Fundación Karisma

Bogotá D.C., mayo 31 de 2021

Comisión de Regulación de Comunicaciones
Sergio Martínez
Director

Ref: Comentarios al proyecto de actualización de la Decisión 638 - "Lineamientos para la protección de los derechos de los usuarios de servicios de telecomunicaciones y de las tecnologías de la información y las comunicaciones (TIC) de la Comisión de la Comunidad Andina

Cordial saludo,

La Fundación Karisma se permite, de manera atenta, presentar los siguientes comentarios sobre el documento "Lineamientos para la Protección de los Derechos de los Usuarios de Servicios de Telecomunicaciones y de las Tecnologías de la Información y las Comunicaciones (TIC)"

La Fundación Karisma es una organización de la sociedad civil colombiana que busca "garantizar la protección y promoción de los derechos humanos y la justicia social en relación con el diseño y uso de las tecnologías digitales. Para este fin, aportamos importantes habilidades interdisciplinarias técnicas, analíticas y de incidencia, además trabajamos en estrecha colaboración con otros".

En concreto presentamos comentarios sobre el contenido de los artículos 3, 6, 8, 11 y 12

Quedamos a su disposición para ampliar el contenido de los comentarios que se adjuntan a continuación.

Atentamente,

Carolina Botero
Fundación Karisma
Directora

Fundación Karisma

***

Comentarios generales

Consideramos esta actualización como un proceso positivo para avanzar en el reconocimiento de un más amplio conjunto de garantías que protejan los derechos de las personas usuarias de los servicios de telecomunicaciones en la región andina, así como una oportunidad igualmente provechosa para la actualización del régimen de obligaciones a cargo de las empresas proveedoras del servicio de internet en la región que pueda incluir buenas prácticas con un carácter vinculante.

En este proceso, creemos que es importante poder considerar los resultados de los informes de distintas organizaciones de la sociedad civil de los países de la CAN así como organizaciones internacionales que evalúan, entre otros, las prácticas y compromisos en materia de protección de datos, libertad de expresión, acceso a la información y transparencia de las empresas proveedoras del servicio de internet.

Informes de este tipo sobre países miembros de la Comunidad Andina han sido efectuados por Hiperderecho en el caso de Perú con el informe "¿Quién defiende tus datos?"[1], y por Fundación Karisma en el caso de Colombia con el informe "¿Dónde están mis datos?"[2].

Además, es importante considerar también el contenido de los informes que organizaciones internacionales que miden dichos compromisos en proveedores del servicio de internet que operan a nivel internacional (incluyendo a América Móvil y Telefónica, por ejemplo) entre los que se incluyen el texto titulado "Who has your back?"[3] de la Electronic Frontier Foundation y el "Corporate Accountability Index"[4] de Ranking Digital Rights.

[1] Hiperderecho (2020) Quién defiende tus datos. Disponible en: https://hiperderecho.org/2020/11/presentamos-el-reporte-quien-defiende-tus-datos-qdtd-peru-2020/
[2] Fundación Karisma (2021). ¿Dónde están mis datos?. Disponible en: https://web.karisma.org.co/donde-estan-mis-datos-2020/
[3] Electronic Frontier Foundation (2019). Who has your back?. Disponible en: https://www.eff.org/es/pages/acerca-de-eff
[4] Ranking Digital Rights (2020). The Corporate Accountability Index. Disponible en: https://rankingdigitalrights.org/index2020/

Fundación Karisma

***

Comentarios específicos

Artículo 3. Derecho a la protección de datos

La redacción de este artículo es relevante en tanto que afirma deberes importantes asociados a la protección de datos y que tienen a su cargo los proveedores del servicio de internet. Creemos que su redacción puede ser ampliada considerando los hallazgos sobre las buenas prácticas que pueden o han desarrollado algunos proveedores del servicio de internet en la región y que han sido identificadas por Karisma, Hiperderecho y Ranking Digital Rights.

