Caracas, 08 de septiembre de 2026

INFORME DE OBSERVACIONES Y OPOSICIÓN INTEGRAL A LOS PROYECTOS DE REFORMA DE LA PROVIDENCIA ADMINISTRATIVA DE ATRIBUTOS DE LAS HABILITACIONES GENERALES Y DE CONDICIONES GENERALES PARA EL ESTABLECIMIENTO DE PUNTOS DE INTERCAMBIO DE TRÁFICO DE INTERNET NACIONAL.

Riesgos para la libertad de expresión, el acceso a la información y otros derechos humanos ejercidos a través de internet.

Nosotros, Asociación Civil Espacio Público, organización dedicada a la promoción y defensa del derecho a la libertad de expresión y el acceso a la información, consignamos ante la Comisión Nacional de Telecomunicaciones y en ejercicio del derecho constitucional a la participación ciudadana en la gestión pública (artículo 62 de la CRBV), nuestras observaciones respecto a los dos procedimientos administrativos concurrentes de consulta pública, a saber:

1. El procedimiento iniciado mediante la **Providencia Administrativa N.º 115** de fecha **29 de junio de 2026**, que ordena la consulta pública del proyecto de reforma de la Providencia Administrativa Contentiva de los Atributos de las Habilitaciones Generales.

2. El procedimiento formalizado mediante la **Providencia Administrativa de la Dirección General**, que ordena el inicio de la consulta pública del proyecto de Providencia Administrativa de Condiciones Generales para el Establecimiento de Punto de Intercambio de Tráfico de Internet Nacional.

Estando ambos procesos en curso legal ante la División de Regulación Sectorial, adscrita a la Gerencia de Planificación y Desarrollo del Sector de Telecomunicaciones, exponemos las observaciones, objeciones y propuestas institucionales que se detallan a continuación:

El presente informe se concentra en identificar y sustentar, artículo por artículo, los riesgos que los textos sometidos a consulta representan para el ejercicio de la libertad de expresión y el acceso a la información, derechos que se materializan hoy, de forma primordial, a través de Internet, así como para otros derechos que dependen transversalmente de la conectividad, tales como la reunión y asociación, y el derecho a la participación electoral y política. Para cada riesgo se explica el mecanismo por el cual el articulado analizado puede lesionar el derecho correspondiente, se ofrece el fundamento jurídico, constitucional e internacional, de la observación, y se indica qué deberían incorporar ambos instrumentos para ser garantistas de los derechos humanos involucrados.

I. Punto previo

1. Marco regulatorio del internet en Venezuela

El marco regulatorio del internet en Venezuela se caracteriza por su **dispersión legal**, ya que no existe una ley única que regule la materia, sino varias leyes que abordan desde la infraestructura técnica hasta el control de contenidos y la seguridad digital. La columna vertebral de este sistema es la *Ley Orgánica de Telecomunicaciones (LOTEL)*, la cual define al internet como un servicio de interés general y faculta a **CONATEL** para otorgar las habilitaciones necesarias a las empresas proveedoras, controlando el uso del espectro radioeléctrico y las redes físicas (arts. 3, 5, 7, 16 y 20).

Por otra parte, el uso cotidiano, la legalidad de los datos y el comportamiento en la red se rigen de manera complementaria por otros instrumentos jurídicos específicos. La *Ley RESORTE-ME* y la *Ley contra el Odio* regulan estrictamente los contenidos en portales web y redes sociales, haciendo responsables a los administradores y usuarios por los mensajes difundidos, lo que ha permitido la aplicación de bloqueos y sanciones por parte del Estado. Asimismo, la *Ley sobre Mensajes de Datos y Firmas Electrónicas* otorga plena validez jurídica a las interacciones y contratos digitales, mientras que la *Ley Especial contra los Delitos Informáticos* se encarga del ámbito penal, sancionando conductas como el *hackeo*, el sabotaje de sistemas y la violación de la privacidad en línea.

2. Regulación del internet mediante Ley Orgánica

El servicio de internet se erige como una condición esencial y presupuesto indispensable para el ejercicio progresivo de los derechos fundamentales a la libertad de expresión y el acceso a la información. Asimismo, constituye una herramienta transversal para la garantía de otros derechos de rango constitucional, tales como la educación, la salud, el trabajo, el derecho de reunión, la asociación, y la participación política y electoral.

En virtud de su impacto directo en el desarrollo de estas garantías fundamentales, y de conformidad con el principio de jerarquía normativa consagrado en el artículo 7 de la Constitución de la República Bolivariana de Venezuela (CRBV), la regulación del internet, incluyendo sus aspectos técnicos especializados como los Puntos de Intercambio de Tráfico (IXP) y los parámetros de calidad del servicio, se encuentra sujeta estrictamente a una **reserva de ley orgánica**.

El marco constitucional venezolano fundamenta esta reserva legal a través de tres artículos clave:

- **Artículo 156, numeral 28:** atribuye al Poder Público Nacional la competencia exclusiva sobre el régimen de las telecomunicaciones, categoría en la que se inscribe internet.
- **Artículo 187:** confiere a la Asamblea Nacional la facultad exclusiva de legislar sobre las materias de competencia nacional.
- **Artículo 203:** determina que las leyes que se dicten para desarrollar derechos constitucionales tienen carácter orgánico. Por ende, de conformidad con el procedimiento constitucional, la Asamblea Nacional debe aprobar por las **dos terceras partes de sus integrantes el carácter orgánico del proyecto antes de iniciarse la discusión de la ley**. Tras su sanción parlamentaria, el texto debe remitirse obligatoriamente a la Sala Constitucional del Tribunal

Supremo de Justicia para que se pronuncie sobre la constitucionalidad de dicho carácter, antes de su promulgación.

Por lo tanto, pretender regular de forma originaria los elementos estructurales del internet mediante una providencia administrativa no solo infringe el artículo 203 de la CRBV, sino que constituye una usurpación de funciones legislativas. Aunque el artículo 132 de la Ley Orgánica de Telecomunicaciones (LOTEL) faculta a CONATEL para dictar condiciones generales de interconexión, dicha atribución técnica no puede instrumentalizarse para delegar de forma abierta una regulación que afecta el núcleo esencial de derechos constitucionales. En este aspecto, el rol de la Comisión Nacional de Telecomunicaciones (CONATEL) no debe ser el desarrollo de normativas sublegales, sino la articulación con diversos sectores para elaborar una propuesta de **ley orgánica y presentarla formalmente ante la Asamblea Nacional**.

