26 de setiembre, 2023
CIT-0039-2023

Señora
Paula Bogantes Zamora
Ministra
Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)
Presente

Asunto: Consideraciones acerca del "Reglamento sobre medidas de Ciberseguridad aplicables a los servicios de telecomunicaciones basados en la tecnología de Quinta Generación Móvil (5G) y superiores", Decreto Ejecutivo Nº 44196-MSP-MICITT.

Estimada señora Ministra:

Reciba un saludo cordial de parte de la **Cámara de Infocomunicación y Tecnología (INFOCOM).**

Los temas relativos a la implementación de las redes 5G, sin duda son de prioritario interés para **INFOCOM** y sus asociados, así como las acciones llevadas a cabo por el país, en materia de **Ciberseguridad y protección de datos** de los habitantes y usuarios de los servicios.

Con relación al reciente **Decreto Ejecutivo Nº 44196-MSP-MICITT**, denominado: ***"Reglamento Sobre Medidas de Ciberseguridad Aplicables a los Servicios de Telecomunicaciones Basados en la Tecnología de Quinta Generación Móvil (5G) y Superiores",*** **(en adelante referido como el "Reglamento"),** desde **INFOCOM** y la industria de telecomunicaciones que ésta representa, respetuosamente, se desea manifestar lo siguiente:

Mediante **comunicado de prensa CP-052-2023, del lunes 28 de agosto**, **INFOCOM** tuvo noticia, por primera vez, acerca de que el Gobierno emitió el referido Reglamento. Ante la justificada inquietud e interés manifestado por parte de los asociados de **INFOCOM**, por conocer mayor detalle sobre el contenido de este importante Reglamento, se le solicitó de inmediato una cita a su persona, para tener un espacio de conversación y le dirigimos el **oficio CIT-0030-2023, de fecha 30 de agosto**, mediante el cual solicitamos que se nos pudiera facilitar el documento, que aún no había sido publicado. En este oficio, mencionamos que **INFOCOM no fue consultada, ni tuvo la oportunidad de participar en un proceso de consulta pública sobre dicho Reglamento**. Finalmente, **el 31 de agosto del 2023,** en el Alcance del Diario La Gaceta, el texto del Reglamento fue **publicado**.

Amablemente, se nos concedió cita el pasado **martes 19 de setiembre** en el MICITT, para que representantes de nuestra Junta Directiva de pudieran reunirse con su persona, y nos acompañó el

señor Hubert Vargas, Viceministro de Telecomunicaciones, el señor Gezer Molina, Director de Ciberseguridad, y otros dos funcionarios del equipo de trabajo.

La Cámara fue clara al externar al MICITT que la **reglamentación emitida no es inocua para la industria de telecomunicaciones que representamos y que se tienen varias consultas e inquietudes sobre el alcance e implicaciones del Reglamento.**

Hemos sido transparentes al comunicar varias de las preocupaciones que tienen los operadores y proveedores de servicios de telecomunicaciones sobre el **impacto del Reglamento en el progreso de sus inversiones; en las gestiones de negocio en el despliegue de sus redes; así como señalar la vinculación de esta normativa en los procedimientos que impulsa el país para el despliegue de redes actuales y para el desarrollo de nuevas tecnologías.**

A continuación, procedemos a detallar formalmente nuestras consideraciones y solicitudes en el presente tema.

I. Consideraciones generales:

En primer lugar, deseamos indicar que **INFOCOM** está de acuerdo y comprometida con aquellos esfuerzos que se puedan realizar para mejorar los niveles de Ciberseguridad en todos los ámbitos aplicables. **La preocupación de las autoridades sobre la Ciberseguridad es absolutamente compartida, válida y necesaria.** El sector de telecomunicaciones en su conjunto, está comprometido para resguardar la seguridad de las redes de telecomunicaciones y siempre ha trabajado arduamente en la implementación de las medidas necesarias para salvaguardar y garantizar la seguridad de las redes que actualmente operan, así como aquellas que se desplegarán en un futuro. Desde la apertura del mercado de las telecomunicaciones nunca se ha producido un ataque o intromisión en las redes de telecomunicaciones del país, con un resultado positivo para los agresores.