- *Debe poder requerirse a los proveedores del servicio de internet que las políticas de tratamiento de datos y avisos en privacidad sean comprensibles y accesibles para las personas usuarias de los proveedores del servicio de internet*

En su informe, tanto Fundación Karisma como Hiperderecho destacan la importancia de que las políticas de tratamiento de datos y avisos de privacidad de los proveedores del servicio de internet puedan ser comprensibles para sus usuarios y suscriptores. En ambos países se detalla cómo la redacción de dichos documentos que calcan el contenido de la ley puede constituir un obstáculo para las personas que ejercen sus derechos.

- *Debe poder requerirse a los proveedores del servicio de internet que las personas sean informadas sobre qué datos personales se recolectan y por cuánto tiempo son retenidos*

Si bien el proyecto de artículo en su numeral primero advierte que debe informarse a los usuarios de los proveedores del servicio de internet "de manera previa, clara y exacta del titular y domicilio del banco de datos o del responsable del tratamiento, de la existencia del banco de datos donde se almacenarán, de los tipos de datos o conjunto de datos que serán tratados, así como de la finalidad específica y la duración del tratamiento", creemos que es importante que se enfatice en la necesidad de que se desagreguen los tipos de información que son objeto de tratamiento.

En su informe anual, la Fundación Karisma identificó cómo la mayoría de proveedores del servicio de internet en Colombia advierten a los usuarios, en términos generales, que recogen o recolectan "datos personales" y tan solo un par de proveedores ha adoptado la buena práctica de informarle a la persona usuaria de sus servicios qué datos son esos: si se asocian a su nombre, dirección de domicilio, IP, si recogen datos personales a través de cookies, datos sensibles y de qué tipo, sobre consumo y facturación, metadatos y de qué tipo, entre otros.

Fundación Karisma

Creemos que esta es una modificación que vale la pena ser incluida en este proyecto de artículo, y que debe poder ser complementado con la aclaración de que los proveedores del servicio de internet tienen que informar sobre el tiempo preciso asociado al tratamiento de esos datos, así como los tiempos de la retención de aquellos otros que las legislaciones de cada país les encarga a los proveedores del servicio de internet y comunicaciones, el tiempo durante el cual los datos deben estar almacenados en caso de ser necesarios para eventuales investigaciones judiciales o incluso de inteligencia -según la ley-.

- *Debe poder requerirse a los proveedores del servicio de internet que se informe a las personas sobre qué terceros tienen acceso a sus datos personales y bajo qué circunstancias*

En su informe anual, la Fundación Karisma dio cuenta cómo algunos proveedores del servicio de internet en el país habían adoptado como buena práctica en la compartición de los datos de sus suscriptores con terceras partes, que éstas contaran con políticas y prácticas similares como garantía para las personas cuyos datos estaban siendo accedidos por estas terceras partes. Creemos que es una buena práctica que merece recepción o eco en el contenido de este artículo.

Así mismo, Ranking Digital Rights sugiere que tratándose de la recolección de datos por terceras partes, los proveedores del servicio de internet deben igualmente estar obligados a informar a las personas que suscriben sus servicios de qué otras fuentes de información, sean públicas o privadas, recogen datos sobre sus usuarios o clientes, para qué fin y por cuánto tiempo[5].

- *Entre los principios del tratamiento de datos debe poder incluirse el de minimización*

Según la Organización de las Naciones Unidas el principio de minimización de los datos tiene que ver con:

> "The amount of data, including its granularity, [meaning that data] ***should be limited to the minimum necessary. Data use should be monitored to ensure that it does not exceed the legitimate needs of its use*** (...) ***data should be permanently deleted upon***

[5] Este es un deber que ya ha sido implementado en el marco jurídico de Chile, puede verse al respecto el informe de "¿Quién defiende tus datos?" de Derechos Digitales. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/QDTD-2021.pdf

> ***conclusion of the time period needed to fulfill its purpose***"[6] (subrayado fuera de texto)

El principio de minimización deriva su existencia, según la Organización para la Cooperación y el Desarrollo Económicos (OCDE), del consenso existente en la legislación de las economías más avanzadas e instrumentos regionales e internacionales nacidos a partir de 1970, y que refieren al principio de minimización como una buena práctica en el tratamiento de datos personales. En el documento "Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)" publicado en 2013, se refirió a dicho principio como aquel según el cual el procesamiento de datos personales "should be relevant to the purposes for which they are used, an, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."[7].