Esta necesidad responde además a la insuficiencia del marco legal vigente. Aunque la Ley Orgánica de Telecomunicaciones (LOTEL) reconoce el interés público de este sector y obliga a CONATEL a promover el acceso universal y otorgar habilitaciones, su enfoque es **genérico e insuficiente**. La LOTEL carece de disposiciones técnicas y especializadas que definan los principios rectores de los IXP, las condiciones específicas para operadores de internet o los estándares mínimos de calidad del servicio.

Experiencias en el derecho comparado regional, como las de **Chile y Perú**, demuestran la eficacia de contar con leyes específicas orientadas a regular el internet, sus principios generales y sus parámetros técnicos, un modelo indispensable para superar el vacío normativo actual en Venezuela.

II. Cuadro síntesis de riesgos, fundamento jurídico y recomendaciones

Artículo(s)	Derecho(s) en riesgo	Riesgo identificado	Qué debe incorporar la Providencia
Reforma: Art. 1(Definiciones IPTV / OTT)	Libertad de expresión y acceso a la información	Al tipificar IPTV y OTT bajo el régimen de "difusión por suscripción", se pretende extender el control discrecional de contenidos de la Ley RESORTE-ME a plataformas de streaming y contenidos de la web.	Excluir explícitamente a las OTT e IPTV del régimen de control de contenidos audiovisuales tradicionales. Garantizar que no se exigirán licencias de contenido para operar sobre internet.
Reforma: Art. 2 (Atributo IXP) y **Providencia IXP:** Arts. 2.4, 5 y 18	Libertad de expresión y acceso a la información (art. 57 y 58 CRBV; art. 13 CADH)	La neutralidad de red se define de forma restrictiva (solo para el plano comercial entre operadores en la Reforma y la Providencia). Deja desprotegido al usuario final. El Art. 5 introduce el	Definir la neutralidad de red conforme al estándar internacional, extenderla expresamente a la relación ISP-usuario final y unificar la terminología eliminando "neutralidad tecnológica".

		concepto ambiguo de "neutralidad tecnológica".	
Reforma: Art. 3 (Disposición Única)	Libertad económica y pluralismo informativo	El lapso de sesenta (60) días continuos para tramitar o adecuar la Habilitación General bajo el nuevo atributo genera una barrera burocrática asfixiante para operadores independientes.	Ampliar el plazo a un mínimo de ciento ochenta (180) días hábiles, estableciendo un procedimiento de homologación automática y gratuita para operadores preexistentes.
Arts. 2.4, 5 y 18	Libertad de expresión y acceso a la información (art. 57 y 58 CRBV; art. 13 CADH)	La neutralidad de red solo protege la relación entre operadores del IXP, no al usuario final frente al ISP; “neutralidad tecnológica” (art. 5) es un concepto distinto y no definido.	Definir la neutralidad de red conforme al estándar internacional, extenderla a la relación ISP-usuario y enumerar taxativamente las excepciones admisibles.
Art. 21	Libertad de expresión y acceso a la información; libre negociación (art. 131 LOTEL)	Interconexión obligatoria y centralizada en un mínimo de IXP, sin prohibición de uso para bloqueo y sin control judicial previo para cortes o exclusiones.	Prohibir expresamente el uso del IXP para bloqueo o filtrado; incorporar un régimen reglado de desconexión con audiencia previa y control judicial.
Disposición Transitoria Segunda	Libertad de expresión; pluralismo informativo	Migración obligatoria de servidores CDN a sedes controladas por el operador del IXP, con riesgo de control físico centralizado de plataformas de contenido.	Que la ubicación de los servidores de CDN en el IXP sea voluntaria, o esté acompañada de auditoría independiente y prohibición de uso para desconexión selectiva.
Art. 28	Acceso a la información	No se aclara si los nodos Anycast del NIC.VE podrían usarse para filtrar o redirigir la resolución de dominios “.ve”.	Aclarar que dichos nodos no podrán bloquear, filtrar o redirigir resoluciones DNS salvo orden judicial motivada.
Arts. 23, 24 y 27	Privacidad de las comunicaciones (art. 60 CRBV; Obs. Gral. N.º 16); libertad de expresión	Acceso directo y en tiempo real de “autoridades competentes” no identificadas a telemetría del tráfico nacional, sin control judicial previo.	Definir taxativamente las autoridades habilitadas; limitar el acceso en tiempo real a datos agregados y anonimizados; exigir orden judicial para datos identificables; crear informes de transparencia.

	(efecto disuasivo)		
Art. 19	Privacidad; libertad de expresión (cifrado)	Exigencia vaga de “mecanismos de criptografía” por “seguridad de la Nación”, sin excluir el debilitamiento del cifrado o las puertas traseras.	Prohibir expresamente exigir el debilitamiento o acceso excepcional al cifrado de extremo a extremo.
Art. 19 y 26.1	Protección de datos personales	Ausencia de ley y autoridad de protección de datos; técnica de anonimización de la matriz de tráfico no definida.	Designar autoridad de supervisión; definir estándar técnico de anonimización auditable.
Arts. 12-16, 20, 31-33	Educación (art. 102 CRBV) y salud (art. 83 CRBV)	La “tarifa social” solo beneficia a ISP pequeños; no hay garantías de asequibilidad o continuidad reforzada para usuarios vulnerables ni instituciones educativas o de salud.	Ampliar la asequibilidad a usuarios vulnerables e instituciones de servicio público, con metas de cobertura universal y continuidad reforzada.
Arts. 6, 8, 9, 10 y 18	Trabajo y libertad económica (art. 87 CRBV)	Idoneidad remitida a una guía inexistente; autorización previa de CONATEL para prácticamente toda decisión societaria y técnica de los operadores.	Publicar criterios objetivos y verificables de idoneidad; limitar la autorización previa a operaciones que comprometan continuidad, seguridad o neutralidad.
Art. 5	Asociación y reunión (arts. 52 y 53 CRBV)	Comité de Gestión Multisectorial facultativo, sin representación mínima garantizada de sociedad civil, academia y usuarios, y sin competencias vinculantes.	Hacer obligatoria su creación; garantizar representación mínima y paritaria; otorgarle competencias vinculantes en materia de neutralidad.
General (sin disposición específica)	Elecciones libres y participación política (arts. 62 y 63 CRBV)	No existe cláusula de no discriminación del tráfico en contextos electorales o de protesta social, pese a la centralización del enrutamiento nacional.	Incorporar cláusula de no discriminación por contexto, con mención especial a procesos electorales y manifestaciones públicas.
Art. 1 y estructura general	Todos los anteriores (art. 203 CRBV)	Se regula por vía sublegal una materia reservada a ley orgánica por	Impulsar un proyecto de ley orgánica sobre internet, con participación multisectorial,

