones - CCPR/C/VEN/Q/4) Caracas – Ginebra, junio de 2015)", en el marco del examen de informes del Estado Venezolano ante el Comité de Derecho Humanos.Disponible:http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/VEN/INT_CCPR_CSS_VEN_20709_S.pdf [Consultado: 2015, septiembre]

360 "Artículo 283. Cualquiera que públicamente o por cualquier medio instigare a otro u otros a ejecutar actos en contravención a las leyes, por el solo hecho de la instigación será castigado: 1. Si la instigación fuere para inducir a cometer delitos para los cuales se ha establecido pena de prisión, con prisión de una tercera parte del delito instigado. 2. En todos los demás casos, con multas de ciento cincuenta unidades tributarias (150 U.T.), según la entidad del hecho instigado. Artículo 284. En el caso indicado con el numeral 1 del artículo 283, nunca podrá excederse de la tercera parte de la pena señalada al hecho punible a que se refiere la instigación. Artículo 285. Quien instigare a la desobediencia de las leyes o al odio entre sus habitantes o hiciere apología de hechos que la ley prevé como delitos, de modo que ponga en peligro la tranquilidad pública, será castigado con prisión de tres años a seis años.". Código Penal de Venezuela, Artículos 283, 284 y 285, disponible en: http://www.mp.gob.ve/c/document_library/get_file?uuid=4d73d650-7f5c-4fb1-8206-b2355fcdef65&groupId=10136

361 *Ibíd.*, artículo 296-A.

362 Espacio Público, *supra* nota 108.

Caso Leopoldo López

Leopoldo López, líder de la oposición venezolana, fue detenido por convocar una protesta contra el gobierno del presidente Nicolás Maduro. Durante la protesta, ocurrieron incidentes de violencia y López fue detenido acusado de instigar dichos actos violentos[363].

Parte de la acusación contra López se sustentó en dos informes que realizó la fiscalía, analizando discursos de López y su cuenta de Twitter. La fiscalía llegó a la conclusión de que, a través de sus expresiones, Leopoldo López instigó a sus seguidores a actuar de forma violenta[364]. Algunos mensajes publicados su cuenta de Twitter fueron:

12-F Al comenzar la retirada entró la Fuerza Pública y los colectivos actuando de manera conjunta y en contra de los manifestantes. Hay heridos.
9-F Aún crees q debemos esperar al 2019 para salir d este régimen? No te quedes en casa el #12F únete a la protesta pacífica y constitucional!
8-F Nuestro terreno de lucha: LaCalle; Nuestra estrategia: la NoViolencia; Nuestro compromiso: LaMejorVenezuela. #12F 6-F Quizá todavía haya quienes crean que la protesta NoViolenta no tiene sentido, a ellos les pregunto: a estas alturas qué otra opción nos queda?"[365].

La Comisión Interamericana de Derechos Humanos emitió el 20 de abril de 2015 la medida cautelar N° 335-14[366] respecto de las condiciones de la detención de López, solicitando que el Estado de Venezuela adopte las medidas necesarias para preservar su vida e integridad. El 25 de septiembre de 2015, la Comisión emitió un comunicado de prensa expresando su preocupación por la sentencia condenatoria contra López en Venezuela por instigación pública, daños a la propiedad, incendio intencional, asociación para delinquir.

Sobre el derecho a la libertad de expresión y el derecho de protesta pacífica, la Comisión sostuvo que;

---

363 "Venezuela: ¿qué pasó con Leopoldo López?", *BBC*, disponible en: http://www.bbc.com/mundo/noticias/2014/03/140317_venezuela_leopoldo_lopez_mes_carcel_dp

364 Morales, Maru, "Caso López criminaliza discurso político y opiniones en Internet", *El Nacional*, 9 de junio de 2014, disponible en: http://www.el-nacional.com/politica/Caso-Lopez-criminaliza-opiniones-Internet_0_424157745.html

365 *Ibíd.*

366 Comisión Interamericana de Derechos Humanos, Medida cautelar N° 335-14, disponible en: http://www.oas.org/es/cidh/decisiones/pdf/2015/MC335-14-ES.pdf

> (…) las voces de la oposición son imprescindibles para una sociedad democrática, sin las cuales no es posible el logro de acuerdos que atiendan a las diferentes visiones que prevalecen en una sociedad. La libertad de pensamiento y expresión está protegida por los artículos IV de la Declaración y 13 de la Convención Americana, y si bien no se trata de un derecho absoluto, las restricciones al mismo deberán tener un carácter excepcional y no podrán limitar, más allá de lo estrictamente necesario, su pleno ejercicio[367].

Además, en línea con lo desarrollado en este informe, la CIDH reiteró que "El abuso de tipos penales vagos y ambiguos, que permiten la atribución de responsabilidades a quienes participan o convocan a una manifestación, genera un efecto amedrentador en el ejercicio del derecho a la protesta, que resulta incompatible con los principios democráticos"[368].

Normas que agravan la pena por el medio

Si bien es poco común la normativa que criminalice únicamente expresiones vertidas en línea, en algunos países se observa la práctica de agravar las penas por el medio en el que se difundan las expresiones. En algunos casos, como el de Perú, la normativa nombra explícitamente a internet, mientras que en otros, como es el caso de las injurias en Brasil, se agravan las penas a las expresiones vertidas en medios que faciliten la divulgación. Por sus características, internet quedaría inherentemente incluida en aquellos medios que faciliten divulgación masiva.

Discriminación

Perú. Discriminación

En Perú, la Ley N° 30.171 de marzo de 2014 modificó el Código Penal[369], agregando el siguiente artículo:

---

[367] Comisión Interamericana de Derechos Humanos, "CIDH manifiesta su preocupación ante la sentencia contra Leopoldo López en Venezuela", 25 de septiembre de 2015, disponible en: http://www.oas.org/es/cidh/prensa/comunicados/2015/107.asp

[368] Comisión Interamericana de Derechos Humanos, "CIDH manifiesta su preocupación ante la sentencia contra Leopoldo López en Venezuela", 25 de septiembre de 2015, disponible en: http://www.oas.org/es/cidh/prensa/comunicados/2015/107.asp

[369] Ley 30171 disponible en http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc02_2011_2.nsf/d99575da99ebfbe305256f2e006d1cf0/e0589bd1613de56e05257c97004d0f7a/$FILE/30171.pdf

Artículo 323. Discriminación e incitación a la discriminación
El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años, ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.

Si el agente es funcionario o servidor público la pena será no menor de dos, ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.

La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación, la incitación o promoción de actos discriminatorios se ha materializado mediante actos de violencia física o mental o a través de internet u otro medio análogo"[370]. (El subrayado es nuestro).

Como desarrollamos previamente, los estándares internacionales de derechos humanos extienden el derecho a la libertad de expresión a aquellas expresiones difundidas por internet y que:

> Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad (la prueba "tripartita")[371].

Esto impone el mismo estándar estricto que se aplica para analizar restricciones a la libertad de expresión a aquellas difundidas por internet. Esta normativa no cumple con los estrictos requisitos impuestos por el test tripartito, en tanto no es lo suficientemente clara y precisa. Términos como "promover en forma pública", "opinión de cualquier índole", "menoscabar el reconocimiento" son vagos y podrían

[370] Disponible en http://spij.minjus.gob.pe/CLP/contenidos.dll?f=templates&fn=default-codpenal.htm&vid=Ciclope:CLPdemo

[371] Declaración conjunta sobre libertad de expresión e Internet, 2011.

dar lugar a una restricción excesiva. Además, tampoco cumpliría con el requisito de proporcionalidad ni de necesidad, ya que existen medios para perseguir el objetivo de evitar la discriminación que son menos restrictivos que la criminalización.

Además, la Relatoría Especial para la Libertad de Expresión de la OEA ha sido clara al expresar que penalizar específicamente el discurso difundido por internet, o agravar las penas, es inaceptable, en tanto "ello significaría una restricción desproporcionada para la expresión en Internet, bajo un paradigma que considera a ese medio más riesgoso que otros. Ese tipo de medidas tendría el efecto de restringir y limitar a Internet como espacio para el libre intercambio de ideas, informaciones y opiniones"[372][373].

En conclusión, esta normativa peruana contra la discriminación online sería contraria a los estándares interamericanos de libertad de expresión en general, pues no cumple con los requisitos del test tripartito, y además impone restricciones desproporcionadas a internet como un espacio de intercambio libre de ideas y opiniones.

Injurias agravadas por el medio de divulgación

Si bien no se refieren específicamente a internet, hay casos en los que el medio utilizado —como blogs, por ejemplo—ha sido causal de un agravamiento de la pena en casos de delitos contra el honor. Los casos presentados a continuación son ejemplo de esta tendencia de incluir a internet dentro de estos medios que facilitan y amplifican la divulgación de estas expresiones consideradas lesivas para el honor.

Estas decisiones judiciales, además de presentar los problemas con el SIDH que ya analizamos (la criminalización de expresiones, informaciones y opiniones críticas sobre asuntos de interés público) se agrava por la utilización de internet cayendo bajo lo que la relatoría ha señalado como un paradigma que la considera como medio "riesgoso" y que permitiría amplificar la lesión al honor. Esta es una tendencia

372 Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. A/HRC/17/27. 16 de mayo de 2011. Párr. 72. Disponible para consulta en: http://ap.ohchr.org/documents/dpage_s.aspx?m=85 En Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. 31 de diciembre de 2013.

373 Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. 31 de diciembre de 2013. Párrafo 74.

potencialmente alarmante, en tanto encontramos tipificaciones similares los códigos penales de la región[374] que podrían ser utilizados para penalizar de forma más rigurosa a la expresión vertida online.

Brasil. Caso Cristián Góes[375]

En 2012, el bloguero Cristián Góes publicó en el sitio Infonet una crónica literaria criticando prácticas de militares. Si bien no lo nombraba, el vicepresidente del Tribunal de Justicia del estado de Sergipe entendió, por un término utilizado en la crónica, que Góes hablaba de él. A raíz de esta publicación, el funcionario le inició una causa civil reclamando daños y además una causa penal por injurias.

Góes fue condenado a siete meses y 16 días de prisión convertidos a servicios comunitarios. El tribunal entendió que la libertad de expresión encuentra un límite en la honra. Además, aumentó la pena ya que la injuria fue publicada en un medio que facilitó la divulgación, un sitio que tiene mucha llegada[376].

La sentencia fue apelada y se agotaron los recursos internos. El caso, finalmente, generó el reclamo de organizaciones globales dedicadas a la libertad de expresión[377] y fue llevado ante la CIDH por organizaciones como Artigo 19 e Intervoces.

La figura utilizada en este caso para perseguir a Góes fue el de injuria, tipificado en el código penal de Brasil. La normativa señala que[378]:

Injuriar a alguien, ofender su dignidad o decoro:
Pena – detención, de uno a seis meses, o multa.
§ 1º - El juez puede no aplicar la pena:
I – cuando el ofendido, de forma reprensible, haya provocado la injuria directamente;

[374] Salvo casos como los de Uruguay y Argentina que introdujeron modificaciones en sus códigos penales respecto de las calumnias e injurias (encuadrados en los que Eduardo Bertoni denomina "modelos de despenalización limitada de los delitos contra el honor") y el México que derogó a nivel federal estos delitos en 2007, persiste en la región la tendencia de criminalizar este tipo de expresiones. *Véase,* Bertoni, Eduardo, *Difamación por Internet. Problemas sobre jurisdicción y ley aplicable*, Buenos Aires, Editorial Ad-Hoc, 2015, p. 42.

[375] Ver denuncia y sentencia enhttp://artigo19.org/centro/casos/detail/20

[376] Juizado Especial Criminal da Comarca de Aracaju/se. Sentencia n° 201245102580. P 7.

[377] Reporteros sin Fronteras, "Pena de prisión contra un periodista por un texto ficticio publicado en su blog", 8 de julio de 2013, disponible en:http://www.rsf-es.org/news/brasil-pena-de-prision-contra-un-periodista-por-un-texto-ficticio-publicado-en-su-blog/

[378] Artículo 140, CP de Brasil, disponible en http://www.oas.org/juridico/mla/pt/bra/pt_bra-int-text-cp.pdf

II – en el caso de represalias inmediatas, que consistan en otra injuria.
§ 2º - Si la injuria consiste en violencia o golpes que, por su naturaleza o por el medio empleado, se consideren degradantes:
Pena – detención, de tres meses a un año, y multa, más allá de la pena correspondiente a la violencia.
§ 3° - Si la injuria consiste en la utilización de elementos sobre raza, color, etnia, religión, origen o condición de persona mayor o con discapacidad; (Redacción según la Ley N° 10.741 de 2003).
Pena – reclusión de uno a tres años y multa. (Incluido por la Ley N° 9.459 de 1997)[379] (Traducción propia)

Específicamente, un inciso de la normativa penal prevé un aumento de la pena si el crimen es cometido "en la presencia de varias personas, o por un medio que facilite la divulgación de la calumnia, la difamación o la injuria".

Disposiciones comunes
Art. 141 – Las penas previstas en este Capítulo se aumentarán en un tercio, si cualquiera de los dos crímenes es cometido:

I- Contra el Presidente de la República, o contra algún jefe de gobierno extranjero;
II- Contra funcionario público, en razón de sus funciones;
III- En presencia de varias personas, o por un medio que facilite la divulgación de la calumnia, la difamación o la injuria.
IV- Contra persona mayor de 60 (sesenta) años, o con discapacidad, excepto en el caso de injuria. (Incluido por la Ley N° 10.741, de 2003)

Párrafo único. Si el crimen es cometido por pago o promesa de recompensa, se dobla la pena.[380] (Traducción y resaltado propios)

---

[379] Código Penal de Brasil, disponible en: http://www.oas.org/juridico/mla/pt/bra/pt_bra-int-text-cp.pdf

Versión original:

"Injuriar alguém, ofendendo-lhe a dignidadeou o decoro:

Pena - detenção, de um a seis meses, ou multa.

§ 1º - O juiz pode deixar de aplicar a pena:

I - quandoo ofendido, de forma reprovável, provocoudiretamente a injúria;

II - no caso de retorsãoimediata, que consista emoutrainjúria.

§ 2º - Se a injúria consiste emviolênciaouvias de fato, que, por suanaturezaou pelo meioempregado, se consideremaviltantes:

Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

§ 3o Se a injúria consiste nautilização de elementos referentes a raça, cor, etnia, religião, origemou a condição de pessoaidosaou portadora de deficiência:(Redação dada pela Lei nº 10.741, de 2003)

Pena - reclusão de um a três anos e multa.(Incluído pela Lei nº 9.459, de 1997)"

Brasil. Caso Blog Do Paulinho

"Paulinho", un periodista deportivo brasileño, publicó en su blog[381] una crítica a un abogado, que lo acusó de injuria. El periodista fue condenado por este delito, con un aumento de la pena por el inciso de "medios que faciliten la divulgación"[382].

Si bien el tribunal de segunda instancia redujo la pena porque se entendió que una de las acciones había prescripto, el periodista está preso desde julio de 2015.Según el artículo 141 del Código de Penal de Brasil, la conducta del periodista se encuadró en el delito de injuria agravada por "*III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria*"[383].

Perú. Caso de José Alejandro Godoy, bloguero sentenciado a prisión por difamación agravada

El 20 de octubre de 2010, el periodista José Alejandro Godoy fue sentenciado a tres años de prisión suspendida, además del pago de 350 mil soles y 120 días de trabajo social, en un juicio por difamación que le entabló el ex congresista Jorge Mufarech Nemy. Esta es la condena máxima que puede imponerse por un delito de difamación agravada en Perú[384].

---

380 *Ibíd.*

Versión original:

"Disposiçõescomuns

Art. 141 - As penas cominadasneste Capítulo aumentam-se de umterço, se qualquer dos crimes é cometido:

I - contra o Presidente da República, ou contra chefe de governoestrangeiro;

II - contra funcionário público, emrazão de suasfunções;

*III - **napresença de váriaspessoas, ou por meio que facilite a divulgação da calúnia, da difamaçãoou da injúria.***

IV – contra pessoamaior de 60 (sessenta) anos ou portadora de deficiência, exceto no caso de injúria.(Incluído pela Lei nº 10.741, de 2003)

Parágrafo único - Se o crime é cometido mediante paga oupromessa de recompensa, aplica-se a pena emdobro"

381 *Véase*,https://blogdopaulinho.wordpress.com/

382 Artículo 141, Código Penal de Brasil.

383 *Ibíd.*

384 Instituto Prensa y Sociedad, Comunicado: "Caso blogger José Alejandro Godoy", 10 de noviembre de 2009, disponible en: http://www.ipys.org/comunicado/38

En el 2009, el entonces congresista demandó a Godoy por un post publicado en su blog político "Desde el Tercer Piso"[385] sobre las amenazas del también ex ministro contra el asesor de la bancada nacionalista Julio Arzibú Gonzales. En el post se difundían diversos documentos, entre estos, una carta del asesor amenazado al legislador nacionalista Fredy Otárola en la que cuenta las amenazas del entonces legislador[386].

El código penal peruano establece que incurrirá en el delito de difamación:

> El que, ante varias personas, reunidas o separadas, pero de manera que pueda difundirse la noticia, atribuye a una persona, un hecho, una cualidad o una conducta que pueda perjudicar su honor o reputación, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a ciento veinte días-multa[387].

La aplicación de la normativa penal en casos de difamación, como vemos, no puede llevar al autor a prisión. Salvo en los casos en que, como en el de Godoy, sea agravada por el medio. El código penal de Perú, específicamente, señala que "Si el delito se comete por medio del libro, la prensa u otro medio de comunicación social, la pena será privativa de libertad no menor de uno ni mayor de tres años y de ciento veinte a trescientos sesenticinco días-multa"[388].

Godoy fue sentenciado por el delito de difamación agravada[389]. Como ya señalamos, el uso del derecho penal para sancionar una investigación periodística sobre un asunto de interés público va en contra de los estándares del Sistema Interamericano y lo que señaló uno de sus organismos, la Relatoría Especial para la Libertad de Expresión en su informe de 2009, al señalar que los Estados no deben usar el derecho penal para sancionar a quienes hacen investigaciones o emiten

---

385 Godoy, José Alejandro, "Jorge Mufarech amenaza asesor parlamentario por caso Rospigliosi", *Desde el tercer piso*, 17 de abril de 2009, disponible en: http://www.desdeeltercerpiso.com/2009/04/jorge-mufarech-amenaza-asesor-parlamentario-por-caso-rospigliosi/

386 "Ciudadano fue sentenciado a tres años de prisión por un 'link' que publicó en su blog", *El Comercio*, 29 de octubre del 2010, disponible en: http://elcomercio.pe/lima/sucesos/ciudadano-fue-sentenciado-tres-anos-prision-link-que-publico-su-blog-noticia-661206

387 Art. 132, Código Penal de Perú, disponible en: http://www.cejamericas.org/index.php/biblioteca/biblioteca-virtual/doc_view/3435-c%C3%B3digo-penal-del-per%C3%BA.html

388 *Ibíd.*

389 Juzgado Penal 33, Sentencia, Expediente 24304, 29 de octubre de 2010, disponible en: http://e.peru21.pe/102/doc/0/0/2/3/7/237981.pdf

opiniones sobre asuntos de interés público y sobre funcionarios públicos en tanto este tipo de discurso goza de una mayor protección bajo la Convención Americana de Derechos Humanos[390].

Finalmente, la decisión contra Godoy fue apelada y, en 2012, se absolvió al bloguero, decisión que fue confirmada por la Corte Superior de Justicia de Lima[391]. El tribunal consideró que la demanda presentada por el ex ministro Jorge Mufarech contra el periodista por el delito contra el honor "difamación agravada" era "infundada e incoherente"[392].

Colombia. Caso Gonzalo Hernán López: 18 meses de cárcel y multa por comentar en la versión digital de un diario - Injuria agravada

El 6 de noviembre de 2008, Gonzalo Hernán López, bajo un seudónimo, escribió en la sección de comentarios del diario *El País* de Cali: "Y con semejante rata como Escalante que hasta del Club Colombia y Comfenalco la han echado por malos manejos que se puede esperar… ¿El ladrón descubriendo ladrones? ¡Bah!"[393].

El comentario era en referencia al artículo "Siguen capturas por cartel de becas en Emcali" y López se refería a Gloria Lucía Escalante, ex gerenta Administrativa y de Recursos Humanos de la prestadora de servicios públicos local Empresa Municipales de Cali (EMCALI).

La funcionaria demandó por injuria al comentarista. En primera instancia, el juzgado décimo penal municipal absolvió a López indicando que la fiscalía no había sido exitosa identificándolo como autor del comentario. En apelación, el Tribunal

390 Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. OEA/Ser.L/V/II. Diciembre de 2009.