De la mano con lo anterior, también es importante manifestar que **INFOCOM** defiende y promueve los **principios de transparencia, la sana competencia y la neutralidad tecnológica.** Estos valores, decididamente reconocidos por nuestra industria, complementan otros principios rectores en el ámbito de las telecomunicaciones, como son: **la competencia efectiva, la no discriminación, y la flexibilidad en la elección de las opciones tecnológicas.**

El país adoptó estos principios desde la promulgación de la *Ley General de Telecomunicaciones*, Ley No. 8642, La *Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector de Telecomunicaciones,* Ley No. 8660; y los hayamos en lineamientos de la OCDE en torno a las políticas de economía digital y expresados como principios regulatorios en el Anexo 13 de los Compromisos Específicos de Costa Rica en Materia de Servicios de Telecomunicaciones, del *Tratado de Libre Comercio entre Estados Unidos, Centroamérica y República Dominicana (CAFTA).*

Es oportuno mencionar sobre este particular, que la Ciberseguridad es una cuestión que trasciende a los operadores de telecomunicaciones y sus proveedores, y que atañe también, muchas veces de manera aún más determinante, el comportamiento y cultura de cuidado y seguridad de los usuarios finales, incluyendo tanto entidades públicas como privadas. Por ende, no se debe entender que la Ciberseguridad es exclusiva responsabilidad de los operadores ni mucho menos, que la adopción de este reglamento, ataque otras vulnerabilidades que exponen al país y las instituciones a ciberataques, como los acontecidos en 2022.

Asimismo, es importante tomar en cuenta que todos los fabricantes de equipos para redes de telecomunicaciones móviles siguen los estándares dictados por la organización internacional 3GPP. Esta organización dicta especificaciones técnicas y de seguridad para equipos de telecomunicaciones. Por otro lado, la GSMA y 3GPP desarrollaron un programa para el aseguramiento de la seguridad de los equipos de red, denominada NESAS. Bajo este programa, se hacen auditorías y pruebas de seguridad en los equipos de red de fabricantes, y busca garantizar la seguridad de esos equipos desde su diseño, desarrollo y uso. En el sitio https://www.gsma.com/security/gsma-network-equipment-security-assurance-scheme-participants/ se puede verificar la lista de fabricantes participantes y en el sitio https://www.gsma.com/security/nesas-results/ se pueden observar los reportes de las auditorías.

Hecha esta salvedad, y compartiendo la preocupación general de la Ciberseguridad que motiva este Reglamento, consideramos que, **de acuerdo con lo establecido en el artículo 361 de la Ley General de la Administración Pública, el mismo debió haber sido consultado entre los actores de la industria de telecomunicaciones, incluyendo los operadores, entre otros, para poder profundizar sobre los aspectos técnicos más relevantes, y las implicaciones en tiempo y costos del despliegue de la red 5G en Costa Rica. El Decreto en cuestión, no presenta ninguna consideración al respecto, como si el mismo fuese a resultar inocuo.**

Para considerar todas las distintas aristas que se pueden ver inmersas en disposiciones de alcance general como el Reglamento bajo estudio, la normativa legal vigente demanda que se realicen las consultas previas a **todas aquellas instituciones y/o interesados que puedan ser potencialmente afectados** con el contenido de la normativa que se emite.

No solo se estipula a nivel de la Ley General de Administración Pública la obligación de consultar el borrador de las disposiciones de alcance general antes de su emisión final, sino que este asunto ha sido ampliamente analizado tanto por la Sala Primera como por la Sala Constitucional de la Corte Suprema de Justicia, según se reseña brevemente a continuación:

> *"El derecho a la participación ciudadana en la toma de decisiones se ha convertido en uno de los pilares fundamentales sobre los que descansa el sistema democrático. (…)*
>
> *Precisamente, uno de los mecanismos ideados para cumplir lo dispuesto en el artículo 9 constitucional es la audiencia pública, que constituye en un medio a través del cual las*

personas interesadas pueden hacer valer sus derechos, participando activamente en temas de relevancia nacional o local, y poniendo en conocimiento de la Administración todas aquellas anomalías o disconformidades en relación con el proyecto que se pretenda desarrollar. Así las cosas, la audiencia pública es un instrumento típico de una democracia madura, mediante el cual se fomente la participación activa del ciudadano en la toma de decisiones públicas. Por su significado, la audiencia debe efectuarse de tal forma que garantice la mayor participación de las personas que puedan verse afectadas, de ahí que cualquier acción u omisión que evite lo anterior, implica una abierta vulneración a los derechos fundamentales de los participantes (véase, entre otras, la sentencia número 2009-018223). (…)