		instrumentalizar derechos constitucionales.	que sirva de marco habilitante.
Art. 30 y régimen sancionatorio	Debido proceso	CONATEL concentra habilitación, supervisión, sanción y resolución de controversias, sin instancia de apelación independiente ni evaluación previa de impacto en derechos humanos.	Establecer procedimiento sancionatorio con audiencia y motivación, vía de revisión independiente, y evaluación de impacto en derechos humanos previa a la implementación.

III. Riesgos para la libertad de expresión y el acceso a la información

La libertad de expresión y el acceso a la información, reconocidos en los artículos 57 y 58 de la CRBV y en el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, dependen hoy, de forma directa, de la arquitectura técnica sobre la cual circula el tráfico de internet. Un Punto de Tráfico de Internet (IXP) nacional que concentre el enrutamiento del tráfico interno, el acceso a las redes de entrega de contenidos (CDN) y la resolución de nombres de dominio se convierte en un punto único de control sobre el flujo de información del país. Los siguientes artículos de la Providencia generan, en ese sentido, riesgos concretos.

1. La extensión del control de contenidos web mediante las definiciones de IPTV y OTT (Artículo 1 de la Reforma)

Riesgo: el artículo 1 de la Reforma incorpora las definiciones de Televisión por Protocolo de Internet (IPTV) y Over-The-Top (OTT) englobándolas de forma genérica como servicios de difusión por suscripción. Al hacerlo, la Reforma crea el puente jurídico para aplicar normativas restrictivas de radiodifusión tradicional (como la Ley RESORTE-ME) a tecnologías y servicios basados puramente en la red de internet.

Por qué representa un riesgo: internet se rige por lógicas de transmisión de datos abiertas y descentralizadas. Forzar a los servicios OTT e IPTV a encajar en la categoría de difusión por suscripción tradicional permite al Estado exigir licencias previas de contenido, limitando el pluralismo informativo y el acceso a plataformas internacionales de *streaming* o medios de comunicación digitales. La Relatoría Especial para la Libertad de Expresión (RELE-CIDH) ha insistido en que los marcos regulatorios de los medios tradicionales no son aplicables a internet, y que condicionar el funcionamiento de plataformas web a habilitaciones de contenido constituye una restricción indirecta incompatible con el artículo 13 de la CADH.[1]

Qué falta: la Reforma de Atributos debe incorporar una disposición aclaratoria expresa que excluya a las tecnologías OTT e IPTV de cualquier mecanismo de censura previa, filtrado de catálogos o control de contenidos aplicable a la televisión por suscripción convencional, garantizando que el atributo solo regula la capacidad de transporte técnico de datos.

2. La neutralidad de red no protege al usuario final frente al bloqueo o la discriminación de contenidos (artículos 2, numeral 4, 5, y 18)

> *Artículo 2.4: "Neutralidad de Red: principio por el cual el Punto de Tráfico de Internet nacional no discrimina, interfiere, restringe o prioriza ningún tipo de uso de infraestructura o tráfico por razones comerciales o competitivas." — Artículo 5: el Comité de Gestión Multisectorial tendrá por finalidad "velar por la neutralidad tecnológica".*

Riesgo: la Providencia define la neutralidad de red únicamente como una garantía entre los operadores que confluyen en el IXP (no discriminación "por razones comerciales o competitivas"), pero no la extiende a la relación entre los proveedores de servicios de Internet (ISP) y el usuario final. El

[1] Relatoría Especial para la Libertad de Expresión (RELE-CIDH), *Libertad de expresión e internet*, doc. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13 (31 de diciembre de 2013), párrs. 11, 53, 55, 91-92, https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf.

artículo 5, además, introduce un concepto distinto, "*neutralidad tecnológica*", para definir el mandato del Comité de Gestión Multisectorial, sin que ese concepto esté definido en ninguna parte del texto ni sea equivalente al de neutralidad de red.

El resultado es que el principio que efectivamente protege la libertad de expresión y el acceso a la información, la prohibición de bloquear, ralentizar o priorizar el tráfico en función de su origen, destino, contenido o aplicación, carece de definición precisa, de sujeto obligado claro (el ISP frente al usuario) y de un órgano con mandato expreso sobre su cumplimiento.

Por qué representa un riesgo: sin una garantía de neutralidad de red oponible frente al usuario final, nada en la Providencia impide que, invocando razones "técnicas" o de "seguridad", se bloqueen, degraden o prioricen selectivamente páginas de medios de comunicación, organizaciones no gubernamentales, redes sociales o herramientas de elusión de la censura (VPN).

La Declaración Conjunta sobre Libertad de Expresión e Internet (2011) de los relatores de libertad de expresión de la ONU y la OEA identifica la neutralidad de la red como una de las condiciones estructurales para que el acceso a internet sirva efectivamente al ejercicio de la libertad de expresión, precisamente porque impide que los intermediarios técnicos, en este caso, la infraestructura de intercambio de tráfico, se conviertan en instrumentos de censura indirecta.[2]

Qué falta: la Providencia debe (i) definir la neutralidad de red conforme al estándar internacional, no discriminación de tráfico por origen, destino, contenido, aplicación o dispositivo; (ii) extenderla expresamente a la relación entre los ISP y el usuario final, y no solo a la relación entre operadores dentro del IXP; (iii) enumerar taxativamente las excepciones admisibles (gestión técnica no discriminatoria de la red, cumplimiento de una orden judicial motivada, protección de personas menores frente a contenido ilegal); y (iv) unificar la terminología, sustituyendo toda referencia a "*neutralidad tecnológica*" por "*neutralidad de red*", con mandato de cumplimiento y supervisión expresamente atribuido al Comité de Gestión Multisectorial y no solo a CONATEL.