391 Corte Superior de Justicia de Lima, Sexta Sala Penal para Procesos con Reos Libres, Resolución 0071, 31 de enero de 2013, disponible en: https://es.scribd.com/doc/134562556/Sentencia-Segunda-Instancia-Caso-Mufarech#scribdhttp://diario16.pe/noticia/13319-anulan-sentencia-contra-blogger-josae-alejandro-godoy

392 Reporteros sin Fronteras, "Perú. La despenalización de los delitos de prensa continúa siendo un gran reto en 2012", 5 de enero de 2012, disponible en: http://www.rsf-es.org/news/peru-la-despenalizacion-de-los-delitos-de-prensa-continua-siendo-un-gran-reto-en-2012/

393 "Año y medio de cárcel por comentar en Internet", *Semana*, 21 de julio de 2014, disponible en: http://www.semana.com/nacion/articulo/ano-medio-de-carcel-por-comentar-en-internet/396477-3 y Herrera, Juan Sebastián Jiménez, "¿Contra la libertad de expresión?", *El Espectador*, 20 julio de 2014, disponible en: http://www.elespectador.com/noticias/judicial/contra-libertad-de-expresion-articulo-505601

Superior de Cali revocó la absolución condenando al comentarista por el delito de injuria agravada, a un año y medio de cárcel y a pagar un multa de 9,5 millones de pesos colombianos[394].

La condena quedó firme luego de que la Corte Suprema de Justicia se negó a revisar un recurso contra esa decisión[395]. Como señalaba el investigador Carlos Cortés Castillo en su análisis del fallo, la Corte Suprema colombiana no analizó en detalle el argumento de agravación punitiva que ponía en cuestión la defensa. (La defensa señalaba que el hecho de que el comentario hubiera sido realizado en un medio de divulgación masiva, no significaba que se estuviera haciendo una divulgación masiva o colectiva)[396].

El Código Penal colombiano señala en su título dedicado a los "delitos contra la integridad moral" que "el que haga a otra persona imputaciones deshonrosas" incurrirá en el delito de injuria y le corresponderá "prisión de dieciséis (16) a cincuenta y cuatro (54) meses y multa de trece punto treinta y tres (13.33) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes"[397]. En su artículo 223, la normativa penal establece que cuando alguna de estas conductas "se cometiere utilizando cualquier medio de comunicación social u otro de divulgación colectiva o en una reunión pública, las penas respectivas se aumentarán de una sexta parte a la mitad".
En noviembre de 2015, la Fundación para la Libertad de Prensa (FLIP) presentó una solicitud ante la Comisión Interamericana de Derechos Humanos para que se tomen medidas para prevenir que López Durán cumpla su condena de prisión y para que se admita este caso y se condene al Estado colombiano por vulnerar los derechos humanos del comentarista.
Según la FLIP,

394 Botero, Carolina, "18 meses de prisión por opinar en Internet", *Digital Rights LAC,* 29 de agosto de 2014, disponible en: http://www.digitalrightslac.net/es/18-meses-de-prision-por-opinar-en-internet/

395 Corte Suprema de Justicia de la República de Colombia, Sala de Casación Penal, 25 de junio de 2014, disponible en: http://es.scribd.com/doc/234654977/Sentencia-Gonzalo-Hernan-Lopez#scribd

396 Cortés Castillo, Carlos, "Cárcel para un comentarista ofensivo: revisando las paredes de los baños públicos", 21 de julio de 2014, disponible en: http://carloscortes.co/blog/2014/7/21/crcel-para-un-comentarista-ofensivorevisando-las-paredes-de-los-baos-pblicos

397 Art. 220, Código penal colombiano, disponible en:http://www.cepal.org/oig/doc/LeyesSobreAborto/Colombia/2000_C%C3%B3digopenal_Colombia.pdf

> El caso de López Durán es relevante porque se desconocieron los estándares nacionales e internacionales que se han fijado para el ejercicio de la libertad de expresión. En primer lugar, la condena penal es una sanción desproporcionada contra una persona que, además, se refirió a asuntos que son de interés público. Segundo, su comentario se encuentra en el marco del derecho a la libertad de opinión, la cual solo puede ser limitada en casos excepcionales. Tercero, se sancionó una expresión que, aunque ofensiva, tiene poca capacidad de daño al ser solamente un comentario dentro de una nota periodística. Finalmente, se trata de un caso en el que el Estado desconoció que el uso de entornos digitales debe interpretarse a la luz de la primacía de la libertad de expresión, sobre todo cuando se hablan temas de interés general[398].

Si bien en estos casos no se hace alusión expresa a internet, se observa que se han utilizado para castigar y perseguir expresiones difundidas en línea. Además, por las características propias de internet y su masividad, quedaría incluida en aquellos medios que faciliten la divulgación, efectuando una restricción desproporcionada a la libertad de expresión en internet, condenada por los organismos internacionales de derechos humanos[399].

Proyectos de ley

Perú. Difamación agravada por la utilización de internet

En Perú se ha presentado un proyecto de ley[400] que propone modificar el artículo 132 del Código Penal para incluir, como forma agravada del delito de difamación, la utilización de internet, blogs y redes sociales. Según este proyecto, la difamación a través de Internet y cualquiera de sus plataformas debería considerarse más grave que la difamación[2401].

---

[398] Fundación para la Libertad de Prensa (FLIP), "Caso de Gonzalo López se presenta ante la CIDH", 20 de noviembre de 2015, disponible en: http://flip.org.co/es/content/caso-de-gonzalo-l%C3%B3pez-se-presenta-ante-la-cidh

[399] Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. 31 de diciembre de 2013. Párrafo 74.

[400] Proyecto de Ley No. 4833/2015-CR, disponible en: http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc03_2011.nsf/0/4f6aae8f28ab4ba705257ec70055588d/$FILE/PL0483320150918.pdf

[401] Borgioli, Martín, "Blogs y redes sociales otra vez amenazados por un proyecto de ley", *Hiperderecho*, 24 de septiembre de 2015, disponible

De ser aprobada la ley, el artículo 132 del Código Penal peruano quedaría redactado de la siguiente manera:

> **Artículo 132.—**El que, ante varias personas, reunidas o separadas, pero de manera que pueda difundirse la noticia, atribuye a una persona, un hecho, una cualidad o una conducta que pueda perjudicar su honor o reputación, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a ciento veinte días-multa.
>
> Si la difamación se refiere al hecho previsto en el artículo 131, la pena será privativa de libertad no menor de uno ni mayor de dos años y con noventa a ciento veinte días-multa.
>
> Si el delito se comete por medio del libro, **el internet o medios virtuales vía blog y/o páginas sociales**, la prensa, u otro medio de comunicación social, la pena será privativa de libertad no menor de uno ni mayor de tres años y de ciento veinte a trescientos días-multa. (El subrayado es nuestro y es lo modificado a través de esta reforma).

Con esta modificación se estarían imponiendo sanciones más severas porque estas ofensas se hayan cometido en línea, cuestión que, como se ha desarrollado previamente en este informe, iría contra el presupuesto del Sistema Interamericano de que las expresiones difundidas a través de internet deben estar protegidas por el derecho a la libertad de expresión.

Al respecto se ha pronunciado la Relatoría Especial para la Libertad de Expresión en el informe "Libertad de expresión e Internet"[402], en el que deja en claro que"(…)no sería aceptable una ley que penalice, específicamente, los delitos contra el honor en línea e imponga penas más rigurosas que para los perpetrados en el mundo offline"[4].

Una iniciativa legislativa como ésta significaría, en términos de la relatoría, una restricción desproporcionada para la expresión en internet, en tanto lo consideraría más riesgoso que otros medios. Este tipo de iniciativas, como indica la relatoría, puede tener el efecto de restringir a Internet como un espacio para el libre intercambio de ideas[403].

---

en:http://www.hiperderecho.org/2015/09/blogs-y-redes-sociales-otra-vez-amenazados-por-proyecto-de-ley/

402 Article 19, *supra* nota 19.

403 Organización de los Estados Americanos, Informe de la Relatoría Especial para la Libertad de Expresión. Libertad de expresión e Internet. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. 31 de diciembre de 2013. Párrafo 74.

Argentina. Proyecto de ley contra la discriminación

En Argentina se presentó recientemente un proyecto de ley[404] que tiene como objetivo actualizar la ley contra actos discriminatorios vigente[405]. Si bien las intenciones del proyecto de garantizar la diversidad y promover la no discriminación son sumamente loables, el texto del proyecto es problemático porque establece una definición amplia de "acto discriminatorio":

> Las acciones y/u omisiones, de autoridades públicas o de particulares, que, de manera arbitraria, tengan como finalidad o resultado impedir… el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos y garantías fundamentales reconocidos por la Constitución Nacional, … motivadas en la falsa noción de raza, así como en las nociones de etnia, nacionalidad, lengua, idioma o variedad lingüística, religión o creencia, ideología, opinión política o gremial, sexo, orientación sexual, género, identidad de género y/o su expresión, edad, color de piel, estado civil, situación familiar, filiación, embarazo, discapacidad, responsabilidad familiar, antecedentes o situación penales, trabajo u ocupación, lugar de residencia, caracteres físicos, características genéticas, capacidad psicofísica y condiciones de salud, posición económica o condición social, hábitos personales **o cualquier circunstancia que implique distinción, exclusión, restricción o preferencia.**…. **Esta enunciación no es taxativa y pueden incluirse otros motivos**, especialmente cuando reflejen la experiencia de grupos sociales histórica o actualmente vulnerados"[406]. (El resaltado es nuestro).

Una definición tan amplia y abierta a interpretaciones no se ajusta a los requisitos del test tripartito desarrollado por el Sistema Interamericano. Como señaló en una nota de opinión, Eduardo Bertoni, director del CELE, "El principal problema es que la vaguedad en las definiciones puede llevar a interpretaciones judiciales que restrinjan la libertad de expresión y otorguen facultades discrecionales a las

---

404 Dictamen, Ley nacional contra la discriminación, disponible en: http://www.vialibre.org.ar/wp-content/uploads/2015/07/DICTAMEN-ACTOS-DISCRIMINATORIOS-Final.pdf

405 Ley 23.592 de actos discriminatorios, 23 de agosto de 1988, disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/20000-24999/20465/texact.htm

406 Artículo 5 del proyecto. Disponible en http://www.vialibre.org.ar/wp-content/uploads/2015/07/DICTAMEN-ACTOS-DISCRIMINATORIOS-Final.pdf

autoridades de manera inadmisible para la Convención Americana de Derechos Humanos"[407].

El proyecto contempla la no discriminación en internet, e impone a los intermediarios la obligación de publicar en sus plataformas los estándares de no discriminación establecidos en el proyecto, y la obligación de contar con un procedimiento para que los usuarios puedan denunciar actos discriminatorios en la web y pedir su remoción[408].

Además, el proyecto prevé elevar las penas de todos los delitos del Código Penal cuando éstos sean cometidos:

> "(…) por persecución u odio bajo pretexto de la falsa noción de raza, o de las nociones de etnia, nacionalidad, lengua, idioma o variedad lingüística, religión o creencia, ideología, opinión política o gremial, sexo, orientación sexual, género, identidad de género y/o su expresión, edad, color de piel, estado civil, situación familiar, filiación, embarazo, discapacidad, responsabilidad familiar, antecedentes o situación penales, trabajo u ocupación, lugar de residencia, caracteres físicos, características genéticas, capacidad psicofísica y condiciones de salud, posición económica o condición social y/o hábitos personales"[409].

Si bien los estándares interamericanos permiten la aplicación de responsabilidades ulteriores, es necesario que se cumplan los requisitos del test tripartito, entre ellos la proporcionalidad. En el caso, la aplicación de normativa penal para criminalizar expresiones parece desproporcionada e innecesaria, dado que puede pensarse en opciones menos restrictivas para perseguir el objetivo de combatir la discriminación[410].

---

[407] Bertoni, Eduardo, "Censura disfrazada de antidiscriminación", *Infobae*, 22 de julio de 2015, disponible en: http://opinion.infobae.com/eduardo-bertoni/2015/07/22/censura-disfrazada-de-antidiscriminacion/

[408] Artículo 21 del proyecto. Disponible en http://www.vialibre.org.ar/wp-content/uploads/2015/07/DICTAMEN-ACTOS-DISCRIMINATORIOS-Final.pdf

[409] Artículo 22 del proyecto. Disponible en http://www.vialibre.org.ar/wp-content/uploads/2015/07/DICTAMEN-ACTOS-DISCRIMINATORIOS-Final.pdf

[410] Ver análisis de Fundación Vía Libre sobre el proyecto, disponible en: http://www.vialibre.org.ar/wp-content/uploads/2015/07/discriminacion.pdf ; ver análisis de la Asociación por los Derechos Civiles al proyecto, disponible en: http://www.adc.org.ar/regular-comentarios-en-internet-el-proyecto-de-ley-anti-discriminacion-es-inconstitucional/ ; ver Crettaz, José, "Avanza un proyecto de ley contra los comentarios en Internet", *La Nación*, 19 de julio de 2015, disponible en: http://www.lanacion.com.ar/1811680-avanza-un-proyecto-de-ley-contra-los-comentarios-en-internet

Otras observaciones

Resultan especialmente preocupantes algunas declaraciones de funcionarios públicos respecto de la libertad para expresarse en internet y redes sociales. En muchos países de la región, se han expresado intenciones de desarrollar normativa para criminalizar contenidos difundidos por internet y, si bien no han llevado adelante esas intenciones, es particularmente alarmante que funcionarios públicos se expresen contra la difusión de ideas, opiniones y expresiones en internet y las redes sociales.

A continuación, se transcriben algunas declaraciones:

- "Yo no voy a permitir esos insultos compañeros, voy a actuar con la ley en la mano y cuando deje de ser Presidente actuaré como ciudadano. Yo creo que ninguno de ustedes va aceptar uno de esos insultos, y esto que sea debate en las próximas elecciones, porque aquí por hacerle daño al Gobierno nos han hecho creer que aguantar esos insultos es libertad de expresión"[411]. Esto dijo el presidente de Ecuador, Rafael Correa, en su enlace ciudadano, a raíz de un tuit en el que se lo había mencionado.
- El 22 de agosto de 2012, el presidente Correa pidió a la Secretaría de Inteligencia de Ecuador que se investigue al autor de ese mensaje y se "proceda judicialmente". El mensaje en cuestión decía: "@MashiRafael el inmoral es ud! Ya quiere adueñarse de la asamblea! Ladrón mitómano".
- Antes, el 24 de noviembre de 2011, Javier Genovez Solano fue detenido acusado de amenazar a Correa a través de Twitter. Las investigaciones contra Genovez Solano también se iniciaron a partir de una denuncia hecha por el presidente durante su enlace sabatino. Genovez fue liberado al día siguiente después de haber admitido haber sido el autor de mensajes como "Ave Mashi Rafael los que te vamos a matar te saludamos".
- En ese mismo país, en el marco de las discusiones en torno a lo que fue el nuevo Código Integral Penal aprobado 2013, el secretario jurídico de la Presidencia, Alexis Mera, propuso que las injurias y calumnias que se vierten en redes sociales sean penalizadas[412]."Yo he propuesto que se regulen todo

[411] Fundamedios, "Presidente de la República pide a Secretaría de inteligencia investigar a tuitero y proceder judicialmente", 22 de agosto de 2012, disponible en: http://www.fundamedios.org/alertas/presidente-de-la-republica-pide-secretaria-de-inteligencia-investigar-tuitero-y-proceder-judicialmente/

[412] "Gobierno ecuatoriano pide que se penalice la opinión en redes sociales", IFEX, 3 de septiembre 2013, disponible en: http://www.ifex.org/ecuador/2013/09/03/penalice_opinion/es/ y

lo que sean procesos de calumnia en las redes sociales **porque estas redes no puede ser un instrumento de impunidad.** He pedido a la Mesa de Justicia que se haga un procedimiento especial cuando hay injurias en Twitter o en Facebook porque ahora una injuria de una persona que tiene unos 10.000 seguidores puede ser más rápida y hacer más daño", dijo Mera, en su momento[413]. (El resaltado es nuestro). Esta iniciativa no prosperó.

- "Esto, hoy, puede afectar a un político, un empresario; mañana a un periodista y en consecuencia a toda una familia. En fin, considero que todos estamos expuestos a estas cuestiones", señaló el diputado paraguayo, Oscar Tuma, cuando propuso penalizar a quienes insulten a través de redes sociales en ese país[414]. "El legislador considera importante reglamentar la utilización de la tecnología, **con especial énfasis en las plataformas de comunicación social de internet, teniendo en cuenta la mala utilización que le dan muchas personas**" (el resaltado es nuestro), señalaba, por ese entonces, la página oficial de la cámara de Diputados paraguaya[415].

- Emir Sader, reconocido cientista político brasileño, publicó en 2007 un artículo de opinión en la web *Carta Maior* argumentando que un ex senador (Jorge Bornhausen) era racista, por declaraciones que éste había realizado. El legislador inició una causa contra Sader por injurias y un tribunal de San Pablo falló en contra de Sader. El tribunal entendió que la posición e influencia de Sader como profesor universitario e intelectual merecía que su pena sea agravada[416].

- El vicepresidente boliviano, Álvaro García Linera, dijo durante un acto que revisa personalmente las redes sociales y anota "con nombre y apellido a los que realizan insultos" contra el presidente Evo Morales. "Aquí está en el

---

413 Ura, Alexa, "Gobierno ecuatoriano propone penalizar la difamación en las redes sociales", Knight Center, disponible en: https://knightcenter.utexas.edu/es/blog/00-14443-gobierno-ecuatoriano-propone-penalizar-la-difamacion-en-las-redes-sociales

414 "Tuma pretende penalizar a quienes insultan en redes", *Última Hora*, 23 de mayo de 2014, disponible en: http://www.ultimahora.com/tuma-pretende-penalizar-quienes-insultan-redes-n797343.html

415 "Tuma pretende penalizar a quienes insultan en redes", 26 de mayo de 2014, disponible en: http://www.mediatelecom.com.mx/index.php/telecomunicaciones/regulacion/item/66115-tuma-pretende-penalizar-a-quienes-insultan-en-redes

416 Gomes, Marcel, "Emir Sader é condenado em processo movido por Bornhausen; cabe recurso", *Carta Maior*, 1 de noviembre de 2006, http://www.cartamaior.com.br/?/Editoria/Politica/Emir-Sader-e-condenado-em-processo-movido-por-Bornhausen-cabe-recurso/4/11971

(teléfono) celular, yo siempre estoy entrando al Internet y voy anotando con nombre y apellido" a quienes insultan al presidente "en Facebook, en Internet", dijo García Linera en esa ocasión. Después de estas declaraciones, el jefe de la bancada del Movimiento al Socialismo (MAS) —el partido que gobierna Bolivia— en diputados, anunció que su partido contemplaba una regulación en la materia y que las personas que insultan al presidente "deberían ser procesadas por discriminación"[417].

- "Este tema de las redes sociales hay que regularlo (…) La conducta del hombre en sociedad tiene que ser regulada", señaló la fiscal general de Venezuela en marzo de este año[418] luego de que circularan rumores en las redes sociales sobre supuestos raptos de menores.

- Su par del estado mexicano de Tabasco, la Procuradora General de Justicia, instó en 2014 a que "se castigue y, sobre todo, se prevenga[n]" la difusión de "mensajes de alarma" a través de las redes sociales[419]. En ese estado, un tiempo antes, se había aprobado una ley que penalizaba con hasta dos años de prisión para aquel que cause alarma o "caos social" a través de cualquier medio de comunicación[420].

Conclusiones

El Sistema Interamericano de Derechos Humanos otorga un lugar primordial al derecho a la libertad de expresión, y establece requisitos muy estrictos a cualquier

417 "Bolivia: oficialismo impulsa proyecto para regular redes sociales", *Ámbito*, 22 de octubre de 2012, disponible en: http://www.ambito.com/noticia.asp?id=659646

418 "La fiscal general de Venezuela: 'Hay que regular las redes sociales'", *ABC.es*, 28 de marzo de 2015, disponible en: http://www.abc.es/internacional/20150328/abci-venezuela-regular-redes-sociales-201503271355.html; IPYS, "Internet: Fiscal de la República considera necesaria la regulación del uso de las redes sociales", 27 marzo de 2015, disponible en: http://ipys.org.ve/alerta/internet-fiscal-de-la-republica-considera-necesaria-la-regulacion-del-uso-de-las-redes-sociales/

419 "Redes sociales se regulan en Tabasco", *Mexican Business Web*, disponible en: http://www.mexicanbusinessweb.mx/negocios-rentables-en-mexico/oportunidades-de-negocio-en-tabasco/redes-sociales-se-regulan-en-tabasco/ y Espinosa, Víctor Adrián, "Tabasco monitorea redes para combatir 'alarma social'", *24 horas,* disponible en: http://www.24-horas.mx/pgj-de-tabasco-persigue-alarma-social-en-twitter/

420 "Modificaciones a Código Penal de Tabasco, atentan contra la libertad de expresión", *Animal Político*, 1 de septiembre de 2011, disponible en: http://www.animalpolitico.com/2011/09/aprueban-ley-contra-el-%E2%80%9Crumor%E2%80%9D-en-tabasco/

limitación de ese derecho. Además, de acuerdo con los estándares internacionales de derechos humanos, la protección de la libertad de expresión debe extenderse también a aquellas expresiones difundidas por internet. Esto significa que no podría aceptarse la criminalización o el agravamiento de penas en casos de discursos simplemente por haber sido difundidos a través de internet. No obstante, en América Latina se observa una incipiente tendencia a criminalizar discurso crítico difundido a través de internet.