Durante la audiencia pública se les deben otorgar a los participantes todas las facilidades para que se encuentren informados y puedan hacerse escuchar, todo dentro de lo razonable, pues tampoco puede convertirse la audiencia en un obstáculo o un recurso para impedir que se dé oportuna resolución a determinada gestión (…)" (Sentencia número 2013-17305, de las once horas treinta y dos minutos del veinte de diciembre del dos mil trece. Sala Constitucional)

Toda nueva regulación tiene un impacto sobre la actividad que pretende regular; precisamente como hemos indicado, no pasa inadvertida. En este caso en particular, el Reglamento tiene, entre otras afectaciones, un efecto práctico de excluir para el despliegue de redes 5G, algunos oferentes del mercado de esta tecnología para redes móviles; en un mercado que es muy limitado a nivel mundial.

En Estados Unidos, cuando se implementaron medidas como las incluidas en este Reglamento, en primer lugar, se hizo una consulta pública previa a todos los participantes del mercado (operadores y fabricantes entre otros). Segundo, las autoridades estimaron el costo adicional que las medidas implicarían para los operadores. Tercero, se estimó como razonable un plazo de diez años para la sustitución de equipos y, en cuarto lugar, se implementó un programa de financiamiento para dicha sustitución, a través del fondo de servicio universal.

El Reglamento conlleva dos efectos inmediatos: En primer lugar, habrá una limitación del mercado nacional de proveedores. La competencia en este mercado -en todo el mundo, y particularmente en América Latina- ha jugado un papel fundamental en los últimos años en cuanto a innovación y mejores precios, que a su vez se ha traducido en mejores condiciones para los usuarios finales y empresas.

Por otro lado, en una primera fase, las redes de 5G se edifican sobre la base de los elementos de red de 4G. Esto se conoce como **red 5G NSA (Non-Stand Alone).** Este tipo de red permite a los operadores desplegar más rápida y eficientemente los servicios 5G. De acuerdo con los estudios de la GSMA, el 80% de los operadores en el mundo optan iniciar con redes 5G NSA. Todos los operadores del país, en mayor o menor medida, mantienen en sus redes 4G elementos de red de los proveedores que

serán limitados del mercado. Esos elementos de las redes que actualmente operan, pretenden ser claves para el despliegue de red 5G. Por lo tanto, **es impreciso señalar que el Reglamento únicamente regula los elementos de red que se desplegarán en un futuro, puesto que muchos de los elementos de red para el despliegue de 5G en el país, ya se encuentran operativos para las redes 4G.**

De acuerdo con las disposiciones del Reglamento, será necesario remplazar estos elementos de red ya existentes, y sobre los cuales se han hecho inversiones cuantiosas. Esto a su vez, genera incertidumbre sobre esas inversiones efectuadas y retrasos en el despliegue de la tecnología 5G.

Las redes móviles operan a gran escala y cualquier restricción en la cadena de suministro tiene efectos en el mercado y repercute en los usuarios finales. Por lo tanto, es fundamental considerar los impactos en toda la industria, antes de tomar decisiones que pueden derivar en retrasos tecnológicos, y afectación de precios y condiciones para los usuarios finales, personas y empresas.

La **Ciberseguridad** es un elemento clave para el despliegue de nuevas redes de telecomunicaciones y la operación de las actuales. Existen desafíos que el Reglamento pretende abordar; pero también **es necesario un análisis minucioso y un enfoque integral para minimizar cualquier impacto negativo en las inversiones, en la capacidad, forma y velocidad de implementación de la tecnología 5G, en la calidad de los servicios de telecomunicaciones móviles actuales y futuros, así como en su asequibilidad.**

Las redes 5G proveerán una plataforma de telecomunicaciones que permitirá la implementación de servicios digitales innovadores, que no serían posibles sin esta tecnología; lo cual dará espacio para nuevos modelos de negocio, permitiendo crear fuentes de trabajo y movilizar la economía.