3. La interconexión obligatoria y centralizada crea un punto único de control sobre el tráfico nacional (artículo 21)

> *Artículo 21: "Los operadores de servicios de internet y cualquier interesado, que operen en el territorio nacional, tendrán la obligación de interconexión total entre sí (…) como mínimo en dos (02) Puntos de Intercambio de Tráfico de Internet Nacional, para cursar el tráfico de internet."*

Riesgo: al imponer que la totalidad de los operadores de servicios de Internet del país deban interconectarse obligatoriamente, sin alternativa, a un número reducido de IXP nacionales, la Providencia concentra en una infraestructura de tránsito la totalidad del tráfico de internet del país. Ninguna disposición prohíbe expresamente que dicha infraestructura centralizada sea utilizada para ordenar cortes, bloqueos, filtrado o degradación selectiva de tráfico, ni se prevé un procedimiento de excepción con control judicial previo, plazos definidos y juicio de proporcionalidad para el caso de que la autoridad pretenda intervenir el tráfico cursado por esa vía.

Por qué representa un riesgo: la obligatoriedad de la interconexión, sin las salvaguardas señaladas, transforma una decisión de arquitectura técnica en un mecanismo potencial de censura estructural; en lugar de que la autoridad deba dirigirse a cada proveedor de internet para ordenar el bloqueo de un

[2] Relatoría Especial para la Libertad de Expresión, "Declaración conjunta sobre libertad de expresión e internet", comunicado de prensa R50/11 (Organización de los Estados Americanos, 1 de junio de 2011), https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=848.

sitio web, bastaría con intervenir el punto de intercambio para afectar, de forma simultánea y con un solo acto, el acceso de todo el país a un contenido, aplicación o servicio determinado.

Este riesgo de concentración ya ha sido advertido expresamente por **LAC-IX** en su posición del 17 de agosto de 2026 sobre esta misma consulta, al señalar que cuanto más centralizada y sujeta a control estatal esté la infraestructura de intercambio de tráfico de un país, mayor es la capacidad de una autoridad para ejercer control total sobre dicho tráfico, incluyendo su eventual bloqueo, filtrado o vigilancia.[3]

Desde la perspectiva de los estándares interamericanos, cualquier medida de bloqueo o filtrado de contenidos en internet debe superar el *test* de legalidad, finalidad legítima y proporcionalidad del artículo 13.2 de la CADH; una arquitectura que permite el bloqueo generalizado sin ese control previo es, en sí misma, incompatible con dicho estándar, sin necesidad de que el bloqueo llegue a materializarse.[4]

Qué falta: la Providencia debe incorporar una prohibición expresa de utilizar la infraestructura del IXP nacional para bloquear, filtrar, degradar o redirigir tráfico por razones distintas de las estrictamente técnicas, así como un procedimiento reglado y excepcional, con control judicial previo, motivación, plazos y proporcionalidad, para cualquier medida de esa naturaleza.

4. La migración obligatoria de las redes de entrega de contenidos (CDN) a infraestructura estatal (Disposición Transitoria Segunda)

> *Disposición Transitoria Segunda: "Los acuerdos, contratos o convenios suscritos entre los Operadores de Servicios de Internet y las empresas que ofrecen CDN, implementados en sus redes, se mantendrán vigentes hasta tanto se realice las gestiones necesarias, para la instalación de equipos servidores de los CDN, en la sede de los Puntos de Intercambio de Tráfico de Internet Nacional y sea efectiva la misma."*

Riesgo: esta disposición transitoria revela que el objetivo final del modelo regulatorio es que los servidores de las redes de entrega de contenidos (por ejemplo, las que alojan plataformas de video, redes sociales o buscadores) migren de su ubicación actual, normalmente distribuida entre distintos operadores, hacia la sede física de los Puntos de Intercambio de Tráfico de Internet Nacional. Aunque ello puede mejorar la velocidad de acceso a esos contenidos, tiene como efecto colateral que copias de las plataformas más consumidas por la población queden alojadas en instalaciones sujetas al control regulatorio directo de CONATEL.

Por qué representa un riesgo: obligar a grandes proveedores globales de contenido y plataformas digitales (como Google, Netflix o redes sociales) a centralizar sus servidores físicos en una infraestructura bajo control estatal directo incrementa drásticamente la vulnerabilidad del ecosistema digital venezolano. Esta concentración física y operativa le otorga a la autoridad administrativa la capacidad técnica de ejecutar un apagón selectivo o la incautación de equipos en momentos de alta tensión política o social, interrumpiendo el flujo de información de manera generalizada. Este escenario de centralización forzada de la infraestructura de comunicación contradice los estándares

[3] Asociación Latinoamericana y del Caribe de Operadores de Puntos de Intercambio de Tráfico (LAC-IX), "Posición de LAC-IX sobre la consulta pública de CONATEL para la regulación de los Puntos de Intercambio de Tráfico de Internet (IXP) en Venezuela" (documento institucional, Montevideo, 17 de agosto de 2026), https://lac-ix.org/posicion-de-lac-ix-sobre-la-consulta-publica-de-conatel-para-la-regulacion-de-los-puntos-de-intercambio-de-trafico-de-internet-ixp-en-venezuela/

[4] Relatoría Especial para la Libertad de Expresión, "Declaración conjunta".

de la CIDH y la ONU sobre libertad de expresión, los cuales advierten que la concentración del control sobre los medios y la infraestructura técnica lesiona gravemente el pluralismo informativo y facilita la censura previa estructural[5].

Qué falta: la Providencia debe garantizar que la ubicación física de los servidores de CDN dentro de las instalaciones del IXP sea una opción voluntaria de los operadores de contenido y no una obligación regulatoria, o, de mantenerse como objetivo de política pública, debe estar acompañada de garantías reforzadas de neutralidad, auditoría independiente y prohibición expresa de que dicha centralización física se utilice como mecanismo de bloqueo o desconexión selectiva de plataformas.

5. El control sobre la resolución de nombres de dominio del ccTLD ".ve" (artículo 28)

> *Artículo 28: "Todos los operadores y cualquier interesado conectados a los Puntos de Intercambio de Tráfico de Internet Nacional deberán configurar sus tablas de enrutamiento para priorizar la resolución de consultas del dominio .ve a través de estos nodos locales (…)."*

Riesgo: la Providencia no aclara si los nodos ***Anycast*** del Centro de Información de Red de Venezuela (NIC.VE), alojados obligatoriamente en la infraestructura del IXP nacional, podrían ser utilizados para filtrar, redirigir o bloquear la resolución de dominios, además para acelerar su resolución legítima.