El objetivo de este informe ha sido identificar algunos casos concretos que puedan dar cuenta de dichas tendencias por parte de los Estados de criminalizar discurso crítico vertido en línea.

Si bien son escasas las normas que penalizan específicamente aquellos discursos difundidos a través de internet, observamos que una práctica común por parte de algunos Estados es la de utilizar tipos penales tradicionales para perseguir discurso online. Algunas figuras utilizadas son los tradicionales delitos contra el honor, terrorismo, figuras de incitación al pánico o desestabilización, delitos financieros, criminalización de actos discriminatorios, entre otros.

Otros casos revelan el agravamiento de penas según el tipo de medio utilizado para difundir las expresiones, por ejemplo cuando el medio utilizado para difundir las expresiones permita el alcance masivo. Por las características de internet, ésta siempre estará incluida en el tipo de medios que permiten un alcance masivo de la información.

Por último, consideramos preocupantes las intenciones que han expresado diversos funcionarios públicos de desarrollar normativa para criminalizar contenidos difundidos por internet ya que, si bien no han llevado adelante esas intenciones, es particularmente alarmante que funcionarios públicos se expresen contra la difusión de ideas, opiniones y expresiones en internet y las redes sociales.

Libertad de expresión y responsabilidad de los intermediarios en Internet (Asociación por los Derechos Civiles)[421]

R. Eduardo Ferreyra[422]

1. Introducción:

Internet ha sido considerado desde sus inicios como un medio apropiado para que miles de personas alrededor del mundo ejerzan los diversos derechos consagrados en los instrumentos internacionales de derechos humanos. En particular, Internet cumple una función valiosa en la difusión de ideas, opiniones y creencias de las personas. Asimismo, también sirve como un medio que permite la difusión de información hacia personas de todos los países, quienes ven facilitadas el acceso a materiales que, de otro modo, serían imposibles de ubicar. Por lo tanto, podemos decir que Internet es clave para el ejercicio de la libertad de expresión tal como la conocemos en la actualidad

Esta situación fue reconocida en 2011 por la Relatoría Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión, quien junto a sus pares de África, América y Europa, emitió la Declaración Conjunta Sobre Libertad De Expresión e Internet[423], en la cual se reconoció que la libertad de expresión se aplica a Internet del mismo modo que al resto de los medios de comunicación

La declaración fue el punto de partida para el desarrollo de prácticas y principios normativos en el ámbito internacional, que buscan establecer estándares democráticos para las regulaciones jurídicas relativas a Internet y la libertad de expresión. El objetivo es lograr que los gobiernos implementen legislación que favorezca el ejercicio de los derechos humanos en el ámbito

[421] Organización no gubernamental, apartidaria y sin fines de lucro con sede en Argentina, dedicada a la defensa de los derechos humanos y la promoción de una cultura democrática. En los últimos años el desarrollo exponencial de las Tecnologías de la Información y la Comunicación (TICs) nos presentó un nuevo desafío y, en consecuencia, ADC expandió fuertemente su agenda en materia de libertad de expresión en el mundo digital, privacidad y acceso a la información, convirtiéndose en un referente nacional y regional. http://www.adc.org.ar/

[422] Abogado egresado de la Universidad Nacional de Tucumán. Posee una Maestría en Filosofía del Derecho en la Universidad de Buenos Aires. Actualmente cursa la Maestría en Derechos Humanos y Democratización en la Universidad de San Martín. Es investigador de ADC en las áreas de Libertad de Expresión y Privacidad.

[423] Disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849

digital.

Dentro de las múltiples aristas que puede adquirir la relación entre Internet y libertad de expresión, la cuestión del marco jurídico a aplicar a los intermediarios adquiere especial relevancia. Los llamados intermediarios de Internet son el nexo entre la persona que produce la información o la opinión, y la persona que la recibe. Gracias a su trabajo, los individuos pueden acceder a un sinnúmero de materiales e ideas suministrados por personas que se valen de los diversos servicios que éstos intermediarios ofrecen.

El problema surge cuando el contenido de lo transmitido afecta derechos de terceros. En muchas ocasiones, lo que se difunde en Internet afecta el honor o la privacidad de los individuos. Otras veces, lo que se divulga viola derechos de propiedad intelectual de los autores. Asimismo, existen opiniones que pueden resultar ofensivas y discriminatorias para determinados grupos sociales. En situaciones como estas, se debe determinar si se debe imponer responsabilidad a los intermediarios por la difusión que llevan a cabo de contenido lesivo generado por terceros.

Este es un asunto que debe ser examinado de manera muy cuidadosa, puesto que una regulación inadecuada podría causar el indeseable efecto de generar instancias de censura en Internet. Una buena regulación debe contemplar algún medio para resguardar a las víctimas de contenidos lesivos difundidos en la web. Sin embargo, no debe perderse de vista que el objetivo que debe orientar toda decisión en la materia es el de robustecer la garantía de la libertad de expresión, ya que ésta "es una piedra angular en la existencia misma de una sociedad democrática"[424]

En el ámbito regional, las pautas vigentes se sustentan principalmente en el Informe 2013 de la Relatoría Especial para la Libertad de Expresión (RELE)[425] que incluye una sistematización de estándares jurídicos destinados a promover el respeto de la libertad de expresión en Internet. Asimismo, utilizaremos también como referencia los Principios de Manila de 2015[426], que reflejan el creciente consenso global en la adopción de buenas prácticas a tener en cuenta al momento de regular sobre la responsabilidad de los intermediarios en Internet

En base a estos elementos, analizaremos en el presente informe la legislación y jurisprudencia de los países latinoamericanos referida a responsabilidad de los intermediarios de internet, para determinar si se ajustan a

[424] CIDH, La Colegiación Obligatoria de Periodistas, Opinión Consultiva OC-5/85 Serie A, No. 5, párr. 70 disponible en www.oas.org/es/cidh/expresion/showDocument.asp?DocumentID=26

[425] Informe Relatoría Especial Para La Libertad De Expresión De La Comisión Interamericana de Derechos Humanos "Libertad de Expresión e Internet" 2013 disponible en http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf

[426] Disponible en www.manilaprinciples.org/es

aquellos parámetros,creados por la necesidad de proteger la libertad de expresión y el carácter democrático de nuestras sociedades.

Este capítulo se desarrollará de la siguiente manera. En primer lugar, se hará una reseña de los estándares protectorios establecidos por la RELE –a través de su Informe 2013- , más las sugerencias aportadas por los Principios de Manila.

Luego, dedicaremos dos capítulos a analizar las legislaciones vigentes en la región y su correspondencia con dichos estándares, y también los principales proyectos de ley relacionados a responsabilidad de intermediarios.

Seguiremos con una reseña y análisis de casos jurisprudenciales emblemáticos, que incluirá también un apartado dedicado a la detección de prácticas tribunalicias novedosas de impacto en la atribución de responsabilidad de intermediarios de internet.

Finalmente, llegaremos a las conclusiones y recomendaciones finales.

2. Estándares internacionales:

La ya mencionada Declaración Conjunta Sobre Libertad De Expresión e Internet dedica su segundo apartado a establecer pautas para la adopción de reglas referidas a los intermediarios de Internet. El documento establece en primer lugar el principio de mera transmisión, por el cual, "ninguna persona que ofrezca únicamente servicios técnicos de Internet como acceso, búsquedas o conservación de información en la memoria caché deberá ser responsable por contenidos generados por terceros y que se difundan a través de estos servicios". Las únicas excepciones que la Declaración contempla a este principio son: cuando el proveedor del servicio haya intervenido específicamente en el contenido o se niegue a cumplir una orden judicial que exija su eliminación cuando esté en condiciones de hacerlo.

Por otra parte, el instrumento establece que los intermediarios no deberían tener la obligación de controlar el contenido generado por los usuarios ni deberían estar sujetos a normas extrajudiciales sobre cancelación de contenidos que no ofrezcan suficiente protección para la libertad de expresión. Como ejemplo de lo último, la propia Declaración menciona el sistema de "notice and takedown"[427]

Siguiendo las pautas de la Declaración, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) profundizó en el dictado de estándares relativos a los intermediarios, en el Capítulo IV del Informe 2013, llamado "Libertad de Expresión e Internet"[428] . Allí, se interpretó que el principio de mera transmisión implica "la exclusión de un modelo de responsabilidad objetiva conforme al cual los intermediarios resulten

[427] Sistema por el cual basta una notificación privada de la parte supuestamente afectada, para que el intermediario tenga la obligación de remover el contenido.
[428] Ver cita 3

responsables por contenidos ilegítimos generados por terceros". La arquitectura de la red vuelve imposible que los intermediarios puedan ejercer un control de los contenidos subidos a la web y por ende, no tienen el control sobre el factor de riesgo que se requiere para este tipo de responsabilidad. De esta manera, la CIDH también afirmó que los intermediarios "no deben estar sujetos a obligaciones de supervisión de los contenidos generados por los usuarios con el fin de detener y filtrar expresiones ilícitas"

El riesgo que un modelo de responsabilidad objetiva implica para la libertad de expresión también es contemplado en el documento. El informe deja en claro que un sistema objetivo implicaría "un fuerte incentivo para la censura privada de un rango amplio de expresiones legítimas". Dado que el control de legitimidad quedaría a cargo de los intermediarios, se corre el riesgo de que, al no poseer el conocimiento jurídico suficiente para discernir cuándo un contenido es violatorio de algún derecho, aquellos terminen eliminando cualquier expresión dudosa, frente al temor de sufrir eventualmente algún tipo de responsabilidad. Por último, se deja en claro que "en la mayoría de los casos, los intermediarios no tienen – ni tienen que tener – la capacidad operativa/técnica para revisar los contenidos de los cuales no son responsables".

Luego de rechazar el sistema objetivo, la CIDH estableció los estándares que deben guiar la adopción de modelos de responsabilidad subjetiva, llamados de "puerto seguro". En estos sistemas, el intermediario puede exonerarse de responsabilidad si demuestra que removió el contenido respecto de los cuales un tercero afirma su ilicitud. La Relatoría sostuvo que estos esquemas de "inmunidad condicionada" son compatibles con la Convención "*en la medida en que establezcan garantías suficientes para la protección de la libertad de expresión y el debido proceso de los usuarios, y no impongan obligaciones difusas o desproporcionadas a los intermediarios*"

En ese sentido, se rechaza la adopción del sistema de "notice and takedown", en el cual la comunicación de la ilicitud del contenido es realizada por un particular. Al igual que el modelo objetivo, este procedimiento genera mecanismos de censura privada, ya que según el informe, también "pone a los intermediarios privados en posición de tener que tomar decisiones sobre la licitud o ilicitud de los contenidos". Asimismo, crea incentivos para que proliferen en forma desproporcional los pedidos de remoción de contenidos, con evidente perjuicio para la libertad de expresión.

Por lo tanto, la Relatoría estableció que la exigencia de remoción solamente debería proceder "cuando sea ordenada por una *autoridad judicial o de naturaleza similar*, que opere con suficientes garantías de independencia, autonomía e imparcialidad y que tenga la capacidad para evaluar los derechos en juego y ofrecer las garantías necesarias al usuario". Por otro lado, afirmó que la notificación debe cumplir ciertos requisitos para su eficacia: en primer lugar, debe establecer con precisión qué contenidos deben ser removidos. En segundo lugar,

la determinación previa de la ilicitud del contenido debe cumplir con las reglas del debido proceso judicial. Por otra parte, se establecen obligaciones de transparencia y acceso a un recurso efectivo, con el objetivo de inhibir abusos en la utilización de este tipo de medidas.

Además del sistema de "notificación judicial", la Relatoría aceptó mecanismos de "notificación y notificación", por medio de los cuales los intermediarios poseen la obligación de transmitir al usuario notificaciones sobre la supuesta ilicitud de determinada expresión. Para que sea efectiva, el Informe sostiene que la notificación debe brindar detalles acerca de "la ubicación del material que se considera ilícito, el fundamento jurídico de la ilicitud, y una adecuada opción de contra-notificación a cargo del usuario productor del contenido con garantías de control judicial". Por último, se deja en claro que los usuarios deben tener derecho a permanecer bajo anonimato y cualquier disputa sobre este punto debe ser resuelta exclusivamente en sede judicial.

Además de los instrumentos internacionales, existe una guía de buenas prácticas elaborada por sectores de la sociedad civil conocida como "Principios de Manila". El 24 de marzo de 2015 se realizó la Convención Rights Con en Manila, capital de Filipinas. Allí, una coalición internacional de organizaciones de la sociedad civil presentó una serie de principios cuyo objetivo es servir de guía para la adopción de leyes sobre responsabilidad de intermediarios que cumplan con los estándares internacionales de derechos humanos. El marco de referencia está compuesto por los siguientes principios:

1- Los intermediarios deberían estar protegidos por ley de la responsabilidad por contenido de terceros.
2- No debe requerirse la restricción de contenidos sin una orden emitida por autoridad competente.
3- Las solicitudes de restricción de contenido deben ser claras, inequívocas y respetar el debido proceso.
4- Las leyes, órdenes y prácticas de restricción de contenidos deben cumplir con los test de necesidad y proporcionalidad.
5- Las leyes, políticas y prácticas de restricción de contenidos deben respetar el debido proceso.
6- La transparencia y la rendición de cuentas deben ser incluidas dentro de la normativa, políticas y prácticas sobre restricción de contenido.

Con estos principios, se busca establecer un piso mínimo de garantías y buenas prácticas, que ayude a que las políticas gubernamentales relativas a la responsabilidad de los intermediarios protejan a las personas frente a conductas del sector público y privado que puedan dar lugar a violaciones a la libertad de expresión u otro derecho humano.

A continuación se analizara la realidad jurídica latinoamericana para determinar el grado de adecuación con respecto a los estándares internacionales recién descriptos.

3. Legislación en América Latina:

Nuestro continente no posee una normativa abundante en la materia. La mayoría de los países no dispone todavía de legislación específica sobre responsabilidad de los intermediarios. A pesar de ello, existen unas cuantas naciones que se han encargado de regular esta materia, ya sea en general o en aspectos particulares. En lo que sigue se analizará la normativa de aquellos países que ya poseen algún tipo de regulación jurídica.

a)-Chile:

La legislación chilena no contempla normas generales sobre responsabilidad de intermediarios en redes digitales por contenidos ilícitos o dañinos. No obstante, en materia de infracciones a derechos de autor y conexos, existe una clara delimitación legislativa de los deberes de los prestadores de servicios, producto del cumplimiento de tratados internacionales.

El 6 de Junio de 2003 Chile y EEUU firmaron un Tratado de Libre Comercio (TLC)[429], cuyo Capítulo Diecisiete establece deberes en materia de Propiedad Intelectual que las Partes deben cumplir. Entre ellas, se dispuso una serie de obligaciones a adoptar por los Estados firmantes en materia de limitación de la responsabilidad de los proveedores de servicios de Internet. Allí figura el compromiso de ambos Estados de adoptar "incentivos legales para que los proveedores de servicios cooperen con los titulares de derechos de autor para disuadir del almacenamiento y transmisión de datos no autorizados de materiales amparados por el derecho de autor" y "limitaciones en su legislación relativas al alcance de los recursos disponibles contra los proveedores de servicio por infracciones a los derechos de autor…" (Cap.17, 23 (a) (II)) Esta normativa generó grave preocupación, ya que se la consideró como un intento de EEUU de imponer el modelo de "notice and takedown" a los países con los que firmase tratados de libre comercio. El sistema de notificación extrajudicial para casos de violaciones a los derechos de autor está vigente en el país norteamericano desde la sanción de la Digital Millennium Copyright Act (DMCA) en 1998 y ha sido considerado como un modelo que no brinda suficientes garantías de respeto a la libertad de expresión.

En cumplimiento de dicha obligación, el 13 de Enero de 2010 fue aprobada en el Congreso chileno la Ley 20.435 de Reforma a la Ley de Propiedad Intelectual[430], la cual entró en vigencia el 4 de Mayo de aquel año. La nueva ley añade un nuevo Título III, cuyo Capítulo III establece el régimen de limitación de responsabilidad de los prestadores de servicio de Internet, en materia de derechos de autor.

A pesar de los temores suscitados, la ley chilena se apartó del modelo

[429] Disponible en http://www.direcon.gob.cl/wp-content/uploads/2010/12/Tratado-EE.UU-I-OPT2.pdf
[430] Disponible en http://www.leychile.cl/Navegar?idNorma=28933

norteamericano e instituyó un sistema que brinda protecciones amplias en materia de responsabilidad. En primer lugar, se dispone que los proveedores no podrán ser obligados a supervisar los datos que transmitan, almacenen o referencien ni deberán realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, salvo orden judicial de investigar alguna infracción al derecho de autor. En segundo lugar, se estableció el sistema de "puerto seguro", por el cual los intermediarios no van a ser responsabilizados por contenidos de terceros en la medida que cumplan con las condiciones impuestas por la normativa. (Art. 85 L).

Las condiciones a cumplir por los proveedores se dividen en generales y particulares. Las primeras deben ser cumplidas por todos los intermediarios -con excepción de los servicios de búsqueda, enlace o referencia-, y son las siguientes (Art. 85 O):

a) Haber establecido condiciones generales y públicas, bajo las cuales éste podrá hacer uso de la facultad de poner término a los contratos de los proveedores de contenido calificados judicialmente como infractores reincidentes de los derechos protegidos por esta ley. No interferir en las medidas tecnológicas de protección y de gestión de derechos de obras protegidas ampliamente reconocidas y utilizadas lícitamente, y

b) No haber generado, ni haber seleccionado el material o a sus destinatarios.

Además, existen condiciones específicas para cada uno de los tipos de servicios distinguidos por la ley:

1- **Servicios de transmisión de datos, enrutamiento o suministro de conexiones** (Art. 85 M): Para gozar de la limitación de responsabilidad los proveedores no deben:

a) Modificar o seleccionar el contenido de la transmisión (no se considerará modificación del contenido, la manipulación tecnológica del material necesaria para facilitar la transmisión a través de la red, como la división de paquetes).

b) Iniciar la transmisión, o

c) Seleccionar a los destinatarios de la información.

2- **Servicios que temporalmente almacenen datos mediante un proceso de almacenamiento automático** (Art. 85 N): Para gozar de la limitación de responsabilidad los proveedores deberán:

a) Respetar las condiciones de acceso de usuarios y las reglas relativas a la actualización del material almacenado establecidas por el proveedor del sitio de origen, salvo que dichas reglas sean usadas por éste para prevenir o dificultar injustificadamente el almacenamiento temporal a que se refiere este artículo.

b) No interferir con la tecnología compatible y estandarizada utilizada en el sitio de origen para obtener información sobre el uso en línea del material almacenado, cuando la utilización de dichas tecnologías se realice de conformidad con la ley y sean compatibles con estándares de la industria

ampliamente aceptados.

c) No modificar su contenido en la transmisión a otros usuarios, y

d) Retirar o inhabilitar en forma expedita el acceso a material almacenado que haya sido retirado o al que se haya inhabilitado el acceso en su sitio de origen, cuando reciba una notificación de conformidad con el procedimiento previsto en la ley.

3- **Servicios que almacenan datos en su red o sistema, o que efectúan servicios de búsqueda, vinculación y/o referencia a un sitio en línea mediante herramientas de búsqueda de información, incluidos los hipervínculos y directorios** (Art. 85 Ñ): Las condiciones que deben cumplir los proveedores para no ser responsabilizados son:

a) No tener conocimiento efectivo del carácter ilícito de los datos. Existe "conocimiento efectivo" allí donde haya una orden judicial, emanada de tribunal competente, que ordene el retiro del contenido o el bloqueo de su acceso.

b) No recibir un beneficio económico directamente atribuible a la actividad infractora, en los casos en que tenga el derecho y la capacidad para controlar dicha actividad.

c) Designar públicamente un representante para recibir las notificaciones judiciales.

d) Retirar o inhabilitar en forma expedita el acceso al material almacenado de acuerdo al procedimiento previsto (**notificación judicial**).

En cuanto a retiro de contenidos, la legislación chilena se apartó del sistema de "notice and takedown" y estableció un **modelo jurisdiccional** para poder dar de baja un contenido de la web. De esta manera, aquel que se considere afectado por una presunta violación a un derecho de autor debe recurrir a un órgano judicial para solicitar el retiro de los datos o el bloqueo del acceso a ellos. Los proveedores de servicios sólo podrán ser responsabilizados por almacenar material violatorio de los derechos de autor cuando hayan tenido un conocimiento efectivo -**vía notificación legal de la resolución judicial tomada al efecto**- y no hayan sido expeditos en retirar el material.

El procedimiento establece que aquel que se considere afectado, deberá presentar ante autoridad judicial una solicitud de baja de contenido, la cual debe indicar claramente:

a) Los derechos supuestamente infringidos, con indicación precisa de la titularidad de éstos y la modalidad de la infracción.

b) El material infractor.

c) La localización del material infractor en las redes o sistemas del prestador de servicios respectivos.

Si lo considera pertinente, el órgano judicial decretará sin demora el

retiro o bloqueo de los contenidos infractores. El proveedor del contenido dado de baja que considere afectado sus derechos podrá requerir al órgano que decretó la orden que deje sin efecto la medida de restricción de acceso o retiro de material mediante solicitud que deberá ser tramitada breve y sumariamente (Art. 85 Q).