Nos preocupa la incidencia de las medidas adoptadas y, en ese sentido, los impactos que estamos puntualizando en los costos y eventuales retrasos en el proceso hacia la ruta de 5G en Costa Rica, que incidirán negativamente en las inversiones, inhibiendo este mercado emergente; lo cual va en detrimento de la economía, las personas y las empresas.

El fortalecimiento de los servicios de telecomunicaciones es de vital importancia para el desarrollo de todas las demás industrias. Parte importante de un desarrollo sostenible, es la participación de las empresas de todos los niveles, de una manera justa, y **basados en los principios rectores que han formado parte del marco normativo costarricense por décadas.**

II. Consideraciones técnicas específicas:

Mencionaremos a continuación, algunos aspectos que consideramos críticos de analizar detenidamente, buscando el fin de **mantener un mercado abierto y competitivo** en la industria de telecomunicaciones del país.

1. El Reglamento omite previsiones sobre los impactos en los despliegues de infraestructura ya realizados.

2. No queda claro el proceso de ajuste o transición que deben seguir los operadores que tienen equipos o infraestructura de proveedores que se ubican “excluidos”, según las referencias del Reglamento.

3. El Reglamento no dimensiona los impactos en el plazo para el proceso de subasta y la entrada en operación de la tecnología 5G en Costa Rica.

4. El Reglamento no dimensiona los impactos y alcances de las limitaciones establecidas, y ajustes que serán necesarios de efectuar, para los operadores de telecomunicaciones, tanto para redes móviles como para redes fijas. Las redes de telecomunicaciones son cada día más convergentes, esto resulta especialmente aplicable para 5G, por lo que cualquier regulación pensada para un entorno puede terminar afectando otras capas o elementos del sistema.

5. Consideramos que se afecta la competencia en el mercado por la violación al principio de neutralidad tecnológica.

6. Sobre lo estipulado en los **Artículos 6, 8, 9 y 10, acerca de los Estándares**, consideramos que se establece el requerimiento de un estándar nuevo, el **SCS9001**, de la Asociación Americana de la Industria de Telecomunicaciones (TIA), que se le impone tanto a los proveedores de equipos, como a los proveedores de servicios de telecomunicaciones. A un año de existencia del estándar, ya se está exigiendo, aunque carece de madurez; y no necesariamente corresponde al ecosistema de servicios móviles; generando la exclusión de ciertos proveedores, sin aportar al mejoramiento de la seguridad en las redes 5G. El desarrollo de un ecosistema móvil, basado en un estándar que no fue hecho para éste, requiere una curva de adopción más compleja para todos los participantes de la industria, lo que conlleva tiempo y costos en su adopción.

7. Por lo anterior, es recomendable que se utilicen los mecanismos y estándares maduros y propios de la industria de tecnología móvil, para garantizar la seguridad de las redes. En ese sentido, **la industria de telecomunicaciones, a través de INFOCOM, puede aportar mucha información acerca de estándares integrales y mejores prácticas, por ejemplo, las emitidas por la GSMA con el esquema NESA (Network Equipment Security Assurance);** y de otras referencias en diseño y desarrollo de especificaciones técnicas, que incluyen recomendaciones y esquemas para garantizar la seguridad de los equipos de telecomunicaciones. **Existen otros ejemplos de estándares o certificaciones que se utilizan para garantizar la seguridad de los procesos y productos; que también permiten una implementación de redes seguras;** y que han sido ampliamente adoptados tanto por los fabricantes de redes 5G, como por los principales operadores de servicios móviles en el mundo. Se extraña que, en el proceso de construcción del Reglamento, no se hubiera propiciado una discusión técnica para elegir los estándares de ciberseguridad mencionados.