El principio de minimización ha sido incluido en diversos reportes del Relator Especial para la Privacidad[8] de Naciones Unidas y el Relator Especial para la promoción y protección de los derechos humanos y la protección de las libertades fundamentales en la lucha contra el terrorismo[9] y se lo ha mencionado al menos por este último como una buena práctica que debe estar presente de manera transversal en el tratamiento de datos a cargo del responsable, sea el Estado o entidades privadas.

En Europa, el Grupo de Trabajo del artículo 29 para la protección de datos, ha señalado con relación a este principio que constituye una salvaguarda en eventos en los que grandes cantidades de datos más allá de lo necesario son procesadas y almacenadas para eventos que puedan llegar a ser usados en el futuro, y que su puesta en práctica obliga a los responsables en el tratamiento de los datos personales a explicar y justificar la necesidad de recoger y retener datos personales, debiendo limitando su uso a fines específicos a tiempos de almacenamiento fijos[10]. En el mismo texto, el Grupo de Trabajo reconoció que la fijación de un tiempo de almacenamiento estaba directamente vinculado al principio de minimización de

---

[6] United Nations Development Group, "Data privacy, ethics and protection: guidance note on big data for achievement of the 2030 agenda", disponible en: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf

[7] OECD, (2013), Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines), disponible en: https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

[8] Report of the Special Rapporteur on the right to privacy, "Right to privacy", A/HRC/40/63, 2019, disponible en: https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf (ver anexos "Draft recommendation on the data protection and the use of health data")

[9] Asamblea General Naciones Unidas (2009). Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Disponible en: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

[10] Data Protection Working Party Article 29, "Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679", adopted on 6 february 2018, WP251rev.01, disponible en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

los datos, y en su Opinión 03/2017 interpretando entre otros el artículo 11 del Reglamento General de Protección de Datos reiteró la importancia del principio de minimización pues permite mitigar riesgos asociados al tratamiento indebido de los datos[11].

La Convención europea n. 108 "Convention for the protection of individuals with regard to automatic processing of personal data" de 1981 y actualizada en 2018, prevé la minimización de los datos en el artículo 5 (4) lit. c, señalando que "[p]ersonal data undergoing processing shall be adequate, relevant and not excessive in relation to the purposes for which they are processed."[12]. Procesar datos que no sean excesivos "not excessive" tiene que ver en concreto, según esta Convención, a que el procesamiento de los datos se limite a lo que resulta necesario para el propósito que motivó el tratamiento.

Los datos personales según la minimización, deben ser procesados sí y solo sí otro tipo de datos - *los no personales*- no permitían lograr el objetivo que motivaba el tratamiento. La minimización no solo se relaciona al aspecto *cantidad* -tan pocos datos personales como sea posible y necesario procesar-, sino al aspecto *calidad*. Este principio es orientador sobre todo en los casos en que los datos pueden parecer adecuados y relevantes para el logro de una finalidad, pero su uso puede resultar desproporcionado por la injerencia que plantea para el ejercicio libre de derechos fundamentales. Considerar dicho principio como una buena práctica en el tratamiento de datos permite alertar sobre situaciones en las que debe detenerse el procesamiento de datos personales por ser considerado "excesivo".

Por su parte, el Reglamento General para la Protección de Datos (GDPR por sus siglas en inglés), en el artículo 5 (1), lit. c., consagró el principio de minimización así "[p]ersonal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[13], una vez más se enfatiza en aspectos como la relevancia, la adecuación, la limitación y la finalidad en el tratamiento.