Por qué representa un riesgo: el Sistema de Nombres de Dominio (DNS), es decir, la capacidad de apagar o redirigir páginas web completas alterando su dirección de internet en los servidores centrales, es uno de los puntos técnicos más utilizados en el mundo para implementar bloqueos de acceso a sitios web; priorizar y centralizar su resolución en nodos controlados por el operador del IXP, sin una prohibición expresa de uso para fines distintos de la resolución técnica, crea una vía adicional, y menos visible para el usuario, de censura de contenidos alojados bajo el dominio nacional.

Qué falta: incorporar una cláusula expresa que aclare que los nodos Anycast del NIC.VE alojados en el IXP no podrán utilizarse para bloquear, filtrar o redirigir resoluciones DNS salvo mediante orden judicial motivada, dictada con las garantías del debido proceso y sujeta a control posterior.

6. El monitoreo en tiempo real del tráfico genera un efecto disuasivo (*chilling effect*) sobre la libre expresión (artículos 23 y 24)

Riesgo: los artículos 23 y 24 obligan a los operadores de servicios de internet y a los operadores del IXP a implementar herramientas de monitorización y medición en tiempo real que permiten identificar, entre otros datos, el tráfico dirigido hacia redes de entrega de contenidos específicas y hacia la red mundial de internet, discriminado por cada proveedor de conectividad internacional, con acceso directo y en tiempo real de CONATEL a dicha información.

Por qué representa un riesgo: aunque el texto indica que la información recolectada es de naturaleza estadística y no debería exponer el contenido de las comunicaciones, la sola existencia de una ventana de visualización estatal en tiempo real sobre los flujos de tráfico hacia servidores de medios de comunicación independientes, redes sociales o plataformas internacionales genera lo que la doctrina de derechos humanos denomina un efecto disuasivo o *chilling effect*: la percepción

[5] Relatoría Especial para la Libertad de Expresión, "Declaración conjunta".

fundada, por parte de la ciudadanía, de estar bajo vigilancia constante que induce a la autocensura y erosiona la confianza en el entorno digital como espacio de libre circulación de ideas.[6]

El Comité de Derechos Humanos de la ONU, en su Observación General N° 34 sobre el artículo 19 del PIDCP, ha señalado que los Estados deben abstenerse de imponer restricciones incompatibles con dicho artículo, incluidas aquellas que generen un efecto disuasivo desproporcionado sobre el ejercicio de la libertad de expresión.[7] Adicionalmente, el conocimiento detallado y en tiempo real de los flujos de tráfico dirigidos a plataformas específicas otorga a la autoridad una ventaja operativa para ejecutar bloqueos selectivos o estrangulamiento de ancho de banda con precisión, particularmente en coyunturas políticas o sociales sensibles.

Qué falta: limitar el alcance del monitoreo a datos agregados y no identificables por proveedor de contenido o servicio específico cuando ello pueda revelar patrones de consumo informativo de la población; exigir el uso de técnicas de *anonimización* robustas y auditadas; y condicionar cualquier acceso a datos más granulares, capaces de identificar el consumo de contenido de medios, plataformas o servicios concretos, a la existencia de un fin legítimo, definido normativamente, y a un control independiente.

IV. Riesgos para la privacidad de las comunicaciones, presupuesto instrumental de la libertad de expresión

La privacidad de las comunicaciones, reconocida en el artículo 60 de la CRBV y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, es un presupuesto instrumental de la libertad de expresión. Sin garantía de confidencialidad de las comunicaciones, el ejercicio de la libre expresión y de la búsqueda de información se retrae. El Comité de Derechos Humanos de la ONU, en su Observación General N°16, sostiene que toda injerencia estatal en las comunicaciones debe estar sujeta a control independiente y ser estrictamente proporcional a un fin legítimo para no ser considerada arbitraria.[8] La Providencia presenta, en este eje, varios vacíos relevantes.

1. Acceso directo y en tiempo real de "*autoridades competentes*" sin control judicial (artículos 23, 24 y 27)

> *Artículo 27: "El operador de Intercambio de Tráfico de Internet Nacional habilitará dentro de su plataforma el acceso de solo lectura (Read-Only) a las autoridades competentes en materia de telecomunicaciones, con el propósito exclusivo de recolectar estadísticas de volumen de tráfico, utilización de ancho de banda, estado de los enlaces y métricas de rendimiento (telemetría)."*

Riesgo: ni el artículo 27 ni los artículos 23 y 24 definen con precisión cuáles son las "autoridades competentes" habilitadas para acceder a esta información, ni exigen orden judicial, administrativa motivada o mecanismo de control independiente previo al acceso.

---

[6] David L. Hudson, Jr., "Panorama general del efecto disuasorio" (Fundación para los Derechos Individuales y la Expresión), consultado el 6 de septiembre de 2026, https://www.fire.org/research-learn/chilling-effect-overview.

[7] Comité de Derechos Humanos de las Naciones Unidas, *Observación general n.º 34: Artículo 19 (Libertad de opinión y libertad de expresión)*, 102.º período de sesiones, doc. ONU CCPR/C/GC/34 (12 de septiembre de 2011), pág. 13, párr. 47, https://www.acnur.org/fileadmin/Documentos/BDL/2012/8507.pdf.

[8] Comité de Derechos Humanos de las Naciones Unidas, *Observación general n.º 16: Artículo 17 (Derecho a la intimidad)*, 32.º período de sesiones, doc. ONU HRI/GEN/1/Rev.7 en 162 (1988), Biblioteca de los Derechos Humanos de la Universidad de Minnesota, https://hrlibrary.umn.edu/hrcommittee/Sgencom16.html.