En los casos que los proveedores de servicios hayan cumplido con las condiciones impuestas a ellos por la normativa, el órgano judicial sólo podrá:

a) Si se trata de las funciones de transmisión, enrutamiento o suministro, disponer la adopción de medidas razonables para bloquear el acceso a un determinado contenido infractor que sea claramente identificado por el solicitante y que no implique el bloqueo de otros contenidos legítimos.

b) Si se trata de las restantes funciones, disponer: 1) El retiro o inhabilitación del acceso al material infractor que sea claramente identificado por el solicitante; 2) La terminación de cuentas determinadas de infractores reincidentes de dicho prestador de servicio y cuyo titular esté usando el sistema o red para realizar una actividad infractora a los derechos de autor y conexos.

Tales medidas pueden ser decretadas prejudicialmente sin audiencia del afectado, habida caución por parte del solicitante y motivos graves fundantes.

La regulación chilena cumple en general con los estándares de derechos humanos, al consagrar la intervención de un tercero neutral y con conocimiento jurídico para la determinación del carácter ilícito del contenido cuestionado. Por otra parte, se deja en claro que la notificación deberá ser detallada y con clara indicación del contenido que se debe restringir. Además, se establece claramente que los intermediarios no tendrán la obligación de ejercer una vigilancia activa en la búsqueda de contenido ilícito en la web. Finalmente, el caso chileno demuestra que los países latinoamericanos firmantes de tratados de libre comercio con EEUU no están obligados a seguir el sistema de "notice and takedown".

Sin embargo, se debe destacar que el modelo jurisdiccional establecido en la legislación únicamente abarca casos de violaciones a derechos de propiedad intelectual. Chile todavía carece de normativa que pueda aplicarse a otros casos en los cuales también está en juego la responsabilidad de los intermediarios, como potenciales afectaciones al honor, la privacidad o la imagen, entre otros.

b) Costa Rica:

El caso costarricense presenta grandes similitudes al de Chile. El país centroamericano firmó –junto con el resto de los países centroamericanos, y República Dominicana- un Tratado de Libre de Comercio con EEUU en 2004[431],

[431] Disponible en http://transparenciafiscal.gob.do/documents/10184/5538703/Acuerdo+DR-CAFTA.pdf/7a598885-f3f1-4fd2-a010-eba4ed16e4b6

cuya entrada en vigencia, en el caso de Costa Rica, fue en Enero de 2009. El artículo 15.11.27 del Tratado estableció que cada Parte garantizará, de acuerdo a la estructura del Acuerdo:

(a) incentivos legales para que los proveedores de servicios colaboren con los titulares de derechos de autor en disuadir el almacenaje y transmisión no autorizada de materiales protegidos por derechos de autor; y

(b) limitaciones en su legislación relativas al alcance de los recursos disponibles contra los proveedores de servicios por infracciones a los derechos de autor que no estén en su control, ni hayan sido iniciados o dirigidos por ellos, y que ocurran a través de sistemas o redes controladas u operadas por ellos, o en su representación.

En virtud de esta obligación, el 18 de Octubre de 2011 se sancionó el Decreto Presidencial 36880[432], que establece el "*Reglamento sobre la limitación a la responsabilidad de los proveedores de servicios por infracciones a Derechos de Autor y Conexos de Acuerdo con el Artículo 15.11.27 del Tratado de Libre Comercio República Dominicana Centroamérica- Estados Unidos*".

Como el título lo confirma, el marco normativo establecido tiene por objeto únicamente las infracciones a los derechos de autor y conexos, y al igual que en Chile, adopta un sistema amplio de protección en materia de responsabilidad. El principio general está contemplado en el art. 4, donde se establece que "los proveedores de servicios no serán sujetos a reparaciones pecuniarias (…) frente a casos de infracciones cometidas contra los derechos de autor y conexos que ocurran a través de sistemas o redes controladas u operadas por éstos o en su representación". El principio está complementado por un sistema de "inmunidad condicionada", por el cual los proveedores de servicios deben cumplir una serie de condiciones generales y específicas para ser eximidos de responsabilidad.

El decreto establece la necesidad de una orden judicial para la remoción de contenido lesivo de los derechos de autor. En ese sentido, los proveedores de servicios únicamente podrán ser responsabilizados cuando hayan recibido la notificación legal de la resolución judicial tomada al efecto y no hayan sido expeditos en retirar el material.

El procedimiento para lograr el retiro de un contenido prevé una solicitud ante la autoridad judicial competente, la cual deberá contener en forma precisa los derechos presuntamente infringidos, el material infractor y su localización.

Además del procedimiento judicial, el decreto establece una novedad en el ámbito latinoamericano, al brindar la posibilidad de recurrir al sistema de notificación y notificación (notice and notice). En este caso, el presunto afectado

---

[432] Disponible en http://www.cerlalc.org/derechoenlinea/dar/leyes_reglamentos/Costa_Rica/Decreto36880.htm

puede enviar una comunicación al proveedor de servicios, indicando la violación al derecho de autor. Una vez recibida dicha comunicación, el proveedor debe comunicarlo inmediatamente al usuario o proveedor del supuesto material infractor en un plazo que no exceda los treinta días de recibida la comunicación original. Tras recibir dicha comunicación y dentro de un plazo razonable que no exceda de quince días naturales contados desde la recepción de la comunicación, el presunto infractor debidamente notificado podrá:

a) Retirar voluntariamente el material presuntamente infractor, lo cual podrá comunicar al proveedor de servicios o al titular del derecho infringido o su representante, o bien salvo mejor derecho;

b) Presentar una contestación que deberá contener la información de descargo, manifestando su decisión de resolver el reclamo correspondiente en la jurisdicción de las autoridades judiciales competentes.

En este último caso, el proveedor de servicios, dentro de un plazo razonable y proporcional no mayor a quince días naturales, a partir de la recepción de la decisión, deberá comunicarla al titular de derecho o su representante para que éste determine si inicia las acciones legales correspondientes.

En caso que el presunto infractor no conteste u omita retirar el contenido el proveedor estará legítimamente facultado para retirar o inhabilitar el acceso a un determinado contenido supuestamente infractor.

La normativa costarricense cumple con los estándares internacionales establecidos por la CIDH al disponer la obligación de retirar contenido en caso de orden de autoridad judicial. Además, se deja en claro que los proveedores no tendrán la obligación activa de monitorear los contenidos que circulan en la red. Por otra parte, el sistema alternativo de “notice and notice” también es respetuoso de la garantía de la libertad de expresión, al permitir la defensa del usuario que subió el contenido calificado de violatorio. Sin embargo, que la normativa haya salido por decreto del Poder Ejecutivo va en contra de la exigencia de que las regulaciones sobre libertad de expresión sean hechas por medio de una ley en sentido formal. En este sentido, hubiera sido deseable que la sanción del marco normativo se hubiese dado con la participación de la Asamblea Legislativa. Sobre todo, por el peligro de que un cambio de circunstancias lleve a considerar la modificación de la actual normativa por otra más restrictiva. En esa situación, resulta más sencillo cambiar un decreto que lograr la sanción de una nueva ley.

Por otro lado, y al igual que sucede con Chile, el sistema adoptado únicamente cubre casos de violaciones a derechos de autor y conexos. Los muchos otros casos que pueden dar lugar a eventuales atribuciones de responsabilidad no han sido contemplados aún por la normativa costarricense.

c) Brasil:

El 23 de Abril de 2014 fue sancionada la ley 12.965 que establece el

"Marco Civil de Internet"[433] con el objetivo de regular los derechos de los ciudadanos brasileños en el ámbito digital. La iniciativa fue ampliamente reconocida en el ámbito internacional como el primer intento de construir una especie de "Carta Magna" para los internautas, ya que pretende regular en diversas temáticas que atañen al ámbito digital, desde neutralidad de la red hasta tratamiento de datos personales. La responsabilidad de los intermediarios también tuvo su tratamiento en la Sección III del Capítulo III, titulada "De la Responsabilidad por Daños que Surjan del Contenido Generado por Terceros".

La normativa brasileña siguió los estándares internacionales y consagró como regla general la irresponsabilidad de los intermediarios por contenidos de terceros. En el caso de los proveedores de conexión el art. 18 establece tajantemente que "no serán responsabilizados civilmente por daños surgidos por contenido generado por terceros". Respecto a los proveedores de aplicaciones, el Marco Civil establece que sí podrán ser responsabilizados civilmente. El modelo adoptado es el jurisdiccional, por lo cual la notificación de la ilegalidad de un contenido deberá ser hecha por orden judicial específica. La comunicación deberá contener, bajo pena de nulidad, la identificación clara y específica del contenido especificado como violatorio, que permita la localización inequívoca del material. En ese caso, los intermediarios serán responsables si no toman las previsiones para volver indisponible el contenido especificado como violatorio, en el ámbito de los límites técnicos de sus servicios y dentro del plazo asignado (Art. 19).

El Marco Civil contiene una excepción al modelo jurisdiccional para aquellos conflictos suscitados por la divulgación, sin autorización de sus participantes, de imágenes, videos u otros materiales que contengan escenas de desnudos o de actos sexuales de carácter privado. En este caso, basta una notificación privada del afectado o su representante para que el proveedor deba eliminar el contenido. Para su validez, la solicitud deberá contener elementos que permitan la identificación específica del material considerado como violador de la intimidad del participante y la verificación de la legitimidad para la presentación del pedido. A pesar de ello, la ley se encarga de aclarar que la responsabilidad será únicamente de carácter "subsidiario".

Sin duda, el Marco Civil de Internet ha sido un acontecimiento en la defensa de los derechos humanos de los ciudadanos en el ámbito digital. Siguiendo los estándares internacionales de derechos humanos, la legislación brasileña ha establecido que los intermediarios no pueden ser responsabilizados directamente por contenidos que no fueron generados por ellos. Por otra parte, el

[433] Disponible en portugués en http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Existe traducción no oficial al español en http://blog.congresointeractivo.org/traduccion-al-castellano-del-marco-civil-de-internet-de-brasil/

requerimiento de notificación judicial garantiza la intervención de un tercero imparcial y con conocimiento jurídico, liberando a los intermediarios de una carga que no es su obligación llevar.

No obstante, subsisten cuestiones que necesitan ser aclaradas. La primera de ellas es el temor a que la reglamentación del Marco desnaturalice el espíritu protectorio de la ley. La segunda cuestión es el tratamiento normativo a aplicar a los pedidos de remoción basados en violaciones a derechos de autor y conexos. A pesar de su amplitud con respecto al resto de los temas, el Marco Civil se ha negado a regular los casos de propiedad intelectual y sólo dispuso la obligación de dictar en el futuro una ley específica sobre la temática. Si bien la norma establece que dicha ley deberá respetar la libertad de expresión y otras garantías reconocidas por la Constitución brasileña (Art.19 Inc.2), persisten las dudas sobre si el régimen a establecer en la futura legislación será respetuoso de los estándares seguidos por Brasil en el Marco Civil. Finalmente, se deberá tener cuidado en que el régimen de notificación privada para casos de "porn revenge" no sea utilizado para censurar casos que no caigan dentro del supuesto previsto.

d) Venezuela:

La legislación venezolana no prevé una regulación general para los intermediarios de Internet. Sin embargo, en Diciembre de 2010, la Asamblea Legislativa incluyó a los medios electrónicos dentro de la regulación prevista por la Ley de Responsabilidad Social en Radio y Televisión (Ley RESORTE)[434], marco legal que rige a los medios de comunicación en Venezuela. La normativa prohíbe la difusión de mensajes que "inciten o promuevan el odio y la intolerancia", "fomenten zozobra en la ciudadanía o alteren el orden público", "desconozcan a las autoridades legítimamente constituidas" o "inciten o promuevan el incumplimiento del ordenamiento jurídico vigente", entre otras. Asimismo, establece la responsabilidad de los medios electrónicos que no restrinjan la difusión de este tipo de mensajes, ante el solo pedido de la Comisión Nacional de Telecomunicaciones, órgano que depende del Poder Ejecutivo. El procedimiento es administrativo y puede ser iniciado de oficio por la misma Comisión, la cual puede ordenar el bloqueo de la página web que esté difundiendo el material presuntamente violatorio.

La norma constituye un grave peligro para la libertad de expresión, ya que deja en manos del gobierno la facultad de controlar los contenidos que se publican en Internet. La vaguedad y ambigüedad de las fórmulas utilizadas para

[434] Disponible en http://www.leyresorte.gob.ve/wp-content/uploads/2012/07/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electr%C3%B3nicos.pdf

calificar los mensajes prohibidos violan el principio de legalidad, que establece que toda restricción a la libertad de expresión debe ser clara y precisa. Por otro lado, el procedimiento para dictaminar la lesividad del contenido es realizado por un órgano administrativo dependiente del poder Ejecutivo, lo cual va en contra del requerimiento de un órgano judicial independiente e imparcial. La situación se agrava si se tiene en cuenta que la Comisión posee facultad para iniciar procesos de oficio y ordenar bloqueos de páginas web. De esta manera, se deja abierta la posibilidad de que la legislación sea utilizada discrecionalmente por el Poder Ejecutivo para restringir expresiones legítimas de opiniones políticas disidentes.

En conclusión, la ley RESORTE constituye una grave amenaza para el debate democrático y plural dentro de Internet, debido a su enfoque punitivista. Frente a la obligación del Estado de garantizar un ámbito libre de restricciones indebidas, la normativa busca desincentivar la emisión de opiniones y fomentar mecanismos de autocensura privada por parte de los medios electrónicos.

e)-Ecuador:

Al igual que en Venezuela, Ecuador también consagró un marco normativo para regular los medios de comunicación, con la sanción de la Ley Orgánica de Comunicación [435] en 2013. La iniciativa fue ampliamente cuestionada por su incongruencia con los estándares internacionales en materia de derechos humanos. En lo que respecta a medios electrónicos, la situación no es la excepción. Si bien la reglamentación estableció que los contenidos que formulen los ciudadanos y las personas jurídicas en sus blogs, redes sociales y páginas web personales, corporativas o institucionales estarán excluidos del control administrativo, las regulaciones impuestas a los medios electrónicos por la difusión de opiniones en sus plataformas, va en contra del principio de no responsabilidad de los intermediarios.

La normativa ecuatoriana establece como principio general que los medios electrónicos serán responsables por las opiniones de terceros publicadas en sus páginas web. Para eximirse de tales sanciones, las plataformas deberán implementar los siguientes mecanismos:

1. Informar de manera clara al usuario sobre su responsabilidad personal respecto de los comentarios emitidos;

2. Generar mecanismos de registro de los datos personales que permitan su identificación, como nombre, dirección electrónica, cédula de ciudadanía o identidad, o;

3. Diseñar e implementar mecanismos de autorregulación que eviten la

[435] Disponible en http://www.cncine.gob.ec/imagesFTP/63228.5_LEY_ORGANICA_COMUNICACION.pdf

publicación, y permitan la denuncia y eliminación de contenidos que lesionen los derechos consagrados en la Constitución y la ley.

Por otro lado, la ley ordena que los medios electrónicos sólo podrán reproducir comentarios de redes sociales cuando el emisor esté debidamente identificado. De lo contrario, tendrán la misma responsabilidad establecida para los contenidos publicados en su página web que no se hallen atribuidos explícitamente a otra persona.

La normativa ecuatoriana establece graves restricciones a la libertad de expresión. La regla general de responsabilidad constituye una forma de promover la autocensura de los medios de comunicación, quienes se verán incentivados a no publicar comentarios que puedan ser considerados lesivos. Esta carga está reforzada expresamente por el deber de los medios de generar "mecanismos de autorregulación" para eliminar contenidos violatorios de derechos. Esta disposición no se ajusta a los estándares internacionales de derechos humanos, que exigen la intervención de un órgano judicial independiente para la calificación de una expresión como lesiva. Por otra parte, la exigencia de registrar los datos personales de los usuarios que deseen publicar comentarios, es contraria a la forma en que habitualmente se desarrolla el debate público en Internet. El anonimato en el ámbito digital es una de las garantías para el establecimiento de una discusión democrática robusta. Internet permite a los ciudadanos expresar sus opiniones sin temor a sufrir represalias. Por lo tanto, implementar mecanismos que requieran la entrega de datos personales como condición para poder emitir una opinión constituye una amenaza a los derechos de los ciudadanos y es una forma de promover la censura de expresiones contrarias a los poderes políticos.

Finalmente, el órgano de control de todo el sistema de medios de comunicación –incluidos los electrónicos- es la Superintendencia de Información y Comunicación, de carácter administrativo. El titular de esta agencia será nombrado por un órgano administrativo colegiado, de una terna enviada por el Presidente y tendrá la facultad de fiscalizar a los medios de comunicación e imponer sanciones a cualquier medio que incumpla las obligaciones previstas en la normativa. De esta manera, los medios electrónicos estarán sometidos a la autoridad de un organismo dependiente del Poder Ejecutivo y podrán verse afectados sus derechos a libertad de expresión, con el agravante de que las resoluciones dictadas por la Superintendencia serán aplicadas de inmediato, sin que la interposición de recursos judiciales produzca efectos suspensivos.

f-) Paraguay:

La legislación paraguaya tampoco establece un marco normativo general para la actividad de los intermediarios de Internet. Sin embargo, en el año 2013,

se sancionó la Ley 4868 de Comercio Electrónico[436], cuyo objetivo es regular el comercio y la contratación realizados a través de medios electrónicos o tecnológicamente equivalentes. A partir del Capítulo III, la normativa establece un régimen de responsabilidad para los intermediarios que actúan en el ámbito del comercio electrónico.

El tratamiento jurídico de las plataformas de comercio electrónico presenta características particulares que van más allá de cuestiones vinculadas a la liberta de expresión, lo cual parecería exceder el alcance de este informe. Sin embargo, las soluciones relativas a la atribución de responsabilidad de intermediarios que se van generando en los distintos ámbitos merecen atención, a fin de que el sistema de atribución de responsabilidad en su conjunto se desarrolle en forma armónica y garantice en forma adecuada la libertad de expresión en todas las esferas de la vida. Es por este motivo que el análisis de la regulación jurídica del comercio electrónico será de utilidad para la discusión sobre la libertad de expresión en otros tipos de intermediarios.

El sistema paraguayo establece un modelo de "inmunidad condicionada" para los intermediarios. En el caso de los proveedores de servicios de alojamiento o de enlace, la ley establece que no serán responsabilizados por los datos almacenados o la información enviada, siempre que no tengan conocimiento efectivo de la ilicitud de la actividad o información remitida. En caso de que tomaren conocimiento, podrán eximirse si actúan con prontitud y diligencia en retirar los datos –en el caso de los proveedores de servicios de alojamiento- o en suprimir el enlace correspondiente –en el caso de los buscadores-.

Los inconvenientes surgen al momento de analizar el carácter de la notificación. La ley establece que la comunicación debe ser hecha por autoridad competente. El decreto reglamentario [437] especificó lo dicho por la ley, al dictaminar que la autoridad de aplicación es el Ministerio de Industria y Comercio. Si bien se debe tener en cuenta que uno de los objetivos de la norma es la protección del consumidor en el ámbito de las actividades comerciales electrónicas, no se debe perder de vista el hecho del carácter administrativo del órgano regulador. En ese sentido, podría existir el riesgo de que bajo la apariencia de un reclamo comercial o de derechos de autor, se intente restringir contenido amparado por la garantía de la libertad de expresión, sin intervención de un órgano judicial independiente.

Asimismo, la normativa permite que en el futuro se apliquen "otros medios de conocimiento efectivo que pudieran establecerse", con lo que deja abierta la posibilidad de que se constituyan mecanismos de retiro de contenido que no cuenten con la participación de ningún órgano, ya sea administrativo o judicial.

[436] Disponible en http://www.eljurista.com.py/admin/publics/upload/archivos/ea41b40fb8ce27bd7ec64237fd75ef89.pdf
[437] Disponible en http://mersanlaw.com/wp-content/uploads/2014/06/decreto__1165_2014_ce0.pdf

Para acentuar esta línea, la normativa consagra expresamente la eficacia de procedimientos de detección y retiro de contenidos que los proveedores apliquen en virtud de acuerdos voluntarios.

Las dudas surgen especialmente en materia de infracciones a los derechos de autor y conexos. La ley 4868 ha establecido el procedimiento de "notice and takedown", por el cual los afectados por alguna violación pueden solicitar mediante notificación privada a los proveedores que retiren el contenido de Internet. Para ello, los proveedores tienen la obligación de establecer procedimientos públicos y accesibles para la remoción de material violatorio de derechos de propiedad intelectual. Como suele suceder con esta clase de modelos, se corre el riesgo de que la decisión sobre los contenidos a los cuales podemos acceder quede en manos de actores privados, sin la intervención previa del Poder Judicial, órgano reconocido en las sociedades democráticas como el encargado de evaluar cuando es legítima una restricción a la libertad de expresión.

Finalmente, se debe tener en cuenta que esta regulación es muy limitada, ya que sólo se refiere a cuestiones de comercio electrónico. Fuera de este ámbito, todavía no hay normativa que regule los casos de responsabilidad de los intermediarios, sobre todo, en aquellas temáticas más vinculadas con la libertad de expresión.