La autoridad europea de protección de datos (European Data Protection Board) ha indicado por su parte, con relación la minimización de datos, que:

---

[11] Data Protection Working Party Article 29, "Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)", wp252, disponible en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

[12] Council of Europe,(2018), "Convention for the protection of individuals with regard to automatic processing of personal data", disponible en : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

[13]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

> "Only personal data that is adequate, relevant and limited to what is **necessary** for the purpose shall be processed. As a result, the controller has to predetermine which features and parameters of processing systems and their supporting functions are permissible. Data minimisation substantiates and operationalised the principle of necessity. In the further processing, the controller should periodically consider whether processed personal data still is adequate, relevant and necessary, or if the data shall be deleted or anonymized.
>
> Controllers must first of all determine whether they even need to process personal data for their relevant purposes. They should verify whether technology, processes or procedures exist that could make the need to process personal data obsolete. Such verification could take place, in a particular point of the processing activity or even throughout the processing lifecycle."[14]

Desde una visión mucho más comprensiva de la privacidad como algo que supera los límites de la protección de datos, la reconocida ONG Privacy International[15], expresó por su parte que este es un principio que dispone que en el tratamiento se procese la mínima cantidad de datos que sean *necesarios* y *relevantes* para el propósito declarado. La *necesidad*, debiendo ser entendida como la condición según la cual los datos recogidos o accedidos, no pueden tener un alcance distinto a la finalidad o propósitos para los cuales han sido procesados, para lo cual existe un test que permite orientar si la necesidad es tal o no respondiendo a la pregunta ¿es la no recolección reducida de información la práctica menos intrusiva para lograr un propósito legítimo?. La *relevancia* en cambio, se refiere a la relación estrecha que guarda el procesamiento de un dato para la satisfacción de un fin particular, y que responde a la pregunta ¿para qué fin en específico se procesa este dato en concreto?

La importancia de la aplicación del principio de minimización, según Privacy International, es hoy más prioritaria que nunca en tiempos en que la era del *big data* facilita el tratamiento masivo de información que puede no ser necesaria para el logro de un fin concreto y que termina en últimas siendo procesada, sin importar quién sea su controlador -público o privado-, cruzando grandes cantidades de datos sin conocimiento de su titular, y que puede orientar la toma de decisiones que le afectan sin que éste, en principio, haya sido advertido, notificado o informado de su procesamiento.

---

[14] European data Protection Board, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, adopted on 13 november 2019, pg. 19, prr 68, 69, disponible en: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

[15] Privacy International, (2018), "The Keys to Data Protection", disponible en: https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

En su redacción, el artículo tercero reitera como principios orientadores los de licitud, legitimidad, transparencia, finalidad, proporcionalidad, calidad, seguridad, confidencialidad y responsabilidad demostrada. En su informe, Ranking Digital Rights sugiere la importancia de que la recolección de datos por los proveedores del servicio de internet se oriente también bajo el principio de minimización según el cual solo debe poder ser recolectada la cantidad mínima de datos personales necesaria para la realización o logro de una finalidad específica, pero además, que en la recolección se valoren las alternativas de datos que permiten el logro de una misma finalidad para que se capturen y traten los de naturaleza menos invasiva o sensible frente a la privacidad de la persona.

En esta misma línea, Access Now, organización internacional no gubernamental, en su texto "Recommendations on Privacy and Data Protection in the fight against COVI-19" recientemente publicado, reiteró que los gobiernos y compañías debían aplicar los principios de protección de datos y privacidad entre los que se incluye el de "purpose limitation and data minimisation" señalando que "[d]ata collection, use, sharing storage, and other processing of health data should be limited to what is strictly necessary for the fight against the virus. A pandemic is no excuse to collect extensive and unnecessary data."[16]

Otra organización igualmente reconocida como la Electronic Frontier Foundation, reiteró por su parte la necesidad de que en el tratamiento de los datos adelantado por los gobiernos para hacer frente a la pandemia actual, se apliquen los principios de protección de datos que constituyen una garantía para el ejercicio de la privacidad de las personas que, en una situación de emergencia, difícilmente podrán oponerse al manejo de su información por parte de terceros especialmente cuando éste sea el Estado. El principio de minimización que también puede ser leído en la clave de los principios de necesidad y proporcionalidad que orientan al limitación de los derechos fundamentales, preceptúa que solo si resulta necesario para satisfacer un fin concreto, se debe proceder al tratamiento de la menor cantidad de datos posibles[17].