El acceso a la infraestructura se plantea en tiempo real mediante protocolos de gestión de red (como SNMP v3) configurados en modo de lectura. Si bien este mecanismo de telemetría restringe la modificación directa de los enrutadores por sí mismo, la centralización masiva de estos metadatos técnicos en manos del regulador es crítica. Esta recopilación provee al Estado la inteligencia de red necesaria (patrones de consumo, volumen y rutas del tráfico nacional) para coordinar medidas externas de estrangulamiento de ancho de banda o bloqueos selectivos. Asimismo, la ausencia de auditorías independientes sobre estos accesos lógicos abre la puerta a que esta infraestructura centralizada sirva como base logística para desviar o duplicar flujos de datos hacia sistemas externos de Inspección Profunda de Paquetes (DPI), facilitando así la vigilancia masiva del tráfico nacional.[9]

Por qué representa un riesgo: un acceso estatal directo, permanente y sin control judicial previo a la telemetría de toda la infraestructura nacional de intercambio de tráfico no satisface el estándar de la Observación General N° 16 del Comité de Derechos Humanos de la ONU, que exige control independiente y proporcionalidad para toda injerencia en las comunicaciones.[10] La indefinición de qué organismos pueden considerarse "*autoridades competentes*" deja abierta la posibilidad de que órganos de inteligencia o de persecución política accedan a esta información sin las garantías mínimas exigibles a una medida de vigilancia estatal, en contravención del artículo 60 de la CRBV y del derecho a la privacidad reconocido en los instrumentos internacionales.

Qué falta: (i) definir taxativamente qué autoridades pueden acceder a la información, mediante ley y no mediante remisión abierta; (ii) limitar el acceso directo y en tiempo real a datos agregados y anonimizados, exigiendo orden judicial motivada para cualquier acceso a datos identificables o susceptibles de asociarse a un usuario, dispositivo o dirección IP concreta; y (iii) crear un mecanismo de transparencia pública sobre el número y naturaleza de las solicitudes de acceso a esta información recibidas y atendidas, siguiendo las mejores prácticas de informes de transparencia.

2. Ambigüedad del concepto de "seguridad de la Nación" y riesgo de debilitamiento del cifrado (artículo 19)

> *Artículo 19: "(…) deberán implementar los mecanismos de criptografía necesarios para salvaguardar la seguridad de la Nación, en estricta concordancia con lo dispuesto en las Leyes que rijan la materia y las directrices emanadas de los organismos competentes."*

Riesgo: el artículo 19 introduce una obligación de implementar "mecanismos de criptografía" orientados a "salvaguardar la seguridad de la Nación", sin definir este último concepto ni acotar su alcance, y remitiendo su desarrollo a "directrices" de organismos no identificados. En el lenguaje técnico de la ciberseguridad, exigencias de esta naturaleza, cuando no se acompañan de una prohibición expresa en sentido contrario, suelen dar cobertura normativa a la instalación de mecanismos de acceso excepcional al tráfico cifrado (conocidos como "puertas traseras" o backdoors) o a la exigencia de claves de desencriptación para fines de inspección estatal.

Por qué representa un riesgo: el debilitamiento del cifrado de extremo a extremo compromete la privacidad de las comunicaciones de la totalidad de los usuarios, por lo que tiene un efecto directo sobre la libertad de expresión y el derecho a buscar, recibir y difundir información, protegido por el

[9] Al respecto, véase M. Díaz Hernández, *Telecommunications and Internet Access Sector: Latin America* (Report to the Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression of the United Nations, Derechos Digitales, 2016), pág. 11, https://archivo.derechosdigitales.org/wp-content/uploads/telecommunications-and-internet-access-sector-latinamerica.pdf.
[10] Comité de Derechos Humanos de las Naciones Unidas, *Observación general n.º 16*.

artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, en la medida en que compromete la seguridad de las comunicaciones de periodistas, personas defensoras de derechos humanos, activistas y ciudadanía en general.[11] Al respecto, la Relatoría Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión ha establecido explícitamente que el cifrado y el anonimato son herramientas esenciales para el ejercicio de los derechos en el entorno digital, y que su debilitamiento generalizado, sin las más estrictas garantías, es incompatible con los estándares internacionales.[12]

Qué falta: La Providencia debe incorporar una cláusula expresa que prohíba exigir a los operadores el debilitamiento, la ruptura o la creación de mecanismos de acceso excepcional (backdoors) al cifrado de extremo a extremo de las comunicaciones de los usuarios. Asimismo, debe precisar que cualquier medida de "seguridad de la Nación" en materia de criptografía debe estar estrictamente definida por una ley formal, motivada, ser proporcional al fin perseguido y estar sujeta a control judicial previo.

3. Ausencia de una ley de protección de datos personales y de una autoridad independiente de supervisión (artículo 19)

Riesgo: el artículo 19 exige que las arquitecturas técnicas de los IXP garanticen la protección de datos de carácter personal "***conforme a los estándares internacionales vigentes*",** pero Venezuela no cuenta actualmente con una ley integral de protección de datos personales ni con una autoridad administrativa independiente encargada de supervisar su cumplimiento, y la propia Providencia no identifica qué órgano sería competente para ello.

Por qué representa un riesgo: una obligación de protección de datos sin ley que la desarrolle ni autoridad que la haga exigible carece de efectividad práctica, porque nadie audita, certifica o sanciona su incumplimiento. Ello resulta especialmente grave frente a la magnitud de los datos de tráfico que la propia Providencia exige recolectar (artículos 23, 24, 26 y 27), y es contrario al principio de efectividad de los derechos humanos (artículo 2 del Pacto Internacional de Derechos Civiles y Políticos), que obliga a los Estados no solo a reconocer formalmente un derecho, sino a garantizar los medios institucionales para su goce efectivo.

Qué falta: como mínimo, mientras no exista una ley de protección de datos personales, la Providencia debe designar expresamente una autoridad, distinta de CONATEL, o con garantías reforzadas de independencia dentro de esta, encargada de supervisar el cumplimiento de las obligaciones de protección de datos derivadas del artículo 19, y remitir a estándares internacionales concretos y verificables (por ejemplo, los principios de minimización, finalidad y limitación del uso de datos).

4. Indefinición de la técnica de *anonimización* de los datos abiertos (artículo 26, numeral 1)

> *Artículo 26.1: obligación de publicar, en un portal de datos abiertos sin necesidad de autenticación, la "matriz de tráfico agregada y anonimizada entre los miembros".*

Riesgo: la Providencia exige la publicación, sin necesidad de autenticación, de una matriz de tráfico "agregada y anonimizada", pero no define qué técnica de anonimización se exige (agregación

[11] David Kaye, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, Consejo de Derechos Humanos de las Naciones Unidas, doc. ONU A/HRC/29/32 (22 de mayo de 2015), párr. 12, https://hchr.org.mx/puntal/wp/wp-content/uploads/2020/06/G1509588.pdf.
[12] Ibíd., págs. 30, 56-60.

estadística simple, k-anonimato, privacidad diferencial, entre otras), ni prevé auditoría independiente sobre su efectividad.