4. Proyectos de Ley

Además de la legislación existente, se han presentado proyectos de ley en otros países latinoamericanos que buscaron regular la responsabilidad de los intermediarios. A continuación se hará un examen de ellos:

a) Colombia:

En 2011 el Ministerio del Interior y Justicia envió al Congreso el proyecto de ley nº 241 **"Por la cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en internet"**[438]**,** más conocido como "Ley Lleras", por el apellido del Ministro de dicha repartición. La intención del proyecto era regular la responsabilidad de los proveedores de servicios de Internet frente a potenciales infracciones a los derechos de autor. La iniciativa era una de las obligaciones que Colombia debía cumplir para adaptar su normativa a exigencias del Tratados de Libre Comercio con EEUU[439], que estaba a punto de entrar en vigencia.

El proyecto contemplaba un sistema de "notice and takedown" para la detección y el retiro de contenido presuntamente violatorio de los derechos de autor. El procedimiento establecido preveía una solicitud de retiro por parte del

[438] Disponible en http://redpatodos.co/blog/wp-content/uploads/2014/12/Gaceta152-2011.pdf
[439] Disponible en http://www.tlc.gov.co/publicaciones.php?id=727

titular del derecho de autor al proveedor de servicios, el cual, si consideraba cumplido los requisitos, debía retirar el contenido dentro de las 72 horas de recibida la solicitud, sin intervención judicial. De lo contrario, el proveedor era considerado co-responsable por las violaciones ocasionadas a los derechos de autor y conexos.

Asimismo, el proveedor debía comunicar al usuario presuntamente infractor del retiro o la inhabilitación del contenido. Si el supuesto infractor realizaba una solicitud de restablecimiento del material retirado o inhabilitado, el prestador de servicios debía restablecer el material dentro de los 14 días de realizada la solicitud, a menos que la persona que realizó la solicitud de retiro o inhabilitación original presente ante el proveedor una orden judicial en virtud de la cual el material objeto de la solicitud deba ser retirado o inhabilitado.

El proyecto fue ampliamente cuestionado, debido a que obligaba a las empresas, bajo la amenaza de incurrir en responsabilidad, a bloquear contenido que fuera denunciado como ilegítimo, sin la participación de ningún órgano judicial, con lo cual se corría el peligro de generar mecanismos amplios de autocensura, sin la debida transparencia. El argumento de que el país debía cumplir con las obligaciones contraídas en el TLC no es sustentable, ya que existen países como Chile que también firmaron acuerdos de libre comercio con EEUU y sin embargo, poseen legislación sobre propiedad intelectual que se ajusta a los estándares internacionales de derechos humanos.

Finalmente, la iniciativa fue rechazada por el plenario del Senado en Noviembre de 2011 en virtud de la grave polémica que originó su contenido. Al año siguiente volvió a presentarse un nuevo proyecto –conocido como ley Lleras 2.0-, que no incluía esta vez la temática de la responsabilidad de los intermediarios. La iniciativa fue aprobada por el Poder Legislativo. Sin embargo, la Corte Constitucional declaró la inconstitucionalidad de la norma debido a vicios en el procedimiento de sanción.

b) Argentina:

Existen varios proyectos de ley que pretenden regular la responsabilidad de los intermediarios en Internet.

Proyecto Pinedo: A fines de 2010 ingresó un proyecto presentado por el diputado Federico Pinedo con Nº de Expediente 8793-D-2010[440], el cual establece que los proveedores de servicios de Internet serán responsabilizados por:

-el almacenamiento automático de contenidos generados por terceros

[440] Disponible en http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=8793-D-2010

exclusivamente cuando tuvieren conocimiento efectivo de que los contenidos almacenados violan normas legales o derechos de terceros.

-la transmisión o retransmisión de contenidos generados por terceros exclusivamente cuando los propios Proveedores de Servicios de Internet sean quienes originen dicha transmisión o retransmisión, o cuando modifiquen o seleccionen los contenidos y/o seleccionen a los destinatarios de la información transmitida o retransmitida.

Además, los Proveedores de Alojamiento, los Proveedores de Contenidos y los Proveedores de Servicios que ofrezcan enlaces a otros sitios webs u ofrezcan información provista por terceros, serán responsables respecto de la información provista por los terceros exclusivamente en los casos en que tengan conocimiento efectivo de que la información almacenada viola normas legales o derechos de terceros.

A los efectos de determinar la responsabilidad, el proyecto, en su versión original, no definía qué se iba a entender por "conocimiento efectivo". La indeterminación fue duramente criticada ya que dejaba abierta la posibilidad de que una simple notificación privada pudiera ser considerada como susceptible de generar tal conocimiento efectivo, al contrario de lo exigido por los estándares internacionales de derechos humanos. Frente a la controversia levantada, el diputado Pinedo reformuló su proyecto y aclaró que el conocimiento efectivo únicamente puede producirse cuando existe notificación judicial.

Sin embargo, los cuestionamientos continuaron. La imputación de responsabilidad a los intermediarios por enlaces a sitios web con información lesiva resulta irrazonable ya que los ISP no pueden controlar los sitios web que enlaza. Actualmente, el proyecto permanece en comisión.

Proyecto Obliglio: En 2012, y mediante expediente 8070-D-2012[441], fue presentado un nuevo proyecto por el diputado Julián Obliglio, el cual prevé un procedimiento de notificación y retiro, sin intervención judicial, para contenidos que violen derechos de la personalidad. En estos casos, los intermediarios deberán dar de baja o impedir el acceso a material que haya sido denunciado por violar la privacidad de una persona, sin necesidad de una orden judicial. Para ello, los proveedores estarán obligados a crear y/o a conservar una cuenta de correo electrónico en la cual puedan ser notificados de contenidos ilícitos. Esta cuenta estará publicada en forma visible y permanente en los sitios web de los proveedores de servicios de intermediación.

Este proyecto también fue objeto de numerosas críticas, ya que el sistema de notificación privada es contrario a los estándares internacionales de derechos humanos, al no incluir la participación de un órgano judicial independiente para la

[441] Disponible en http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=8070-d-2012

determinación de la ilegalidad del contenido. Si bien la iniciativa acota este sistema únicamente a aquellos casos en que están en juego derechos de la personalidad, el carácter general del término plantea el peligro de que se incluyan casos que en realidad no pertenecen a aquel, con lo que se generarían mecanismos de censura privada por parte de los intermediarios, que ante la duda, optarían por retirar el material cuestionado. De esta manera, el proyecto va en contra de los principios internacionales, que exigen que toda ley que restrinja la libertad de expresión deba estar formulada en forma clara, precisa y accesible.

Al igual que el proyecto del legislador Pinedo, la iniciativa del legislador Obliglio continúa en comisión.

Proyecto Fellner: En 2015 presentada un nuevo proyecto para regular la responsabilidad de intermediarios de Internet a través de la Senadora Liliana Fellner. La iniciativa lleva como Nº de Expte. el 1865/15[442] y actualmente está en la comisión de Sistemas, Medios de Comunicación y Libertad de Expresión. La propuesta tiene como ámbito de aplicación únicamente la actividad de los servicios de enlace y búsqueda de contenidos y establece como principio general que aquéllos no serán responsables por los daños y perjuicios generados por contenidos alojados en sitios de terceros. La responsabilidad nacerá únicamente cuando sean notificados, conforme el procedimiento establecido y no adopten las medidas para eliminar el enlace.

El procedimiento para solicitar la remoción varía de acuerdo a si el contenido es manifiestamente ilegítimo o aparentemente ilegítimo. En el primero caso, el modelo adoptado es el de notificación privada: la persona afectada podrá solicitar directamente a los proveedores de servicios de enlace y búsqueda que eliminen el enlace. La iniciativa entiende por contenidos manifiestamente ilegítimos aquellos que en forma clara e indiscutible: a) faciliten la comisión de delitos o instiguen a cometerlos; b) pongan en peligro la vida o integridad de una persona; c) hagan apología del genocidio, racismo u otra forma de discriminación o incitación a la violencia; d) desbaraten o adviertan sobre investigaciones judiciales en curso que debieran permanecer secretas; e) produzcan daños graves al honor, la intimidad o la imagen de las personas o f) exhiban pornografía infantil.

A los fines de facilitar la notificación, los proveedores estarán obligados a crear y conservar de forma permanente y visible en sus respectivos sitios web una cuenta de correo electrónico o formulario on line en los cuales puedan ser notificados de contenidos ilegítimos.

Respecto a los contenidos aparentemente ilegítimos, el proyecto adopta el modelo jurisdiccional: los proveedores deberán eliminar los enlaces cuando haya

[442] Disponible en http://www.senado.gov.ar/parlamentario/comisiones/verExp/1865.15/S/PL

una orden judicial que, a solicitud de la persona afectada, así lo disponga. La propuesta dispone que se entienda por contenidos aparentemente ilegítimos, aquellos que importen eventuales lesiones al honor, a la intimidad, a la imagen o a cualquier otro derecho que resulte afectado por la difusión de tales contenidos, pero que exijan un esclarecimiento para su efectiva determinación.

Esta iniciativa contiene numerosas disposiciones que resultan violatorias de los estándares internacionales de derechos humanos. En primer lugar, establece la posibilidad de remover contenido sin intervención judicial. En segundo lugar, el lenguaje utilizado no es claro, preciso ni accesible. Términos como "manifiestamente ilegítimo o aparentemente ilegítimo" conllevan una gran carga de ambigüedad, problema que se agrava en este caso, ya que la diferencia entre uno y otro caso implica la aplicación de regímenes jurídicos distintos. Si bien el proyecto intenta describir las categorías, las palabras utilizadas no logran despejar la confusión. Por ejemplo, no se delimita claramente la diferencia entre "daño grave" –considerado manifiestamente ilegítimo- y "lesión" -considerada aparentemente ilegítimo- al honor, la intimidad o la imagen de las personas. En tercer lugar, el proyecto prevé la posibilidad de retirar contenido frente a "eventuales" lesiones. Es decir, la iniciativa permitiría la remoción de material que todavía no ha producido daño alguno, violando de manera flagrante una de los principios más básicos en materia de libertad de expresión.

c)- Perú:

El 12 de Abril de 2006 se firmó el Tratado de Libre Comercio entre Perú y Estados Unidos[443], por el cual el país sudamericano se compromete a dictar legislación sobre la materia. A fines de 2012 el gobierno peruano manifestó su intención de plasmar en la legislación nacional los lineamientos sobre responsabilidad de los intermediarios previstos en el TLC. Sin embargo, este proceso fue detenido posteriormente sin que hayan surgido proyectos de ley o resultados claros. Por lo tanto, hasta la fecha todavía está pendiente la sanción de la ley correspondiente.

d)- México:

A fines de 2013, se presentó en la Cámara de Diputados un proyecto de ley que buscaba detener la distribución de contenidos en línea que infrinjan derechos de autor y propiedad intelectual mediante el castigo a infractores con el bloqueo al acceso a Internet, multas y cárcel.

La iniciativa –conocida como "Ley Beltrones"- facultaba al Instituto Mexicano

[443]Disponible en www.acuerdoscomerciales.gob.pe/images/stories/eeuu/espanol/Propiedad_Intelectual_limpio.pdf

de Propiedad Industrial (IMPI) para que investigue, de oficio o mediante solicitud de parte, la presunta infracción e inicie el procedimiento administrativo. Los proveedores de Internet debían suministrar al IMPI todos los datos del presunto infractor para su localización, incluyendo nombre, domicilio físico, dirección IP del infractor o la asociada al servidor donde se hospeda el contenido. Por último, el IMPI tenía la facultad para ordenar a los proveedores de Internet la suspensión del acceso a sitios que presuntamente infrinjan la ley.

La iniciativa fue duramente cuestionada, ya que la amenaza de bloqueo de sitios web generaba incentivos para que los proveedores de servicios en Internet adoptaran medidas de autocensura, con el consiguiente perjuicio de la garantía de la libertad de expresión. Asimismo, que la determinación de las infracciones esté en manos de un órgano administrativo resulta contrario al principio de que el encargado de realizar dicha tarea debe ser un órgano judicial independiente

Finalmente, la iniciativa no prosperó en el Congreso Nacional y fue archivada. Sin embargo, hubo un intento de reflotar el proyecto en Febrero de 2015 que tampoco tuvo éxito.

5. Jurisprudencia

Frente a la carencia de normativa específica, las decisiones de los tribunales judiciales sirvieron como guía para delimitar el alcance de las responsabilidades de los intermediarios por contenido generado por terceros. Si bien son pocos los países en los cuales se planteó este tipo de conflictos, conviene realizar un repaso para tener una idea acerca de los estándares utilizados por los tribunales para la resolución de esta clase de controversias.

a) Chile:

• *Fuentes vs ENTEL I*

El primer antecedente jurisprudencial data de 1999 con el fallo "Fuentes vs ENTEL I"[444], en el cual se discutía la responsabilidad de la Empresa Nacional de Telecomunicaciones S.A. (ENTEL S.A.) por la difusión en sus páginas web www.entelchile.net y www.tribu.grupoweb.cl, de avisos de ofrecimiento de servicios sexuales de una chica menor de edad. El padre de la menor responsabilizaba a ENTEL S.A., en su carácter de administrador del sitio web, ya que, a su juicio, había permitido irresponsablemente la publicación del aviso y otros de similar

[444] Caso: Entel, recurso de protección, Causa Rol No 243-99, Corte de Apelaciones de Concepción, 6 de Diciembre de 1999. Ver fallo en https://censorshipcases.wordpress.com/2012/03/27/caso-entel-recurso-de-proteccion-causa-rol-no-243-99-santiago-6-de-diciembre-de-1999/

naturaleza por parte de personas anónimas sin verificar la identidad de sus fuentes. La empresa adujo que no era responsable, pues el aviso provenía de un usuario en uso de la plataforma gratuita facilitada por el proveedor, pero cuyo contenido era total responsabilidad de quien exponía el aviso.

La Corte de Apelaciones de Concepción, tribunal encargado de resolver el caso, rechazó el recurso debido a que para el momento de la sentencia, los avisos ya habían sido retirados. Sin embargó, estableció diversos estándares para el análisis de la temática. En primer lugar, estableció el principio de que "la responsabilidad por conductas realizadas en Internet dependerá de las funciones que el actor de Internet o usuario de la red" desempeñe. Para ello, identifica cuatro clases de actores: el proveedor de acceso, el proveedor de almacenamiento, el proveedor de contenido y los destinatarios finales. En segundo lugar, el tribunal sostuvo que tal responsabilidad recaerá únicamente en el proveedor de contenido en la red. Sin embargo, también puede caber la extensión de la responsabilidad al proveedor de acceso y al proveedor de alojamiento de la página Web respectiva, cuando, a sabiendas de la actividad ilícita que se realiza por los abonados a su servicio, no ha retirado los datos o no ha hecho que el acceso a ellos sea imposible. En ese sentido, la Corte de Apelaciones no establece cuándo se considera que los proveedores tienen el conocimiento del carácter ilegítimo del contenido.

Otro aspecto polémico del fallo radica en que establece la obligatoriedad de los proveedores de verificar el contenido del sitio en el que ofrece alojamiento y de tomar, por consiguiente, si es necesario, las medidas necesarias para proteger los derechos de la personalidad, derechos de autor y de marcas, entre ellas, la eliminación de publicaciones contrarias al ordenamiento jurídico. Actualmente, dicho deber sería contrario a los estándares internacionales sobre libertad de expresión que exigen la no obligación de un monitoreo activo por parte de los intermediarios.

• *Fuentes vs ENTEL II*

Una segunda etapa de este conflicto tuvo lugar en 2007, cuando el señor Fuentes, padre de la menor involucrada, solicitó un resarcimiento económico a ENTEL por los daños ocasionados a su hija. En este caso, conocido como "Fuentes vs ENTEL II"[445] la Corte de Apelaciones sostuvo que el proveedor no podía ser considerado responsable, ya que "no se encuentra obligado a controlar el ingreso de contenido a la red", en virtud del principio de libertad de la información

[445] Caso: Carmen Yañez con Entel, demanda civil, sentencia de apelación, rol 1223-2003, 21-12-2007 Corte de Apelaciones de Concepción. Ver fallo en https://censorshipcases.wordpress.com/2012/03/27/caso-carmen-yanez-con-entel-demanda-civil-sentencia-de-apelacion-rol-1223-2003-21-12-2007/

que circula en internet. Por otra parte, el tribunal consideró que el ENTEL no actuó con negligencia, ya que removió el contenido cuestionado, apenas recibió la notificación por parte del padre de la menor.

Este fallo representó un paso adelante al anterior, ya que dejó en claro que los intermediarios no pueden tener la obligación de controlar el contenido subido a la red. Sin embargo, dejó dudas en cuanto a que aceptó la notificación privada como medio de poner el carácter ilegítimo del contenido en conocimiento efectivo del proveedor.

• *Suazo vs Reclamos.cl*

El conflicto entre libertad de expresión y derecho al honor fue tratado por los tribunales chilenos en "Suazo vs Reclamos.cl" del 2009. Allí se demandó el retiro de mensajes anónimos publicados en el sitio demandado, que contenían quejas e injurias contra una institución escolar y algunos de sus profesores. La Corte de Apelaciones de Santiago [446] rechazó la demanda con base en el derecho constitucional de emitir opinión e información sin censura previa. El tribunal sostuvo que "la limitación del libre acceso y libre tráfico a Internet por la vía de obligar al proveedor a revisar todos los contenidos, conduciría casi ineludiblemente a transformar a éste en censor, con el serio riesgo de caer en una censura previa que atentaría contra la garantía constitucional de la libertad de expresión". Por otra parte, estableció expresamente el carácter de intermediarios de los proveedores, al sostener que las "empresas proveedoras se obligan únicamente a prestar los medios materiales siendo el usuario quien determina el lugar de navegación o adonde dirigir sus comunicaciones, por lo que respecto del contenido que circula en la red no tendrían un papel que desempeñar que no sea el de distribuir la información".

La resolución fue apelada ante la Corte Suprema[447], que en un escueto fallo confirmó lo dictado por el tribunal de apelación, al sostener "que no se encuentra establecido que se haya producido por parte del recurrido una manifestación abusiva al ejercicio del derecho".

• *Abbott vs. Google*

Al contrario que en "Suazo", en "Abbott vs. Google"[448] los tribunales hicieron prevalecer el derecho al honor. Allí, el abogado Jorge Abbott solicitó que se

[446] Corte de Apelaciones de Santiago Fallo 11.538-2008, ver fallo en http://iura.cl/jp/apelaciones/santiago/2008/11538.html
[447] Corte Suprema Fallo 3047-2009, ver fallo en http://iura.cl/jp/suprema/2009/3047
[448] Causa nº 228/2012. Resolución nº 50461, de Corte de Apelaciones de Valparaíso, de 30 de Julio de 2012, ver fallo en http://www.derecho-chile.cl/sentencia-responsabilidad-de-los-administradores-de-las-paginas-webs/

eliminen publicaciones web que contenían lo que él consideraba eran expresiones injuriosas, contra su persona y su familia. Asimismo, solicito que Google establezca filtros para evitar que aparezcan en su lista de búsquedas las afirmaciones ya mencionadas, que lo acusaban de corrupto y de haber colaborado con la dictadura militar. La Corte de Apelaciones de Valparaíso hizo lugar a la demanda, ya que las publicaciones difundidas violaban la garantía del "respeto y protección a la vida privada y a la honra de la persona y su familia", prevista en la Constitución chilena. El tribunal estimó que la existencia de expresiones injuriosas era evidente, y que a pesar del retiro voluntario de contenidos y enlaces por parte de los respectivos proveedores, existía una "persistencia" en publicar tales contenidos En consecuencia, ordenó la eliminación de las informaciones injuriosas de las páginas donde fueron publicadas. Asimismo, ordenó a Google que establezca los filtros necesarios para evitar publicaciones que presenten inequívocamente expresiones de carácter injurioso.

El fallo resulta cuestionable ya que, además de promover la censura de información que resulta de interés público, obliga a los buscadores a establecer una vigilancia activa para detectar expresiones "inequívocas". La vaguedad del término utilizado implica el riesgo de que los adopten prácticas de autocensura que seguramente lleven a que supriman vínculos que no son violatorios de ningún derecho, con el consiguiente perjuicio para la libertad de expresión.

b) Colombia:

En este país los casos llevados ante los estrados judiciales tuvieron que ver con el ejercicio del llamado "derecho al olvido".

- *Martínez vs Google y El Tiempo*

El primer caso tuvo su resolución a principios de 2013 y trató sobre la solicitud de un ciudadano de apellido Martínez a Google y al sitio web del periódico El Tiempo[449] de que se elimine un artículo periodístico, en el que se lo mencionaba como miembro de una organización criminal dedicada al narcotráfico y sometido a un proceso penal. Dicho proceso finalizó sin que se dicte condena en su contra, debido a que prescribió la acción penal.