Artículo 6. Privacidad e intimidad

Creemos que es importante el contenido de esta disposición que aboga por establecer una prohibición general de interceptación de las comunicaciones u otros tipos de vigilancia de

[16] Access Now, (2020), Recommendations on Privacy and Data Protection in the Fight against COVID-19", disponible en: https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf
[17] Electronic Frontier Foundation (2020), "Protecting civil liberties during a public health crisis", disponible en: https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis

todos los datos y metadatos personales de las personas usuarias de los servicios que ofrecen las compañías que proveen internet.

Es igualmente importante que dicha previsión pueda ser afirmada en su vigencia en los momentos en que se declaran estados de emergencia sanitaria, económica, ecológica o social, de excepción o conmoción interior frente a las que los proveedores del servicio de internet no pueden suspender automáticamente sus obligaciones de protección a la privacidad e intimidad de las personas.

En los casos de Colombia[18] y Perú[19] se reportó cómo los Estados decidieron acudir a los proveedores del servicio de internet y telefonía para requerir acceso a los datos de geolocalización de sus usuarios con justificación en la pandemia y el rastreo de contagios. Solicitudes que, tal y como lo informó la sociedad civil en cada caso, carecían de la advertencia clara sobre la finalidad y la temporalidad en el uso y acceso a datos sensibles.

Los proveedores del servicio de internet deben tener el deber de efectuar, ante solicitudes de este tipo análisis de impacto en privacidad para valorar debidamente la legalidad, proporcionalidad y razonabilidad de su contenido. Así también, en el marco de emergencias que parezcan suspender la vigencia de algunos derechos fundamentales, deben poder ser revestidos de garantías que faciliten su trabajo como *gatekeepers* en la protección de la privacidad de sus usuarios y suscriptores.

Afirmar igualmente el alcance de las disposiciones de este artículo a los contextos de crisis social, como la protesta social, o en general de ejercicio de derechos de alcance colectivo frente a los que las empresas proveedoras del servicio de internet deben garantizar la existencia de mecanismos que les permitan resistir pedidos de vigilancia selectiva de las comunicaciones de las personas, no justificada o amparada en los eventos consagrados por la ley del país en que funcionen.

Según la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos[20] los Estados han acostumbrado, en el marco de las protestas sociales, a elevar ante los proveedores del servicio de internet solicitudes de limitación del anonimato de las

---

[18] Fundación Karisma (2020). Comunicado sobre la circular 01 de 2020 de la SIC. Disponible en : https://web.karisma.org.co/organizaciones-de-la-sociedad-civil-rechazan-circular-de-la-sic-sobre-uso-de-datos-personales-para-controlar-la-pandemia/

[19] Gobierno de la República del Perú (2020). Decreto Supremo 070-2020-PCM. Disponible en: https://busquedas.elperuano.pe/normaslegales/dictan-medidas-complementarias-al-decreto-supremo-n-044-202-decreto-supremo-n-070-2020-pcm-1865590-4/

[20] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (2019). Protesta y derechos humanos. Disponible en: http://www.oas.org/es/cidh/expresion/publicaciones/ProtestayDerechosHumanos.pdf

personas al navegar en la red, de entrega de datos de georreferenciación de protestantes, entre otros (prr. 302).

Los proveedores del servicio de internet, en vigencia de las responsabilidades que les son aplicables en materia de derechos humanos, tienen que poder ser requeridos en el contenido de este artículo, para que puedan materializar ante contextos de presión estatal la vigencia de la privacidad e intimidad en la red y las comunicaciones de las personas.