Por qué representa un riesgo: no toda técnica etiquetada como "anonimización" impide efectivamente la reidentificación de personas o patrones de uso específicos; la ausencia de un estándar técnico mínimo, verificable y auditado agrava el riesgo de que datos publicados terminen permitiendo, por reidentificación o correlación con otras fuentes, la asociación de patrones de tráfico con usuarios o instituciones concretas, en un contexto, como el señalado en el numeral anterior, de ausencia de ley y autoridad de protección de datos.[13]

Qué falta: precisar en la Providencia, o en la guía técnica que la desarrolle, el estándar mínimo de anonimización exigible, sujeto a evaluación técnica periódica e independiente, antes de autorizar la publicación de cualquier dato de tráfico en el portal de datos abiertos.

5. Derecho de reunión y asociación: gobernanza multisectorial facultativa y no vinculante (artículo 5)

> *Artículo 5: "La Comisión Nacional de Telecomunicaciones podrá dictar lineamientos para la conformación de una Asociación Civil Multisectorial (…)".*

Riesgo: el artículo 5 prevé la posibilidad, no la obligación, de que CONATEL dicte lineamientos para la conformación de un Comité de Gestión Multisectorial, en forma de asociación civil sin fines de lucro integrada por los sectores público y privado (Administración Pública, operadores de servicios de internet, sector académico, científico, técnico y usuarios), con la finalidad de velar por la neutralidad, aprobar políticas estratégicas y supervisar la gestión del IXP nacional. Sin embargo: (i) su creación es facultativa ("podrá") y no obligatoria; (ii) es la propia CONATEL quien dicta los lineamientos para su conformación y, previsiblemente, para su funcionamiento, sin que la Providencia garantice un número mínimo de representantes de la sociedad civil, la academia o los usuarios, ni reglas base sobre la toma de decisiones; y (iii) al integrar a órganos de la Administración Pública como miembros del propio comité, este no constituye una instancia independiente de gobernanza, sino una instancia tutelada por el regulador.

Por qué representa un riesgo: los artículos 52 y 53 de la CRBV reconocen el derecho de toda persona a asociarse con fines lícitos y el derecho de reunión, respectivamente; el modelo de gobernanza multisectorial de los IXP más exitosos de la región, como IX.br en Brasil, CABASE en Argentina, NAP Colombia y PIT Chile, se caracteriza precisamente porque la participación de la comunidad técnica, la academia y la sociedad civil está garantizada estatutariamente y con capacidad decisoria real, y no queda sujeta a la discrecionalidad del regulador estatal.[14] Cuando la creación de un espacio de participación multisectorial es meramente facultativa y sus reglas de conformación las define unilateralmente la propia autoridad regulada, el derecho de asociación de los sectores no gubernamentales se vuelve ilusorio en la práctica; pueden ser convocados, pero no tienen garantizada una voz vinculante en las decisiones que afectan la infraestructura crítica de Internet del país.

---

[13] Véase Natalia Ponomareva et al., "How to DP-fy Your Data: A Practical Guide to Generating Synthetic Data With Differential Privacy" (arXiv, 2 de diciembre de 2025), https://doi.org/10.48550/arXiv.2512.03238.

[14] LAC-IX, "Posición de LAC-IX sobre la consulta pública de CONATEL", págs. 2-3, https://lac-ix.org/posicion-de-lac-ix-sobre-la-consulta-publica-de-conatel-para-la-regulacion-de-los-puntos-de-intercambio-de-trafico-de-internet-ixp-en-venezuela/.

Qué falta: hacer obligatoria, no facultativa, la creación del Comité de Gestión Multisectorial; garantizar en el propio texto de la Providencia, y no solo por vía de lineamientos discrecionales de CONATEL, una representación mínima y paritaria de la sociedad civil, la academia y los usuarios; dotar al Comité de competencias vinculantes, y no meramente consultivas, en la aprobación de las políticas técnicas del IXP, en particular en materia de neutralidad de red; y precisar que su documento constitutivo estatutario será elaborado y aprobado por sus propios miembros fundadores, y no impuesto por vía de lineamientos unilaterales del regulador.

6. Derecho a elecciones libres y a la participación política: ausencia de salvaguardas en contextos electorales y de protesta

Riesgo: la Providencia no contiene ninguna disposición específica sobre el tratamiento del tráfico de internet durante procesos electorales o manifestaciones públicas, pese a que centraliza el enrutamiento del tráfico nacional en un número reducido de IXP y otorga a CONATEL acceso a su monitoreo en tiempo real.

Por qué representa un riesgo: los artículos 62 y 63 de la CRBV reconocen el derecho de toda persona a participar en los asuntos públicos y el derecho al sufragio mediante elecciones libres, y el artículo 25 del Pacto Internacional de Derechos Civiles y Políticos protege especialmente el debate público sobre asuntos de interés general, entre ellos los procesos electorales. La experiencia comparada demuestra que los cortes, la degradación selectiva o el bloqueo de aplicaciones de comunicación y redes sociales en períodos electorales o de protesta social son una de las formas más frecuentes de restricción indebida de la libertad de expresión y del derecho a la participación política. El Consejo de Derechos Humanos de la ONU ha condenado en diversas resoluciones las medidas que impiden o alteran intencionalmente el acceso a la información en línea, incluidas las adoptadas para influir en elecciones o silenciar la disidencia.[15]

Una infraestructura de intercambio de tráfico centralizada, sin una prohibición expresa de uso discriminatorio en esos contextos, queda potencialmente disponible como instrumento de restricción del debate electoral y de la protesta social, con independencia de que la Providencia no declare ese propósito.

Qué falta: incorporar una cláusula expresa de “no discriminación por contexto” que impida degradar, priorizar o suspender el servicio de internet por razones distintas de las estrictamente técnicas, con mención especial y de protección reforzada a los procesos electorales y a las manifestaciones públicas, y coordinar dicha garantía con el **Consejo Nacional Electoral (CNE)** para asegurar la total disponibilidad y continuidad de las plataformas de información y comunicación ciudadana durante los eventos comiciales.

7. Ausencia de una instancia de control independiente y de evaluación previa de impacto en derechos humanos (artículo 30 y régimen sancionatorio)

[15] Véase Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "Desconectar internet causa daños incalculables: informe de la ONU", 27 de junio de 2022, https://www.ohchr.org/es/stories/2022/06/switching-internet-causes-incalculable-damage-un-report.