La Corte Constitucional determinó que, en este caso, **no es competencia ni responsabilidad de Google, rectificar, corregir, eliminar o complementar la información que arroja una búsqueda concreta**. El tribunal confirmó el carácter de mero intermediario establecido por la Sala de Revisión al decir que "**Google presta un servicio de búsqueda de la información que hay en toda la red, y no es quien redacta o publica tal información**, **sino que es un simple motor**

[449] Sentencia T-040/13 de la Corte Constitucional, ver fallo en http://www.corteconstitucional.gov.co/relatoria/2013/t-040-13.htm

de búsqueda al cual no se le puede endilgar la responsabilidad sobre la veracidad o imparcialidad de un respectivo artículo, noticia o columna que aparezca en sus resultados". No obstante, la Corte se cuidó de establecer un precedente para futuros casos y afirmó que pueden existir casos en los que "por características distintas, una base de datos que cumple la función de Google, pueda generar alguna vulneración de un derecho fundamental por la información que administra".

Respecto a El Tiempo, la Corte declaró que el periódico era responsable, ya que había desconocido el principio de veracidad por haber emitido una noticia en la que no se aclaraba las circunstancias y razones por las cuales se relacionaba al demandante con el contenido de la misma. No obstante, la Corte consideró que la rectificación procedente en este caso no era eliminar el artículo periodístico sino aclarar las razones por las que el accionante apareció en el contexto descripto en la noticia. En razón a esto ordenó la modificación del título del artículo y la inclusión de la frase "personas presuntamente vinculadas" al referir el listado de las personas investigadas, así como la inclusión de un relato sucinto de las razones por las que se incluyó al señor Martínez en la publicación y su relación con el contexto descripto.

- *Menor vs El Nuevo Día*

El mismo criterio fue utilizado para resolver el pedido de una madre de que se elimine información aparecida en el periódico "El Nuevo Día"[450]que podría dar lugar a la revelación de la identidad de su hijo de cinco años de edad, en el marco de un caso de abuso sexual. La Corte se remitió a lo dicho en "Martínez" para rechazar el pedido. Sin embargo, consideró que el periódico Nuevo Día era responsable y debía proceder a eliminar de sus archivos web las noticias que contengan datos que puedan llevar a la identificación del menor.

- *Gloria vs Casa Editorial El Tiempo*

En el 2015 se dictó un fallo clave para la libertad de expresión en Internet en Colombia. En la causa "Gloria vs Casa Editorial El Tiempo"[451] la demandante solicitó que se eliminen de los motores de búsqueda toda información sobre su participación en hechos de trata de personas, en relación con los cuales nunca fue declarada culpable. La Corte Constitucional utilizó el caso para analizar si el ordenamiento jurídico colombiano consagraba el "derecho al olvido" y además,

[450] Sentencia T-453/13 de la Corte Constitucional, ver fallo en http://www.corteconstitucional.gov.co/relatoria/2013/T-453-13.htm

[451] Sentencia T-277/15 de la Corte Constitucional, ver fallo en http://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm

para establecer estándares relacionados con la actuación de los buscadores en relación con contenido generado por terceros.

En primer lugar, el Tribunal estableció que Gloria había sufrido una violación a su derecho a la honra, debido a que la información publicada era verdadera pero incompleta, ya que había omitido mencionar su absolución en el proceso. En segundo lugar, la Corte ratificó lo dicho en los fallos anteriores y dictaminó que Google no era responsable por las informaciones aparecidas en su lista de búsqueda. Para llegar a tal conclusión, el Tribunal se hizo eco del informe de la Relatoría Especial para la Libertad de Expresión de la CIDH, y determinó que "imponer responsabilidades a los intermediarios de Internet por los contenidos transmitidos limitaría de forma importante la difusión de ideas por este medio de comunicación, pues les daría el poder para regular el flujo de información en la red". En tercer lugar, la Corte sí estableció la responsabilidad de los medios de comunicación por los contenidos generados por ellos en sus páginas web. Por lo tanto, ellos deben ser los encargados de dar respuesta al pedido realizado por "Gloria".

El tribunal consideró que los medios tienen la obligación de actualizar de oficio –haya o no petición al respecto- las notas sobre procesos judiciales aunque haya pasado mucho tiempo desde su publicación. De esta manera, la Corte determinó que cuando hay un desenlace favorable para el implicado en un proceso judicial, se debe actualizar la información de manera tal que se difunda el resultado favorable y se dificulte la búsqueda de la noticia no actualizada. Según el tribunal, el medio debe responder la solicitud del afectado y, si es necesario, desindexar el contenido de los buscadores de tal forma que la información se actualice y permanezca online pero no sea posible acceder a ella a través de buscadores. Esta regla no aplica a personas con alta notoriedad pública o servidores públicos, ni en casos de crímenes de lesa humanidad o violaciones de derechos humanos.

Para cumplir con la obligación, el tribunal dispuso que la noticia permanezca publicada en la página web de la Casa Editorial El Tiempo, pero limitando su difusión a través de Internet. El medio para lograr esta limitación es el uso, por parte del periódico, de herramientas técnicas como "robots.txt" y "metatags", que permite a los titulares y administradores de un sitio web impedir que contenidos específicos sean mostrados como resultados al realizar una consulta por medio de un buscador de internet. En ese sentido, la Corte explicó que utilizando la herramienta "robots.txt", lo que se logra es que un determinado contenido no sea rastreado por el buscador, mientras que con los "metatags" se logra que un determinado URL, pese a ser indexado, no sea mostrado como resultado de búsqueda.

La Corte concluye que esta forma de limitación de contenido es la que mejor permite equilibrar los principios constitucionales en tensión, ya que es factible mantener la publicación de la noticia, sin que se corra el riesgo de alterar

la verdad histórica y evitando, en todo caso, que el dato negativo que afecta los derechos de la accionante resulte accesible de manera indiscriminada a partir de la mera digitación de su nombre en un buscador de internet.

Entre los aspectos positivos del fallo, figura la clara decisión judicial de no hacer recaer la responsabilidad en los intermediarios, sino en los generadores de contenidos, quienes deben ser los encargados de adoptar las medidas necesarias para no afectar derechos de terceros. En este sentido, la Corte colombiana tomó un camino diferente a la jurisprudencia europea, que en el fallo "Costeja"– de características similares a "Gloria"- había consagrado la obligación de los buscadores de desindexar de sus listas aquellas noticias que fueran irrelevantes.

Por otra parte, la Corte entendió el importante papel que los intermediarios cumplen para el ejercicio de la libertad de expresión, al otorgarle la inmunidad necesaria para que desarrollen sus funciones. De lo contrario, se hubiera corrido el riesgo de transformar a los buscadores en censores privados con la facultad de desindexar contenido, ante la solicitud de cualquier particular.

Sin embargo, existen zonas grises en la sentencia, que merecen atención. En primer lugar, la obligación de actualizar permanentemente las noticias sobre procesos judiciales resulta una carga desproporcionada para los sitios web de los medios de comunicación, máxime si se tiene en cuenta que no requiere solicitud del afectado. En segundo lugar, las soluciones tecnológicas propuestas por la Corte ("robots.txt" y "metatags") pueden dificultar el acceso a contenidos que son de relevancia para el debate público. Finalmente, el fallo coloca en una delicada situación a los medios de comunicación chicos o blogs periodísticos, quienes enfrentarán grandes obstáculos técnicos y financieros para poder cumplir con las obligaciones establecidas en la resolución. De esta manera, se corre el peligro de que desaparezcan muchos medios o periodistas independientes que utilizan internet para dar a conocer información que no es difundida por los grandes medios, con la consiguiente pérdida para el debate democrático.

c) México:

En Enero de 2015, el Instituto Nacional de Acceso a la Información, órgano de carácter administrativo, dictaminó a favor del empresario Carlos Sánchez de la Peña y ordeno a Google México que removiera de su motor de búsqueda tres links que contenían información y comentarios negativos acerca de los negocios de la familia de Sánchez, en las que su nombre aparecía mencionado[452].

El INAI basó su decisión en la Ley Federal de Datos Personales en Posesión de Particulares (LFPDPPP), la cual prevé los derechos de acceso,

[452] Instituto Nacional para el Acceso a la Información (INAI), Carlos Sánchez de la Peña v. Google México S.R.L. PPD.0094/14,ver fallo en http://http//inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf

rectificación, cancelación y objeción, que las personas pueden ejercer contra el tratamiento de sus datos por parte de particulares. Los comisionados del INAI consideraron que el señor Sánchez cumplía con los requisitos que permiten la remoción de información cuando su "persistencia causa daño", aun si la información fue publicada legítimamente.

El fallo fue cuestionado por haber introducido el "derecho al olvido" –no contemplado en la legislación mexicana- , bajo el paraguas de la protección de los datos personales. Asimismo, la INAI ni siquiera hizo una aplicación correcta de la LFPDPPP, ya que ésta prevé excepciones a la privacidad en caso de que la información sea de interés público. Si bien el INAI no aplicó la excepción con el argumento de que Google no la había planteado al momento de ejercer su derecho a la defensa, la obligación de aplicar el marco normativo que mejor proteja los derechos humanos debe ser cumplida, aun cuando no haya mediado solicitud de parte. Finalmente, el hecho de que sea un órgano administrativo el encargado de resolver cuestiones de acceso a contenidos en la red resulta contrario a la exigencia internacional, que requiere la intervención de un órgano judicial independiente e imparcial.

d) Brasil:

- *Xuxa vs. Google Brasil*

En 2012, el Supremo Tribunal de Justicia (STJ) rechazó una demanda de la famosa conductora de televisión Xuxa[453], que solicitaba a Google la restricción de búsquedas que la vinculaban con una vieja película en la que aparecía teniendo sexo con un adolescente. El tribunal sostuvo que Google no es responsable de los contenidos que organiza y cuya búsqueda facilita en la red. Por lo tanto, el filtrado de contenido no es una actividad intrínseca de los servicios de búsqueda.

Por otra parte, el STJ considero que sería imposible delimitar parámetros certeros de los que puedan valerse los proveedores de búsqueda para determinar cuándo un contenido es potencialmente ofensivo, ante la subjetividad del daño psicológico o a la imagen. En consecuencia, consideró "temerario" otorgar tal juicio de discrecionalidad a los intermediarios.

El STJ también aseveró que los proveedores de contenido no pueden ser obligados a eliminar de su sistema los resultados derivados de la búsqueda de

[453] 429Superior Tribunal de Justicia "Google Brasil Internet vs María Da Graca Xuxa Meneghel" Recurso Especial N° 1.316.921 – RJ (2011/0307909-6), ver fallo en https://ww2.stj.jus.br/revistaeletronica/Abre_Documento.asp?sSeq=1161904&sReg=201103079096&sData=20120629&formato=HTML

determinados términos o expresiones, tampoco los resultados que apunten a una foto o texto específico, independientemente de la indicación del URL de la página donde esté el contenido. Finalmente, el tribunal afirmó que no se puede, afectar el derecho colectivo a la información con el objeto de dificultar la propagación de contenido ilícito u ofensivo. Al ponderar los derechos en juego, se debe privilegiar la garantía de la libertad de información, sobre todo considerando que Internet representa en la actualidad un importante vehículo de comunicación social masivo.

• *Margarete Santos Silva vs. Google Brasil*

El mismo año, el STJ tuvo la oportunidad de decidir en un caso de difamación a través de las redes sociales. El tribunal rechazó un recurso especial presentado por Google contra resoluciones de tribunales inferiores que condenaban a la empresa por haber demorado más de dos meses en retirar del sitio de la red social Orkut (propiedad de Google) un perfil falso que venía denigrando la imagen de una mujer llamada Margarete Santos Silva[454]. El tribunal estableció que una vez notificado por la afectada de que determinado texto o imagen tiene contenido ilícito, el proveedor debe retirar el material en un plazo de 24 horas, bajo pena de responder solidariamente como autor directo del daño, en virtud de la omisión incurrida. Dentro de este plazo, el proveedor no está obligado a analizar el contenido de la denuncia recibida, debiendo aplicar únicamente una suspensión preventiva, hasta que tenga tiempo suficiente para analizar la veracidad de las alegaciones. El análisis no puede ser postergado indefinidamente y el proveedor debe, en el tiempo más breve posible, dar una solución final al conflicto, confirmando la remoción definitiva de la página o restableciéndola en el *site*.

La resolución judicial reconoció que este procedimiento puede violar los derechos de usuarios que vean impropiamente suspendidas sus páginas. Sin embargo, consideró que al momento de sopesar los derechos involucrados, debe prevalecer la dignidad y el honor de las personas afectadas.

El fallo introduce un sistema de notificación privada para la remoción de contenidos contrarios a los principios que guían la materia. Sin embargo, con el posterior dictado del Marco Civil, que consagró un modelo de notificación judicial, la vigencia del fallo quedó desactualizada, aunque puede permanecer como referencia para aquellos casos de exhibición de videos sexuales privados, en que la notificación privada está permitida.

[454]Superior Tribunal de Justicia "Google Brasil Internet vs. Margarete Santos Silva" Recurso Especial N° 287.046- RS (2013/0016267-0), ver fallo en http://www.stj.jus.br/SCON/decisoes/toc.jsp?livre=1323754%2FRJ&&b=DTXT&thesaurus=JURIDICO&p=true

• *Google Brasil vs Dafra*

En materia de infracciones a los derechos de propiedad intelectual, la ausencia de regulación, aun después de la entrada en vigencia del Marco Civil de Internet – que expresamente excluye de su regulación este tipo de conflictos-, ha provocado que la jurisprudencia siga siendo importante para delimitar los lineamientos de la responsabilidad de los intermediarios. En ese sentido, uno de los fallos más importantes involucró a la empresa de motocicletas "Dafra"[455]. En este caso, el STJ siguió una orientación más restrictiva de la libertad de expresión, al responsabilizar en 2014 a Google por no tomarlas medidas necesarias para impedir que se vea por la plataforma de videos You Tube (propiedad de Google) una parodia de un comercial realizado por la empresa demandante. Si bien Google había accedido a la solicitud de Dafra de remover el video, luego fueron subidas a You Tube numerosas versiones de la parodia con diferentes títulos. La empresa requirió entonces que Google implementara mecanismos de bloqueo de búsquedas que impida el posteo de cualquier material no autorizado relacionado con la campaña publicitaria de Dafra.

El tribunal manifestó que determinar cuáles son los límites de la responsabilidad de los intermediarios se vuelve relevante en virtud de las múltiples violaciones a derechos que se producen a través de Internet. En este sentido, el tribunal manifestó que "no parece adecuado que el Poder Judicial adopte esta involución humana, ética y social -la violación de derechos- como un módico e inevitable precio a pagar por la evolución tecnológica, figurando en ese escenario como mero espectador".

Frente a la defensa de Google acerca de la imposibilidad técnica de remover todos los videos publicados, el STJ sostuvo que You Tube sí cuenta con la posibilidad técnica de controlar todos los videos que se suben a su plataforma y suscribió lo afirmado por la pericia respecto a que si no lo hacía era solo por una cuestión de "conveniencia u oportunidad". Incluso, si eventualmente fuera cierto lo afirmado por el demandado, su responsabilidad subsistiría ya que si "Google creó un monstruo inmanejable, debe ser el único que cargue con las desastrosas consecuencias generadas por la falta de control de los usuarios de sus sitios." De esta manera, el Tribunal consideró que el proveedor de Internet debe retirar los contenidos difamatorios para terceros, subidos por sus usuarios, independientemente de si hubo o no una indicación precisa del URL por parte del ofendido. En consecuencia, ordenó a Google que remueva todos los videos que parodien la campaña de Dafra en un plazo de 24 horas desde que sean subidos a

[455] Superior Tribunal de Justicia "Google Brasil vs. Dafra" Recurso Especial N° 1306157/SP http://ww2.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroUnic%20o&termo=90432250520098260000&totalRegistrosPorPagina=40&aplicacao=proce%20ssos.ea

You Tube.

El fallo presenta muchas dudas, ya que la orden de restricción genérica emitida no cumple con el requisito de indicar en forma clara el contenido que viola el derecho presuntamente afectado. La no exigencia de precisar el URL implica el riesgo de colocar al intermediario en una posición de monitoreo activo de todos los contenidos que circulan en la red y la carga puesta al proveedor de evaluar la legalidad de los contenidos subidos a los fines de su remoción, conlleva el riesgo de provocar actos de censura de material no lesivo de ningún derecho en particular.

• *Orkut (Google Brasil)*

Por otra parte, el STJ adoptó postura más favorable a los estándares internacionales con el dictado del fallo "Orkut"[456] de 2015. Allí, el tribunal sostuvo que los proveedores de contenido no pueden ser considerados responsables por violaciones de copyright hechas por terceros si no hay un aprovechamiento económico de tales conductas. Para así decidir, el STJ adoptó la doctrina anglosajona de "secondary liability" (contributory y vicarious liability) y consideró que la estructura de Orkut no había contribuido a la infracción, ya que la red social no tenía como objetivo el intercambio de archivos ni suministraba los instrumentos técnicos para que fuese posible su descarga. De esta manera, la arquitectura de la red social no proveía sustancialmente de los medios necesarios para la violación de derechos. Asimismo, considerar al proveedor responsable sería como considerar responsable al Correo por delitos perpetrados en las correspondencias privadas.

Por último, el tribunal sostuvo que tampoco podía responsabilizarse a la red social por los enlaces subidos por los usuarios, que redireccionaban a páginas con contenido violatorio de los derechos de autor.

e) Argentina:

• *S. M. y otro c/ JUJUY DIGITAL y/o JUJUY.COM s/daños y perjuicios- Cámara Civil y Comercial de Jujuy*

En 2004 una persona no identificada ingresó al sitio Jujuy.com y publicó un comentario donde hacía alusión a actos de adulterio por parte de uno de los integrantes de un matrimonio, a los cuales los identificaba con nombre y apellido. Frente a esta situación, la pareja demandó al titular del sitio por haber

[456] Tribunal Superior de Justicia Recurso Especial Nº 1512647/MG , ver análisis en inglés en https://cyberlaw.stanford.edu/blog/2015/06/brazilian-supreme-court-adopts-common-law-tests-intermediary-liability-copyright-case

permitido la publicación de dicho comentario. La Cámara Civil y Comercial de la Provincia de Jujuy dio la razón a los demandantes y de esta manera, responsabilizó a los administradores de la página web por los comentarios difamatorios que se realizaron en su plataforma[457]. Para ello, el tribunal sostuvo que al sitio debía aplicársele el sistema de responsabilidad objetiva, en virtud del riesgo de la cosa o de la actividad empresarial. Por otro lado, la Cámara estableció que la página web cumplió el papel de "editor o difusor" del comentario injurioso y por ende, podía ser responsabilizada por omisión, al no haber evitado la difusión del contenido ilícito. El extremo rigorismo del fallo se manifestó toda vez que el tribunal ni siquiera tomó en cuenta el hecho de que la página retiró los comentarios denunciados luego de que recibieran una carta documento por parte de los afectados.

- *S. M., M. S. c/ Yahoo de Argentina SRL y Google- Cámara Nacional de Apelaciones en lo Civil*

El beneficio económico también fue un argumento utilizado para avalar la postura objetiva. En el fallo "S. M., M. S. c/ Yahoo de Argentina SRL y Google"[458] del 2013 la Sala L de la Cámara Nacional de Apelaciones en lo Civil dictaminó que los buscadores eran responsables por los enlaces indexados, con base en la teoría del riesgo creado. El tribunal consideró que los servicios de búsqueda constituyen una actividad por medio de la cual las empresas que lo brindan obtienen enormes ganancias. Por lo tanto, deben reparar los daños ocasionados por la difusión de contenidos de terceros que ellos se encargan de propagar, máxime cuando disponen de la posibilidad técnica de establecer filtros para evitar la difusión de contenidos ilícitos.

- *Bluvol, Esteban Carlos c / Google Inc. y otros s/ daños y perjuicios- Cámara Civil de Apelaciones (Exp. N° 59.532/2009)*

En forma paralela, otra parte de la jurisprudencia comenzó a adoptar estándares más acordes con un sistema de responsabilidad subjetivo. En "Bluvol"[459] (2009), la sala H de la Cámara Civil considero que la responsabilidad de los buscadores no debe ser de carácter objetivo, ya que llevaría a considerarlos responsable siempre, sin importar su conducta. Por el contrario, el estándar a utilizar es el de responsabilidad por culpa, y lo que debe analizarse es si el buscador tuvo "conocimiento efectivo" del contenido ilegítimo y no lo removió de sus listas de

[457] Ver fallo en http://derechoinformaticoynuevastecnologias.blogspot.com.ar/2012/02/fallo-completo-del-caso-jujuycom.html
[458] Ver fallo en www.advaserver.com/a2/index.cfm?fuseaction...ext...

[459] Ver fallo en http://www.diariojudicial.com/nota/31816

búsqueda. A los fines de especificar el conocimiento, el tribunal estableció que es suficiente la notificación privada por parte del particular afectado.