Artículo 8. Derecho a la información

En los comentarios siguientes nos orientamos en el contenido del informe de Fundación Karisma e Hiperderecho sobre los aspectos que vale la pena que sean fortalecidos a nivel normativo para ampliar los deberes que tienen a su cargo los proveedores del servicio de internet en materia de acceso a la información y que puedan al tiempo constituir garantías para las personas que suscriben sus servicios.

- *Es importante que se requiera a los proveedores del servicio de internet que amplíen y mejoren la manera como informan sobre las solicitudes de acceso a la información de los datos y comunicaciones de sus usuarios y suscriptores cuando son efectuadas por parte de entidades públicas*.

Según Karisma, se precisa que a los proveedores del servicio de internet se les requieran mayores niveles de desagregación en la entrega de información sobre las solicitudes de acceso a sus datos y sus comunicaciones. Es importante que dichos reportes provean detalles sobre qué tipo de solicitudes reciben (interceptaciones, bloqueos de sitios web o dominios de internet, solicitudes de datos de sus suscriptores, entre otros), su cantidad o número, diferenciación según qué entidad en ejercicio de qué facultades elevó la solicitud, aquellas recibidas frente a las rechazadas y la razón del rechazo.

De acuerdo con Hiperderecho (2020) también es importante que se puedan requerir a los proveedores del servicio de internet que se fortalezcan las tareas de difusión, visibilización y accesibilidad a dichos informes para que las personas suscriptoras de dichos servicios puedan orientar mejor la toma de sus decisiones sobre qué operador elegir.

Así, los informes de Colombia, Perú como los de la Electronic Frontier Foundation y Ranking Digital Rights sostienen que la desagregación de la información debe poder detallar (i) el número de solicitudes recibidas por año y mes para permitir la realización de estudios comparativos, (ii) el país desde el que se origina la solicitud, (iii) la autoridad que eleva la solicitud y amparada en qué facultad, (iv) el número de solicitudes recibidas, así como las concedidas y rechazadas.

Fundación Karisma

Es igualmente relevante que se requiera en la actualización de este artículo, que dicha información sea provista en formato de datos abiertos que faciliten su análisis y reutilización.

- *Es importante que se requiera a los proveedores del servicio de internet que notifiquen a las personas suscriptoras de sus servicios sobre los eventos de solicitud de acceso a sus datos y comunicaciones elevadas por entidades del Estado*

De acuerdo con ambos informes de Colombia y Perú así como con el índice de responsabilidad corporativa de Ranking Digital Rights (2021) es importante que las personas suscriptoras de los servicios de los proveedores del servicio de internet sean notificadas de los eventos en que una entidad pública ha solicitado acceso a sus datos o sus comunicaciones, y que debe, de acuerdo a éste último informe, ser exigido a los proveedores sin importar la jurisdiccional nacional en que funcionen.

- *Es importante que se requiera a los proveedores del servicio de internet que informen de manera pública sobre las solicitudes de censura, moderación del tráfico o apagones de internet*

El informe de Ranking presta especial atención al deber de fortalecer las obligaciones en materia de transparencia a cargo de los proveedores del servicio de internet para que informen claramente sobre las solicitudes de censura de contenidos en internet, sobre las solicitudes de gestión del tráfico de internet así como solicitudes oficiales de apagar internet de manera sectorizada o generalizada.

Artículo 11. Derecho al libre acceso a contenidos, aplicaciones y servicios, así como a su correspondiente uso

Si bien es importante que se afirme, tal y como lo hace el artículo, el deber de garantizar a los usuarios de los proveedores del servicio de internet el derecho al acceso libre e irrestricto de contenidos, aplicaciones y servicios a su elección, creemos que es importante poder asociar a este deber de garantía el deber de transparencia, sobre todo en la aplicación de las excepciones que según el artículo autorizan al bloqueo o limitación de contenidos, aplicaciones, desarrollos o servicios según así lo ordene una autoridad competente.