La Providencia concentra en CONATEL las funciones de otorgar habilitaciones, imponer obligaciones, supervisar su cumplimiento y resolver las controversias que surjan entre los operadores (artículo 30), sin prever una instancia de apelación o control independiente distinta de la propia Comisión, ni un procedimiento sancionatorio detallado con garantías de audiencia y motivación. Tampoco se exige una evaluación de impacto en derechos humanos como requisito previo a su implementación, en línea con las recomendaciones que, en el ámbito de la regulación de infraestructura de internet, han formulado los relatores especiales de libertad de expresión de las Naciones Unidas.[16] La concentración de funciones normativas, ejecutivas y cuasi jurisdiccionales en un mismo órgano, sin control independiente, es en sí misma un factor de riesgo para el debido proceso de los operadores y, por extensión, para la estabilidad y previsibilidad del entorno en el que se ejercen los derechos analizados en este informe.

CONCLUSIONES

La propuesta de Providencia Administrativa analizada presenta **vicios estructurales de nulidad** al pretender regular por vía sublegal una materia estrictamente sometida a la **reserva de ley orgánica** (arts. 7, 156.28, 187 y 203 de la CRBV). Más allá de este vicio formal, el texto actual configura un **modelo de centralización técnica y regulatoria** que transforma los Puntos de Intercambio de Tráfico (IXP) en un **punto único de control estatal sobre el flujo de información del país**.

Al carecer de salvaguardas explícitas, la normativa habilita la **censura estructural, el monitoreo del tráfico sin control judicial y el debilitamiento de la privacidad de las comunicaciones**. Esto violenta los estándares constitucionales e internacionales más elementales en materia de libertad de expresión, acceso a la información, debido proceso y gobernanza multisectorial de Internet.

PETITORIO

Con fundamento en las consideraciones que anteceden, se solicita a la Comisión Nacional de Telecomunicaciones (CONATEL):

PRIMERO: que reconsidere la vía normativa elegida y, en su lugar, **impulse la elaboración** de un **proyecto de ley orgánica sobre internet**, con participación multisectorial, que sirva de marco habilitante para la regulación específica del internet, en cumplimiento del artículo 203 de la Constitución Nacional.

SEGUNDO: para el caso de que CONATEL decida proseguir con la aprobación de este instrumento sublegal, se **reforme integralmente su articulado** para incorporar las siguientes modificaciones de carácter obligatorio y garantista:

1. **Exclusión de control de contenidos en IPTV y OTT:** Excluir explícitamente a las tecnologías OTT e IPTV de cualquier mecanismo de censura previa, filtrado de catálogos o control de contenidos aplicable a la televisión por suscripción convencional.
2. **Garantía real de Neutralidad de Red (Arts. 2.4, 5 y 18):** sustituir el concepto ambiguo de “neutralidad tecnológica” por el estándar internacional de neutralidad de red. Extender esta

[16] Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, *El impacto de la vigilancia digital en la libertad de expresión en las Américas*, doc. OEA/Ser.L/V/II, CIDH/RELE/INF.33/25 (septiembre de 2025), pág. 93, https://www.oas.org/es/cidh/expresion/informes/vigilanciaRELE.pdf.

obligación expresamente a la relación entre los ISP y el usuario final, tipificando y enumerando de forma taxativa las únicas excepciones técnicas admisibles.

3. **Prohibición de censura en la interconexión (Art. 21):** prohibir expresamente el uso de la infraestructura centralizada del IXP para ejecutar bloqueos, filtrados, redireccionamientos o degradación de tráfico. Supeditar cualquier medida excepcional de interrupción técnica a un procedimiento reglado con control judicial previo.
4. **Voluntariedad de las Redes de Entrega de Contenidos (Disposición Transitoria Segunda):** eliminar la migración obligatoria y establecer que la ubicación de los servidores CDN en las sedes del IXP sea estrictamente voluntaria, protegiendo el pluralismo informativo frente a la concentración física de plataformas.
5. **Garantías en la resolución de dominios (Art. 28):** incorporar una cláusula de salvaguarda que aclare que los nodos Anycast del NIC.VE en el IXP no podrán ser utilizados para bloquear, filtrar o redirigir resoluciones DNS sin orden judicial motivada.
6. **Control judicial para el acceso a telemetría (Arts. 23, 24 y 27):** Definir taxativamente qué organismos constituyen "autoridades competentes". Limitar el acceso en tiempo real exclusivamente a datos agregados y anonimizados, exigiendo orden judicial previa para datos identificables, y obligar a la publicación periódica de informes de transparencia.
7. **Protección absoluta del cifrado (Art. 19):** Prohibir de forma explícita cualquier directriz que exija el debilitamiento, ruptura o creación de accesos excepcionales ("puertas traseras") en el cifrado de extremo a extremo de las comunicaciones de los usuarios.
8. **Estándares de Protección de Datos (Arts. 19 y 26.1):** Designar una autoridad de supervisión técnica independiente de CONATEL para el resguardo de datos y definir un estándar técnico de anonimización robusto y auditable antes de la publicación de matrices de tráfico en datos abiertos.
9. **Ampliación del impacto social y asequibilidad (Arts. 12-16, 20, 31-33):** Extender los beneficios de la "tarifa social" a usuarios vulnerables e instituciones de servicio público (salud, educación), fijando metas claras de cobertura universal y continuidad reforzada.
10. **Gobernanza Multisectorial Obligatoria y Vinculante (Art. 5):** Establecer el Comité de Gestión Multisectorial como un órgano de creación obligatoria, con representación paritaria y garantizada de la sociedad civil, academia y usuarios, otorgándole competencias vinculantes en políticas técnicas y neutralidad de red.
11. **Cláusula de no discriminación por contexto**: Incorporar una salvaguarda de protección reforzada que prohíba expresamente la alteración, corte o degradación del tráfico de internet en contextos electorales o de manifestaciones públicas.
12. **Debido proceso y revisión independiente (Art. 30):** Modificar el régimen sancionatorio para descentralizar las facultades de CONATEL, instituyendo una vía de revisión o apelación independiente, y ordenar una Evaluación de Impacto en Derechos Humanos previa a la puesta en marcha de la normativa.

Por la Organización,

A.C. Espacio Público.