• *Da Cunha, Virginia c. Yahoo de Argentina S.R.L. and Google Expte. Nº 99.620/2006 Cámara Nacional de Apelaciones en lo Civil de la Capital Federal*

Por otra parte, en "Da Cunha"[460] del 2010, la Sala D de la Cámara Nacional de Apelaciones en lo Civil de la Capital Federal determinó que los buscadores no deben ser juzgados en base a un modelo de responsabilidad objetiva basado en la teoría del riesgo creado, ya que "si bien (…) actúan proporcionando una herramienta al usuario que utiliza la computadora para localizar los contenidos o la información por él definida, dichos contenidos o información no son creados o puestos en la red o editados por los buscadores". Por lo tanto, la responsabilidad de los intermediarios debe ser considerada de carácter subjetivo y aquel que pretenda el resarcimiento debe demostrar la culpa o negligencia en que incurrió el buscador. El tribunal especificó que la responsabilidad solo puede hacerse efectiva contra los intermediarios en la medida en que "frente a una situación ilícita, y advertidas a través de los mecanismos pertinentes, no realicen la conducta atinente y necesaria para obtener la cesación de las actividades nocivas", pues, recién en ese momento, se configuraría una conducta susceptible de ser considerada como una falta. La Cámara resaltó que "con anterioridad a cualquier reclamo del afectado solicitando el bloqueo del contenido que considera agraviante y disponible en Internet a través de los buscadores demandados, no puede a los mismos serle atribuida o adjudicada culpa alguna por los contenidos cuestionados".

• *Sujarchuk, Ariel Bernardo C/ Warley Jorge Alberto s/daños y perjuicios*

El primer fallo que dictó la Corte Suprema en materia de libertad de expresión en Internet fue "Sujarchuk"[461] (2013). El señor Ariel Sujarchuk era subsecretario de la Universidad de Buenos Aires y demandó al periodista Jorge Warley por un artículo publicado en el blog "Desde el aula", que se titulaba "Noticias sobre la presencia del siniestro Ariel Sujarchuk en la UBA". En dicho documento se transcribían una serie de expresiones desfavorables a Sujarchuk realizadas por el gremio de la UBA.

Tanto en primera como en segunda instancia se dio la razón al demandante, con el argumento de que debía distinguirse entre "opinión" –la cual merece todo el

[460] Ver fallo en http://saberleyes.blogspot.com.ar/2010/08/da-cunha-virginia-v-yahoo-de-argentina.html

[461] Ver dictamen del Ministerio Público Fiscal –al cual se remitió la Corte Suprema- en http://www.mpf.gov.ar/dictamenes/2012/GWarcalde/junio/Sujarchuk_Ariel_Bernardo_S_755_L_XLVI.pdf

amparo de la garantía de la libertad de expresión- e "insulto" –el cual se sitúa fuera de la libertad de informar-. Los tribunales inferiores entendieron que la inclusión del término "siniestro" en el título constituía un insulto, que era susceptible de generar responsabilidad por lesión a la dignidad de la persona.

Sin embargo, el máximo tribunal va a revocar las sentencias y consagrará la irresponsabilidad del periodista. Para ello, va a remitirse al dictamen del Ministerio Público Fiscal, quien sostuvo que debía aplicarse al caso en cuestión, la doctrina establecida por la Corte Suprema en "Campillay". En este famoso caso, la Corte sostuvo que la reproducción de los dichos de otra persona no genera responsabilidad si se ha atribuido el contenido de la información a la fuente pertinente y se haya efectuado una transcripción fiel a lo manifestado por aquélla. De esta manera – sostiene el dictamen- la publicación de un documento ajeno se ajusta a lo establecido por la doctrina y por lo tanto, no puede traer aparejada responsabilidad alguna al periodista, quien sólo se limitó a publicarlo en el blog, mencionando en forma expresa la fuente de dónde provino.

Por otro lado, y en lo que respecta al calificativo "siniestro", el dictamen del fiscal llegó a la conclusión de que su uso no fue reflejo de un insulto, sino que sintetizó la opinión de un tercero. En ese sentido, aun cuando el título pudiera considerarse ofensivo para el demandante, su condición de funcionario público habilita a que se extreme la tolerancia en pos de la libertad de expresión.

El fallo resultó un valioso precedente, ya que estableció por primera vez que la garantía de la libertad de expresión se debe aplicar a todos los espacios donde pueda ejercerse, entre ellos, el ámbito digital. De esta manera, resolvió –en parte- la incertidumbre normativa en materia de regulación de medios de comunicación que operan en internet, al extender a aquéllos los mismos estándares y criterios que los tribunales utilizan para el análisis de casos que involucran a medios tradicionales.

Sin embargo, el alcance de la sentencia no alcanzaba a cubrir los casos de responsabilidad de otro tipo de intermediarios, tales como los buscadores. Para esto, habría que esperar al dictado del fallo "Belén Rodríguez".

- *Rodríguez, María Belén c/ Google Inc. y Otro s/ Daños y Perjuicios Expte. Nº 99.613/06*

La disparidad de criterios judiciales en materia de responsabilidad de los buscadores vino a ser resuelta por la Corte Suprema de Justicia de la Nación (CSJN) con el dictado del fallo "Belén Rodríguez" en 2014[462]. La señorita Rodríguez demandó a Google –y posteriormente a Yahoo- por el uso comercial y no autorizado de su imagen, y por violaciones a sus derechos personalísimos, al habérsela

[462] Ver fallo en http://www.telam.com.ar/advf/documentos/2014/10/544fd356a1da8.pdf

vinculado a determinadas páginas de Internet de contenido erótico y/o pornográfico. La demandante exigió una reparación monetaria y el cese de los vínculos referidos.

La Corte sostuvo claramente que la responsabilidad de los buscadores no puede ser juzgada con base a un modelo objetivo de responsabilidad, que prescinda de la idea de culpa. Para ello, citó la Declaración Conjunta sobre Libertad de Expresión e Internet, que sostiene que, como principio, nadie que ofrezca únicamente servicios técnicos de Internet deberá ser responsable por contenidos generados por terceros. Asimismo, el máximo tribunal consideró que un sistema objetivo haría mellar la libertad de expresión al desechar un juicio de reproche a aquel que se pretende endilgarle responsabilidad.

Sin embargo, el máximo tribunal se ocupó de aclarar que los buscadores no gozan de absoluta inmunidad. Ellos pueden ser declarados responsables cuando hayan tomado "efectivo conocimiento" de la ilicitud del contenido si tal conocimiento no fue seguido de un actuar diligente. En estos casos, quedará probado el actuar culposo del motor de búsqueda. Para determinar cuándo se considera que los buscadores tienen ese "conocimiento efectivo", la Corte hizo una distinción entre ilicitud manifiesta y no manifiesta. La primera se refiere a aquellos casos en que el daño es manifiesto y grosero. En esta hipótesis, bastará la mera comunicación fehaciente del damnificado o –según el caso- cualquier otra persona. La Corte hace la siguiente enumeración de contenidos considerados como manifiestamente dañosos: pornografía infantil, datos que faciliten la comisión de delitos, que instruyan acerca de éstos, que pongan en peligro la vida o la integridad física de alguna o muchas personas, que hagan apología del genocidio, del racismo o de otra discriminación con manifiesta perversidad o incitación a la violencia, que desbaraten o adviertan acerca de investigaciones judiciales en curso y que deban quedar secretas, como también los que importen lesiones contumeliosas al honor, montajes de imágenes notoriamente falsos o que, en forma clara e indiscutible, importen violaciones graves a la privacidad exhibiendo imágenes de actos que por su naturaleza deben ser incuestionablemente privados, aunque no sean necesariamente de contenido sexual.

Por otra parte, en el caso de las ilicitudes no manifiestas, cuyo contenido dañoso exija un esclarecimiento que deba debatirse o precisarse en sede judicial o administrativa para su efectiva determinación, no bastará la simple comunicación del particular sino que se requerirá notificación judicial o administrativa de autoridad competente.

Respecto al pedido de que los buscadores establezcan filtros para evitar búsquedas en el futuro, el tribunal sostuvo que es improcedente debido a que tiene una fuerte similitud a la censura previa. Por lo tanto, todo sistema de filtrado de contenido tiene una fuerte presunción de inconstitucionalidad y solo puede ceder frente a "supuestos absolutamente excepcionales", por ejemplo, para proteger la identidad de un menor.

Finalmente, y en relación a los thumbnails (versiones en miniaturas de imágenes que los buscadores utilizan para ayudar a su organización y reconocimiento) la Corte también estableció que los buscadores no son responsables por su uso, ya que no corresponde aplicar al "buscador de imágenes" y al de "textos" normas distintas, debido a que ambos “enlazan" a contenidos que no han creado.

La decisión de la Corte supuso un avance importante en materia de libertad de expresión, al establecer estándares altos para remover contenido en la red. La necesidad de exigir una orden judicial resulta acorde a los principios internacionales y la prohibición de establecer sistema de filtrados o bloqueos masivos garantiza que sólo se eliminará contenido que realmente afecte algún derecho, luego de una decisión judicial que así lo acredite. Sin embargo, algunas cuestiones suscitan mayores dudas. En primer lugar, la Corte dictaminó que existen casos en los cuales bastará una notificación privada. Si bien los supuestos constituyen una excepción a la regla general, la mayor parte están descriptos con tal grado de ambigüedad que podrían llegar a justificar soluciones contrarias a la garantía de la libertad de expresión. Por ejemplo, en caso de material presuntamente violatorio de derechos de propiedad intelectual, una interpretación de mala fe podría llegar a justificar la implantación de un sistema de “notice and takedown” con el argumento de que constituyen “datos que facilitan la comisión de delitos”.

Por otro lado, la expresión “manifiestamente ilegítimo” tiene una carga de profunda vaguedad, lo cual va en contra de la exigencia de que las regulaciones estén escritas con claridad y precisión. De esta forma, existe el peligro de que la indeterminación semántica dé lugar a que se incluyan dentro de la expresión más casos de los que realmente deberían encajar. En este sentido, debe tenerse en cuenta que lo “ilegítimo” resulta una noción que depende mucho de valoraciones y preferencias subjetivas, las cuales pueden dar lugar a una multiplicidad de interpretaciones perjudiciales para la garantía de la libertad de expresión.

Finalmente, se debe tener en cuenta que el voto de la minoría reconoció la eventual admisibilidad de una acción de tutela preventiva para eliminar enlaces existentes pero no identificados, y para evitar que en el futuro se produzcan enlaces a páginas lesivas de derechos personalísimos. La Corte argentina ya no cuenta con dos de los integrantes de la mayoría en Rodriguez vs Google (Zaffaroni y Fayt) y se desconoce la posición de quienes los reemplacen. El criterio asentado en “Rodríguez” sirvió para resolver varias causas de la misma índole que también estaban a la espera de ser resueltas por el máximo tribunal. Así, en “Da Cunha”[463]– cuyo fallo de Cámara fue mencionado anteriormente- y en “Lorenzo”[464] la CSJN

[463] Disponible en http://servicios.csjn.gov.ar/confal/ConsultaCompletaFallos.do?method=verDocumentos&id=718262
[464] Disponible en http://servicios.csjn.gov.ar/confal/ConsultaCompletaFallos.do?method=verDocumentos&id=718259

directamente se remitió a lo decidido en "Rodríguez" para resolver en favor de los intermediarios.

- *Kodama vs. Taringa- Cámara del Crimen*

Lo resuelto en "Belén Rodríguez" causó pronto impacto en la jurisprudencia argentina. La Sala I de la Cámara del Crimen confirmó el sobreseimiento, dictado en primera instancia, de los dueños del sitio "Taringa"[465], en el marco de una causa por defraudación iniciada por la señora María Kodama, heredera de los derechos de las obras del escritor Jorge Luis Borges. Para así decidir, los jueces extendieron el criterio establecido por la CSJN en el fallo "Rodríguez" a un servicio distinto a los motores de búsqueda, en este caso, los sitios que almacenan contenidos subidos por sus usuarios. Para ello, el tribunal afirmó que ambos son "intermediarios cuya única función es servir de enlace" del material subido. Asimismo, no existe "una obligación de verificar ex ante el material de intercambio sino posteriormente cuando este resulte denunciado". En este sentido, la Cámara valoró que Taringa removió el contenido una vez que fue notificado por la parte afectada. Por lo tanto, el tribunal afirmó que no se puede determinar la producción de un comportamiento delictuoso por parte de los denunciados.

Medidas cautelares contra buscadores por violación a derechos personalísimos:

La afectación de derechos personalísimos suele ser un motivo para justificar restricciones a la libertad de expresión. La difusión de imágenes, videos o noticias puede generar perjuicios a la honra o a la intimidad de las personas. Internet no ha hecho más que ampliar los efectos de tales lesiones, a través de la actividad de los buscadores. La difusión instantánea que puede alcanzar un contenido lesivo encontrado a través de los servicios de búsqueda ha provocado que los individuos que se consideran afectados recurran a medidas cautelares para ordenar a los intermediarios el bloqueo de los contenidos denunciados. En Argentina, numerosas celebridades y modelos han solicitado el dictado de medidas cautelares a su favor que ordenasen suspender, bloquear o dejar sin efecto cualquier vinculación efectuada por el buscador entre su nombre (o imagen) y páginas de contenido sexual, de acompañantes, tráfico de sexo o simplemente difamatorias. Si bien resulta atendible la protección de las personas afectadas, dicha tutela debe ejercerse de manera que no vulnere la libertad de expresión. Esta necesidad de balancear ambas garantías ha puesto a la jurisprudencia en la tarea de elaborar soluciones que resguarden los derechos de

[465] Disponible en http://www.diariojudicial.com/documentos/2015_Mayo/Taringa_Camara.pdf

los denunciantes pero sin establecer obligaciones en manos de los buscadores que los lleve a adoptar conductas que provocarían una mella en la libertad de expresión. A continuación, analizaremos el camino que la jurisprudencia argentina ha tomado en materia de medidas cautelares por afectaciones a derechos personalísimos.

- *Ceriscioli Lorena c. Yahoo Argentina y otro s/ medidas cautelares*

En un primer momento las solicitudes de remoción de contenido exigían que los buscadores eliminaran el vínculo a toda página que contuviera material lesivo a los derechos de la accionante. Parte de la jurisprudencia dio respuesta favorable al pedido y no requirió la individualización de los sitios que violaban los derechos de las personas afectadas. De esta manera, se dictaron medidas cautelares genéricas que establecían el deber de los buscadores de remover todos los sitios que puedan ser lesivos de la intimidad y el honor de las accionantes. Los fundamentos utilizados apuntaban a que los servicios de búsqueda son los que están en mejores condiciones de detectar los contenidos violatorios de derechos. Así, en "Ceriscioli Lorena"[466](2009) la sala I de la Cámara Nacional de Apelaciones en lo Civil y Comercial dijo que "no está suficientemente acreditada -en este estado- la imposibilidad de la apelante (Yahoo) de individualizar sitios del tipo cuestionado mediante el rastreo a través de expresiones genéricas utilizadas en esa clase de sitios, carga que no es razonable imponer a la actora, máxime cuando se relaciona con la actividad específica de la demandada. Frente a la posibilidad de que una medida genérica constituya un bloqueo preventivo, el tribunal rechazó tal afirmación y que lo que se busca es "hacer cesar las vinculaciones existentes que se produzcan a través de la utilización de su buscador."

- *Nara, Wanda c. Yahoo Argentina y otro s/ medidas cautelares*

Sin embargo, el peligro para libertad de expresión que conllevan las medidas genérica fue reconocido en "Nara"[467] (2010) donde se sostuvo que "la orden genérica de cesar toda vinculación con sitios que revistan determinadas características, aun cuando sea provisoria, comportaba cierta desmesura porque además de las dificultades que entraña el examen a priori y generalizado de todos los sitios relevados por las demandadas, una medida de esa índole resulta potencialmente lesiva de la libertad de expresión". Por otra

[466] Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala I, 11/06/2009, "Ceriscioli Paszkowicz Lorena Valeria c/ Yahoo de Argentina S.R.L. y otro s/ medidas cautelares", elDial.com - AF47AF

[467] Cámara Federal en lo Civil y Comercial Sala II , "Nara, Wanda Solange", causa n° 8.952/09

parte, el tribunal reconoció la regla imprescindible de examinar el contenido del sitio denunciado para calificar si es lesivo de algún derecho personalísimo. Por lo tanto, la jurisprudencia adoptó el criterio de exigir la individualización de los sitios lesivos, ya que es la medida que mejor se corresponde con la garantía de la libertad de expresión

- *Giovanetti, Laura c. Yahoo Argentina y otro s/ daños y perjuicios*

El estándar de individualización fue ratificado por los tribunales en Giovanetti"[468] (2015), donde se determinó que a los efectos de establecer el momento del "conocimiento efectivo" necesario para poder atribuir responsabilidad –de acuerdo al criterio del fallo "Rodríguez"- las medidas cautelares poseen "aptitud suficiente para determinar prima facie la ilicitud de los contenidos cuyos vínculos han sido expresamente identificados". Sin embargo, dicha medida no debe ser general, ya que no resulta admisible un retiro genérico de contenidos lesivos "sin individualizar de modo concreto los sitios que la actora considera lesivos para sus derechos personalísimos", debido a que "la protección expedida de manera genérica puede conducir a un bloqueo excesivo, sustrayendo información que interese a la comunidad y bloqueando el acceso a direcciones de contenidos lícitos". Además, iría en desmedro de garantías de raigambre constitucional, tales como la libertad de expresión, la prohibición de censura previa y el derecho al acceso a la información. Por último, un bloque genérico podría afectar "derechos de terceros", como los de aquellas personas homónimas, quienes en virtud de un bloqueo genérico "verían imposibilitadas sus posibilidades de difundir ideas y brindar información."

- *Albertario Claudia c. Yahoo Argentina y otro s/daños y perjuicios*

Sin embargo, aun cuando la solicitud haya sido realizada en forma genérica, los buscadores pueden ser responsabilizados si de otros elementos presentes en la demanda, se pueden individualizar los sitios que alojan contenidos lesivos. Esto fue decidido en "Albertario"[469] (2015), que al igual que el caso anterior, trataba sobre un pedido de eliminación de vínculos hacia páginas de contenido difamatorio.

La diferencia con "Giovanetti" residía en la forma que había sido planteada la pretensión. Mientras en el anterior fallo, la Cámara interviniente había reconocido que la actora había individualizado los sitios cuya vinculación

[468] Cámara Nacional de Apelaciones en lo Civil y Comercial Federal Sala II "Giovanetti, Laura c. Yahoo Argentina y otro"

[469] Cámara Nacional de Apelaciones en lo Civil y Comercial Federal- Sala II, 02/06/2015 "Albertario, Claudia c. Yahoo Argentina y otro s/ daños y perjuicios"

solicitaba sean eliminados, en “Albertario” se trataba de un pedido de bloqueo genérico. El tribunal ratificó el criterio jurisprudencial de que no basta un pedido genérico para generar responsabilidad, por lo cual pesa sobre la demandada “la necesidad de individualizar los sitios ofensivos a su persona”. Sin embargo, el tribunal afirmó que el presente caso no versaba sobre el cumplimiento de la medida cautelar ordenada, ya que al haber sido dictada en término genéricos, dicha resolución no era susceptible de generar responsabilidad en los buscadores. En cambio, lo que debía dilucidarse era “si las demandadas dieron cumplimiento al bloqueo de los sitios en concreto”. De esta manera, el tribunal tomó en cuenta el hecho de que si bien el objeto de la medida cautelar fue de carácter genérico, en la prueba documental acompañada por la actora figuraba el listado de sitios que contenían imágenes lesivas de los derechos de la señorita Albertario. Por lo tanto, los magistrados afirmaron que las empresas tuvieron conocimiento suficiente de los sitios individualizados cuando se dictó la medida cautelar genérica. En consecuencia, Google fue considerado responsable, ya que “no arbitró las medidas técnicas que tiene a su alcance para evitar la propagación del daño que aquellos contenidos generaron al honor, buen nombre y dignidad” de la afectada, los cuales fueron identificados al momento de la presentación de la demanda, aunque el pedido hubiera revestido carácter genérico.

En resumen, la jurisprudencia ha admitido que la tramitación y eventual notificación de medidas precautorias se considera válida, a los fines de cumplir con el requisito de notificación judicial. Sin embargo, no debe perderse de vista los peligros que un mal uso de esta figura procesal puede tener para la libertad de expresión. En primer lugar, existe el riesgo de que los efectos de las medidas cautelares se extiendan por largo tiempo, ante la demora en iniciar el juicio principal. En segundo lugar, una vez iniciado, los procesos judiciales suelen durar años hasta que se llegue a la sentencia final, máxime si en el medio hay apelaciones. Finalmente, no hay que olvidar que las medidas precautorias se dictan sin la intervención de la otra parte, con lo cual no se respeta el derecho de la otra parte a ser oído. Esta situación ha sido contemplada en los Principios de Manila, que han recomendado que antes de que se bloquee cualquier contenido debe darse al intermediario y al usuario la posibilidad de hacer escuchar su voz, salvo circunstancias excepcionales. Pero aun en este caso, debe hacerse una revisión post facto de la orden, tan pronto como sea posible.