Dicho deber de transparencia se alinea con las previsiones de la Relatoría para la Libertad de Expresión en su informe de 2013 al decir que:

> Las normas sobre neutralidad de la red deben exigir que los prestadores del servicio de internet sean transparentes respecto de las prácticas que emplean para la gestión del tráfico o la información. Cualquier información relevante sobre tales prácticas debe ser puesta a disposición del público y del órgano encargado de supervisar el cumplimiento del principio de neutralidad de la red, en un formato que resulte accesible para los interesados[21].

El deber de transparencia debe poder interpelar a dos actores. A las autoridades de las comunicaciones de los países de la CAN así como a los proveedores del servicio de internet.

El caso de Colombia es ejemplificador sobre cómo debe poder ser ejercido ese deber de transparencia por la autoridad reguladora. Así, la Comisión de Regulación de las Comunicaciones fue facultada durante la pandemia para proveer instrucciones a los proveedores del servicio de internet en caso de que, por la saturación en el uso de la Red, fuera preciso ordenar la priorización del tráfico de internet en Colombia[22]. En vigencia de dichas facultades --que todavía no han sido ejercidas propiamente limitando el tráfico de internet--, se han emitido informes de transparencia bajo criterios que creemos valdría la pena que fueran considerados en la redacción de esta norma.

Dichos informes proveen información accesible en datos abiertos, su actualización es constante y provee mediciones sobre la hora de mayor saturación del servicio de internet según cada proveedor, el tipo de contenido más accedido, así como el día de la semana en que esto sucede según se trate de internet móvil o fijo.

Frente al cumplimiento del deber de transparencia por los proveedores del servicio de internet que tengan que efectuar acciones de gestión del tráfico, es importante que éstos informe sobre: la duración de las medidas de gestión del tráfico, los contenidos afectados, qué tipo de entidad la ordena y atendiendo qué norma o facultad legal, sobre pedidos recibidos y el desagregado entre aquellos concedidos y negados. Nuevamente, en formatos que sean accesibles y faciliten el reuso posterior de la información.

Artículo 12. Derecho al trato equitativo y no discriminatorio del tráfico (gestión del tráfico)

---

[21] Informe anual de la Comisión Interamericana de Derechos Humanos (2013). Informe de la relatoría especial para la libertad de expresión, prr. 31. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/anuales/2014_04_22_IA_2013_ESP_FINAL_WEB.pdf

[22] Comisión de Regulación de Comunicaciones (2020). Nuevas normas sobre gestión de tráfico, Resolución 5969 CRC. Disponible en: https://cv19.karisma.org.co/docs/Resolucion5969CRC/

- *Es importante que se requiera a los proveedores del servicio de internet la preservación del principio de neutralidad de internet y resistirse a las solicitudes de apagones de internet*

Según el informe de la Electronic Frontier Foundation (2019) y Ranking Digital Rights (2020) que han evaluado de manera cercana el rol de los proveedores del servicio de internet en la preservación del principio de neutralidad, se destaca la importancia de que se requiera legalmente a dichas compañías que declaren de manera pública sus compromisos en el mantenimiento de dicho principio, central en el funcionamiento de internet, así como los mecanismos internos que deben poder diseñar para lograr su preservación. Es una buena práctica que debe poder ser dotada de obligatoriedad en el plano jurídico.

Según la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (2019) los Estados han acostumbrado, en el marco de las protestas sociales, a elevar ante los proveedores del servicio de internet solicitudes de "limitaciones en el acceso a internet, incluyendo las desconexiones totales o parciales, la ralentización de internet, los bloqueos temporales o permanentes de distintos sitios y aplicaciones, antes durante o después de reuniones pacíficas constituyen restricciones ilegítimas a los derechos de asociación y reunión" (prr 298).

Los proveedores del servicio de internet, en vigencia de los deberes que les son aplicables en materia de derechos humanos, tienen que poder ser requeridos para que puedan materializar ante contextos de represión estatal la vigencia del principio de neutralidad de la red así como la vigencia de los derechos a la privacidad e intimidad de las personas.

***

Fin