Medidas cautelares y asuntos de interés público:

El peligro que una mala utilización de las medidas cautelares implica para la libertad de expresión resulta evidente en aquellos casos en que, bajo la excusa de presuntas afectaciones al honor, se pretende la censura de información que resulta de interés para el público. A continuación daremos cuenta de dos casos en

los que se privilegió el interés público, aunque pueda considerarse que también se afectó la reputación de las personas

- *Servini de Cubría, María c. Yahoo Argentina y otro s/medidas cautelares*

En "Servini de Cubría"[470] (2009) una jueza electoral había solicitado una medida genérica por la cual se ordenaba a los buscadores bloquear todo tipo de información referida a ella, así como también la publicación de imágenes, sin su consentimiento. La Cámara interviniente había otorgado medidas similares a actrices y modelos. Sin embargo, en este caso se apartó de su criterio, en consideración a la función y el carácter de los actos de la solicitante. El tribunal consideró que la situación de la magistrada no podía ser equiparable a la de modelos y artistas, ya que "sus actos en ejercicio de sus funciones despiertan interés en los medios de difusión y en la sociedad en general". Por lo tanto su carácter de funcionario público la expone "voluntariamente a un mayor riesgo de sufrir perjuicio por noticias difamatorias", ya que "el ejercicio de la libre crítica de los funcionarios por razón de actos de gobierno es una manifestación esencial de la libertad de prensa".

De esta manera, la Cámara extiende al ámbito digital la doctrina de que los funcionarios públicos deben tolerar un mayor escrutinio por parte de los medios de comunicación y la sociedad, el cual puede incluir noticias difamatorias que un privado no estaría obligado a soportar.

- *De Priete Yamila c. Google Inc. y otro s/medidas cautelares*

Además del carácter de la función de la persona, otro elemento a tener en cuenta es la trascendencia del hecho al cual puede ir acompañada la difusión de imágenes que, a primera vista, pueden constituir una afectación al derecho a la privacidad. En "De Priete"[471] (2015) la demandante solicitó el bloqueo de todo vínculo con páginas que publicasen fotografías sacadas de su Facebook, en el marco de la noticia sobre la muerte del fiscal Alberto Nisman. La Cámara rechazo la solicitud y utilizo dos argumentos para sustentar su decisión de no aplicar aquello que anteriormente había otorgado a actrices y modelos. En primer lugar, el tribunal consideró que al tratarse de un caso de notorio interés público, debía prevalecer el principio de "máxima divulgación de la información pública". Frente a

[470] Disponible en http://www.cij.gov.ar/nota-1563-Rechazan-un-pedido-de-Servini-de-Cubr-a- para-no-aparecer-en-Google-y-Yahoo.html

[471] Cámara Civil-Sala H "De Priete, Yamila c Google Inc. y otro s/medidas cautelares" 02/09/2015

ello, la prohibición de reproducir imágenes sin autorización debe ceder frente al interés general por tener acceso a dicha información.

En segundo lugar, el tribunal se cuestionó por los límites de la privacidad en el marco de una red social como Facebook, en donde justamente se trata de compartir imágenes y eventos para otras personas. Dentro de este ámbito, parece sugerir el tribunal, se debe ser más cauteloso a la hora de afirmar una violación a la privacidad, máxime cuando se trata de imágenes vinculadas a hechos de carácter público, como sucedió en este caso.

Medidas precautorias y derechos de propiedad intelectual:

- *CAPIF y otros c. The Pirate Bay s/medidas precautorias*

La defensa de derechos de propiedad intelectual también ha sido utilizada como excusa para responsabilizar a los intermediarios por supuestas infracciones cometidas por terceros. El caso más importante en materia de derechos de autor fue el bloqueo de The Pirate Bay (TPB)[472], la plataforma más conocida en todo el mundo para compartir archivos vía torrents. Frente a una solicitud de la Cámara Argentina de Productores de Fonogramas y Videogramas (CAPIF) institución que agrupa a las empresas discográficas y la Sociedad de Autores y Compositores de Música (SADAIC), el magistrado interviniente responsabilizó al sitio, ya que sostuvo que su rol no era el de un mero intermediario que cumple una función inocua. Por el contrario, según el juez, el sitio actuaba como un "facilitador de medios para que los usuarios puedan compartir y descargar gratuitamente archivos que contienen obras sin las respectivas autorizaciones de los autores", ya que "ofrece el ámbito, suministra herramientas y los incentivos para que tales múltiples y complejas infracciones se lleven al cabo por miles o millones de usuarios en otras tantas "entradas" al sitio, como un nodo necesario para ese tráfico de archivos digitales en violación del derecho de autor".

Por otra parte, el magistrado tomó en cuenta que TPB obtenía ganancias por ingresos derivado de publicidad, lucrando con un servicio que "provee el ámbito, índices y registros para la infracción de derechos intelectuales". De esta manera, se debe aplicar el principio de que quien lucra con una actividad debe afrontar los costos que se derivan de ella.

Por otro lado, el juez reconoció que en caso de colisión entre la libertad de expresión y el derecho de autor, debe prevalecer la primera. Sin embargo, niega que en este caso se presente tal choque, ya que no se puede considerar que el régimen de intercambio de bytes del P2P (forma en que opera el intercambio de archivos en TPB) tiene el rango de "información" amparado por la garantía de la

[472] Disponible en http://derechoaleer.org/media/files/tpb/232015119-CAPIF-CAMARA-ARG-DE-PRODUCTORES-DE-FONOGRAMAS-Y-OTROS-c-THE-PIRATE-BAY-s-MEDIDAS-PRECAUTORIAS.pdf

libertad de expresión. Asimismo, el magistrado adujo que las redes P2P pueden lesionar la libertad de expresión, ya que debilitan financieramente las editoriales y desalientan el trabajo de autores o periodistas, artífices del intercambio de ideas e información constitutivos de aquella garantía.

En consecuencia, el magistrado ordenó a los proveedores de servicios de internet que bloqueen el acceso desde Argentina a las direcciones IP que opera TPB expuestas en la demanda. Además, se ordenó el bloqueo de todos los DNS conocidos actualmente que fueron adoptados por el sitio. Sin embargo, se debe destacar que el magistrado decidió no ordenar a los buscadores que bloqueen de sus resultados cualquier término de búsqueda relacionado con The Pirate Bay, porque consideró que de esta manera se lo "invisibilizaba". Asimismo, se rechazó el pedido de CAPIF de ser la encargada de determinar, de tanto en tanto, cuáles son las direcciones IP o DNS que deban bloquearse del sitio TPB, e instruir en ese sentido a los proveedores de servicios de internet. El fundamento fue que dicha autorización equivaldría a que tal entidad se arrogue "funciones de virtual censor que no tiene ni puede conferírsele". Por lo tanto, si surgieran nuevas IP o DNS ajenas a las mencionadas en la demanda, los accionantes deberán acreditar su vinculación a TPB en el procedimiento de ejecución de sentencia.

El fallo resulta ampliamente cuestionable por diversas razones. En primer lugar, resulta desproporcionado, ya que el bloqueo del sitio impide que las personas puedan acceder a obras cuya descarga está permitida, como aquellas cuyo autor ha autorizado su intercambio, contenidos con licencia "Creative Commons" entre otros. Si el magistrado pretendía proteger las descargas ilícitas, tendría que haber bloqueado los enlaces que únicamente apuntaban a obras sobra las que se presume infracción.

En segundo lugar, la medida constituye un ejemplo de censura previa que está prohibido por los principios internacionales que protegen la garantía de la libertad de expresión, ya que impide a los individuos el acceso a una amplia gama de información que puede ser relevante para el interés público.

Finalmente, la medida resulta poco eficaz desde el punto de vista técnico, ya que existen medios para burlar la sentencia, a través de la creación de otros sitios y enlaces que logran evadir el bloqueo y redireccionar a la misma página.

Responsabilidad de los intermediarios por infracciones a derechos marcarios

Las infracciones al derecho de autor no son el único ejemplo que se han presentado en materia de derechos de propiedad intelectual. La comercialización de productos a través de sitios electrónicos ha dado lugar a reclamos empresarios por las violaciones a los derechos marcarios que podrían incurrir algunos de los oferentes que actúan dentro de dichas plataformas. Claro está que los reclamos de las empresas no se dirigen a los usuarios sino a los sitios que

ofrecen servicios de intermediación.

En principio, la problemática de las infracciones marcarias plantea cuestiones que no atañen directamente a la libertad de expresión. En ese sentido, la inclusión en este informe de jurisprudencia referida a la temática puede resultar excesiva. Sin embargo, entendemos que es necesario dar cuenta de lo resuelto por los tribunales, ya que en definitiva se trata de sentencias que se refieren a la responsabilidad de intermediarios –en este caso plataformas comerciales- por contenido de terceros – ofertas comerciales-, las cuales pueden servirnos para pensar aquellos casos en los cuales sí está en juego la defensa de la libertad de expresión.

La jurisprudencia argentina se ha pronunciado sobre las infracciones marcarias en dos recientes fallos sobre reclamos de la empresa Nike.

- *Nike International LTD c. De Remate.com s/cese de uso de marcas y daños y perjuicios*

El primero de ellos fue dirigido contra el sitio DeRemate.com[473] y versaba sobre la violación de un convenio suscripto entre ambas partes, por el cual la demandada se comprometía a utilizar todos los medios tecnológicos y humanos disponibles para evitar que en su sitio se comercialicen artículos que sean ilegales o infrinjan de alguna manera los derechos de propiedad marcaria de Nike. La empresa solicitó que DeRemate.com cese de comercializar productos que lleven la marca Nike y les brinde los datos identificatorios de las personas que comercializan productos "truchos" de la marca para poder iniciar las acciones legales correspondientes.

A los fines de determinar la responsabilidad de la demandada por violaciones al derecho de marcas por parte de terceros, la Cámara analizó si los servicios de intermediación prestados por aquella revestían carácter "pasivo o neutral". El tribunal tuvo en cuenta que DeRemate.com había contratado el servicio de enlaces patrocinados con Google, por el cual cada vez que una persona ingresaba las keywords "zapatillas Nike" en su buscador, el sitio aparecía a la cabeza de la lista de resultados. De esta manera, los magistrados sostuvieron que la accionada había utilizado la marca Nike con "finalidad comercial para captar clientela para operar e interactuar en su propia plataforma on line". Por lo tanto, la contratación de estos servicios "revela una conducta de la demandada que beneficia a los anunciantes de su plataforma" ya que "su conducta optimiza las posibilidades de los oferentes y conlleva un mayor lucro por el posicionamiento de un mayor número de ofertas." De esta manera, la accionada habría incurrido en una infracción marcaria, que consiste en captación de clientela

[473] CAUSA N° 2060/2008 – S.I. – NIKE INTERNATIONAL LTD. C/DEREMATE COM DE ARGENTINA S.A. S/CESE DE USO DE MARCAS. DAÑOS Y PERJUICIOS

para el propio servicio, confusión del consumidor y dilución de marca notoria ajena.

Por otra parte, los magistrados remarcaron que la demandada proporcionaba “un servicio de pago on line, que presta asistencia en ocasión de la concreción de las operaciones.”, con lo cual el sitio obtenía un beneficio económico de la actividad comercial desplegada por los terceros que interactuaban en su plataforma.

En base a estos dos hechos, la Cámara concluyó que DeRemate.com había cumplido un papel activo en la realización de las operaciones, y en consecuencia, debía ser responsabilizado por las infracciones propias y de las ajenas por operaciones de terceros.

Además de establecer el estándar del “papel activo”, el tribunal sostuvo que puede existir otro caso más en el que los servicios de intermediación comercial puedan ser responsabilizados: “cuando hubieran tenido conocimiento efectivo de la actividad ilícita de un tercero (es decir, del carácter presuntamente ilícito de las ofertas de venta o subasta de sus clientes registrados) y no hubiese actuado con prontitud”.

Respecto al pedido de entrega de los datos de los presuntos infractores, el tribunal sostuvo que Nike tenía derecho a dicha solicitud, debido a “su interés legítimo a defender la competencia leal en el mercado argentino, sea real o virtual” para así poder denunciarlos ante los organismos públicos competentes.

Luego de determinada su responsabilidad, el Tribunal estableció los deberes a cumplir por la demandada:

1- En primer lugar, se rechazó el pedido de la demandante de que cese toda aparición de sus marcas "Nike" y toda comercialización de productos identificados con tales marcas en la plataforma, ya que “se trata de un sistema de comercialización dinámico que incluye transacciones lícitas”, las cuales no pueden ser prohibidas. En su lugar, se ordenó a la demandada dar de baja las ofertas de productos presuntamente en infracción de los derechos de la actora, dentro de las 24 horas de recibida la notificación fehaciente –por parte de la empresa- de la aparición de esa oferta en infracción.

2- DeRemate.com deberá comunicar a Nike los datos completos de identificación de los infractores, los cuales deberá haber registrado al tiempo de la inscripción del usuario en falta, y los mantendrá por un plazo de tres años.

3. La demandada deberá dejar de contratar servicios de enlaces patrocinados que utilicen las marcas de la actora.

- *Nike International LTD v. Compañía de Medios Digitales s/cese de uso de marcas*

La figura de “prestador activo” también fue utilizada en la demanda contra Compañía de Medios Digitales[474], administradora del sitio masoportunidades.com. A diferencia del caso anterior, en esta oportunidad no existía un acuerdo previo que obligara a la plataforma a adoptar un sistema de filtros. Es por ello que la sentencia debe ser analizada con más cuidado, ya que sus efectos pueden ser expandidos a futuros casos.

En su resolución, la Cámara interviniente entendió que la plataforma cumplía un papel activo en las operaciones realizadas en su sitio, ya que “brindaba a sus clientes la posibilidad de potenciar las ofertas de venta y/o promoverlas mediante el abono de un plus”, situación que le brindaba “la posibilidad cierta de acceder a un mejor control de los datos”. De esta manera, la demandada era responsable por “no haber tomado las medidas idóneas que evitaran que en su sitio se vendieran productos que infringieran los derechos marcarios de la actora, cuando tales medios existen y son posibles de implementar sin obstaculizar la comercialización por medios electrónicos”.

Respecto a la solicitud de entrega de los datos identificatorios de los potenciales infractores, la Cámara sostuvo “que el ordenamiento jurídico debe habilitar la persecución del autor de la infracción, siendo insuficiente una práctica comercial que no asegure al consumidor y todo tercero portador de un interés legítimo (…) la posibilidad de conocer el nombre completo, inscripción registral en caso de ser persona jurídica, domicilio y dirección electrónica, número de telefónico y de identificación fiscal -CUIT o CUIL-, del presunto infractor”. Por lo tanto, se estableció el derecho de Nike a disponer de esa información para proceder a las acciones legales correspondientes.

No obstante, el tribunal rechazó la pretensión de la actora de ordenar el cese de toda aparición de sus marcas "Nike" y de toda comercialización de productos identificados con tales marcas en la plataforma de la demandada, ya que ésta también puede incluir transacciones lícitas (ej.: reventa de productos usados). En cambio, ordenó a masoportunidades.com que establezca un sistema de filtros para eliminar anuncios y ofertas que ostensiblemente sean violatorios del derecho marcario de Nike. La carga de notificar los avisos conflictivos queda en manos de Nike, y la demandada deberá eliminar el contenido lesivo dentro de las 24 horas de recibida la denuncia. Asimismo, y de manera inmediata al “alerta de infracción”, masoportunidades.com deberá comunicar a la actora los datos completos de identificación (esto es, nombre completo, inscripción registral en caso de ser persona jurídica, domicilio y dirección electrónica, número telefónico y de identificación fiscal, CUIT o CUIL del presunto infractor) que el sitio deberá registrar

[474] Causa N°3239/2007 “Nike International Ltd c/ Compañía de Medios Digitales CMD SA s/ Cese de uso de marcas”. Juzgado N°1, Secretaría N°2.

al tiempo de la inscripción del usuario/vendedor, los cuales permanecerán en los registros por el plazo de tres años. Por último, la plataforma deberá advertir a los usuarios que suban anuncios de productos que lleven la marca “Nike” de que sus datos podrán ser comunicados a la empresa titular de las marcas y que eventualmente podrá ser pasible de sanciones.

6. Conclusiones finales y recomendaciones:

En general, nuestra región se caracteriza por la ausencia de legislación específica sobre la materia. La mayoría de los países latinoamericanos no dispone de normativa sobre responsabilidad de los intermediarios. Y en aquellos donde sí existen tales disposiciones, su campo de aplicación no es total. Por ejemplo, en Chile y Costa Rica, pioneros en la sanción de normas sobre la materia, su legislación únicamente regula los casos de violaciones a derechos de autor. Incluso Brasil, que con su Marco Civil pretendía regular la totalidad de los derechos de los ciudadanos en la red, expresamente excluyó de su ámbito de aplicación a las infracciones de derechos de autor.

Respecto a la regulación existente, se puede afirmar que se han dado pasos para adoptar los estándares recomendados. En este sentido, el modelo de responsabilidad subjetiva a través de notificación judicial ha sido el adoptado por la legislación, tal como recomiendan el informe de 2013 de la RELE y los Principios de Manila. Sin embargo, persisten numerosas cuestiones que es necesario revisar. Entre ellas, figura la necesidad de ampliar la regulación normativa a los casos no alcanzados y la consagración normativa de ciertos deberes de transparencia, como la obligación de gobiernos e intermediarios de publicar informes que den cuenta –en el primer caso- de los requerimientos de restricción de contenido, y –en el segundo- de las restricciones adoptadas.

Los tratados de libre comercio celebrados por muchos estados latinoamericanos con EEUU han sido utilizados como excusa para instalar mecanismos de protección de derechos de autor contrarios a la garantía de la libertad de expresión, bajo el argumento de cumplir con obligaciones internacionales. El ejemplo de Chile y Costa Rica demuestra que la firma de tales acuerdos no es un obstáculo para instituir sistemas más protectorios de los derechos humanos.

En materia de proyectos de ley, la situación resulta más preocupante. La mayoría de las propuestas buscan instalar sistemas de notificación extrajudicial, que pueden dar lugar a situaciones de censura privada. Sin embargo, hasta el momento tales proyectos no han podido ser transformados en leyes, en parte debido a las posibles afectaciones que planteaban al ejercicio de los derechos humanos.

Finalmente, la jurisprudencia ha adoptado una actitud oscilante, sobre todo en aquellos países que todavía no cuentan con legislación específica. En general, la mayoría de las sentencias judiciales han rechazado aplicar sistemas de responsabilidad objetiva a los intermediarios. Los tribunales han establecido que debe mediar una notificación para que nazca la responsabilidad. Al momento de determinar el carácter de dicha notificación, la jurisprudencia de los países latinoamericanos ha respaldado, en general, la notificación judicial como el medio idóneo de comunicación, descartando la validez de notificaciones privadas. Sin embargo, aún persisten muchas zonas oscuras. En primer lugar, todavía existen fallos que para ciertos supuestos -en particular infracciones a derechos de autor - establecen sistemas de notificación privada contrarios a los estándares internacionales de derechos humanos. En segundo lugar, los criterios establecidos para determinar cuándo recurrir a un sistema de notificación privado adolecen de una extrema vaguedad, con lo cual se corre el riesgo de incluir una gran cantidad de casos que no deberían estar allí. En tercer lugar, la aparición de pedidos de remoción de contenido basados en un supuesto "derecho al olvido" amenaza con poner en riesgo la garantía de la libertad de expresión, en especial debido a la acogida favorable con que fue recibido en algunas jurisdicciones. Finalmente, el recurso a una medida precautoria judicial sin intervención del usuario o del intermediario, como medio idóneo para cumplir con el requisito de notificación judicial, plantea dudas respecto a las garantías de defensa de aquel que subió el contenido o del propio intermediario.

En ese sentido, creemos necesario hacer las siguientes recomendaciones para que los ordenamientos jurídicos de los países del sistema interamericano se ajusten a lo establecido por los estándares internacionales de derechos humanos.

- En aquellos países que aún no cuentan con normativa específica, se debería sancionar legislación que proteja la actividad de los intermediarios.
- Los intermediarios no deberían ser considerados responsables por contenido producido por terceros.
- No deben adoptarse sistemas de responsabilidad objetiva para juzgar la actuación de los intermediarios.
- Los intermediarios no deben monitorear o vigilar el contenido que circula en la red.
- Todas las restricciones de contenidos deben hacerse mediante orden emitida por una autoridad judicial independiente e imparcial.
- Las órdenes judiciales que restrinjan contenido deben especificar claramente el material violatorio, no admitiéndose órdenes genéricas de bloqueo. Asimismo, deben respetar los requisitos de necesidad y proporcionalidad
- Los supuestos en los cuales procede el bloqueo de contenido deben ser de carácter excepcional, a fin de no afectar la garantía de la libertad de

expresión.

- La legislación debería estar redactada en términos claros y precisos, para no dar lugar a interpretaciones restrictivas de la libertad de expresión.
- Las prácticas de restricción de contenidos deben respetar la garantía del debido proceso. Los efectos de las medidas precautorias deberían estar limitados temporalmente, e inmediatamente se debería garantizar el derecho de los usuarios e intermediarios a ser escuchados, antes de tomar cualquier decisión definitiva.
- Los gobiernos deben publicar informes de transparencia, que aporten información acerca de los requerimientos efectuados por ellos ante los intermediarios.
- Los intermediarios deberían publicar sus propios informes de transparencia, que den cuenta de todas las restricciones de contenido adoptadas.

por los Derechos Civiles