8. Se ha mencionado sobradamente en distintas opiniones surgidas con posterioridad al conocimiento del Reglamento, sobre la referencia que el mismo impone acerca del ***Convenio de Budapest***, y al respecto, consideramos importante tener claridad de que **no es un estándar internacional de ciberseguridad**, no tiene provisiones de ciberseguridad, ni redes de telecomunicaciones, es un convenio emitido hace más de veinte años (cuando apenas iniciaba la tecnología 3G) dirigido a recomendar una tipificación legal estándar de crimen cibernético relacionado con la confidencialidad, integridad y disponibilidad de sistemas, redes y datos informáticos y cooperación internacional entre autoridades judiciales en la persecución de ese tipo de delitos. Precisamente por el carácter integral de la Ciberseguridad en todos sus extremos, como hemos comentado anteriormente, incorporar esta obligación dentro del reglamento al catalogarlo como un riesgo alto, no evitaría que ciberdelincuentes radicados en países no firmantes, ataquen otras vulnerabilidades como los mismos usuarios finales. La pregunta es sí realmente, entiendo esta integralidad, la incorporación de esta obligación en este Reglamento con las implicaciones en materia de infraestructura actual y mercado de suministros, es efectiva para los fines que se persiguen.

9. Se reitera que el Reglamento impone limitaciones y restricciones para los operadores, en cuanto al diseño de sus redes y escogencia de sus proveedores. **No se infiere del Reglamento, un criterio claro para diseñar el modelo de diversificación y planificación de la red que cada operador debe seguir, lo cual además resultaría intrusivo en su proceso;** por lo que la regulación carece de seguridad jurídica y técnica en el eje de sus disposiciones. Precisamente, las decisiones estratégicas de los operadores son las que contribuyen a que los usuarios obtengan ofertas y servicios diferenciados y acorde a sus necesidades; posibilidad que se verá mermada con la imposición de este Reglamento.

10. Siempre en referencia a la estrategia que cada operador implementa para su red, **no debe olvidarse que cada uno considera la interoperabilidad y/o sinergia con redes como el 4G, o sistemas y/o plataformas existentes,** entre otros elementos o capas de la red. Esto permite en el ámbito de mercado, acelerar su lanzamiento y ofertas comerciales, en una forma atractiva para los usuarios.

11. **Considerando que todos los equipos de la red intervienen en el transporte y gestión de los datos de 5G,** al forzar el cumplimiento de lo dispuesto en el Reglamento, en cada elemento que expida datos de 5G, se está infiriendo que los equipos del proveedor, considerado de Alto Riesgo, deben ser reemplazados, sea cual fuere el lugar de la red en que se encuentren, requiriendo para ello inversiones mucho mayores y tiempos de implementación más prolongados.

12. Es criterio de nuestros asociados que nuestro marco normativo, y específicamente la *Ley N°8660 de Fortalecimiento y modernización de las entidades públicas del sector de telecomunicaciones,* dispone que el diseño de redes públicas debe hacerse de conformidad con las condiciones técnicas, jurídicas y económicas que permitan su **interoperabilidad**. La entidad que podría

establecer estas condiciones sería SUTEL. Un detalle interesante es que la Sala Constitucional examinó el Artículo 42 de la Ley General de Telecomunicaciones y que se utiliza como base normativa para reglamentar la imposición de condiciones de adquisición de infraestructura a los operadores. La Sala señaló (Exp: 08-003439-0007-CO) al respecto de los artículos 42 y 43 de la referida Ley, que no existe inconstitucionalidad, siempre y cuando, se entienda que lo que desarrollaran las normas reglamentarias son cuestiones meramente operativas. La SUTEL sí tiene competencia para imponer diseño de redes a operadores (Artículo 75 de la Ley No. 8660).

13. Evidentemente, el Reglamento impone condiciones en ese ámbito; por lo que constituye un aspecto importante de analizar dentro de las competencias de cada entidad, del Rector y Regulador.

14. El Reglamento impone condiciones de adquisición de tecnología violentando el Artículo 46 de la Constitución Política. El precepto consagrado en nuestra legislación más bien se orienta hacia la libertad de adquisición de cualquier tecnología. Así lo menciona el CAFTA cuando hace referencia los principios de "***Flexibilidad en las Opciones Tecnológicas***", que obliga a que Costa Rica no impedirá que los proveedores de servicios públicos de telecomunicaciones tengan la flexibilidad de escoger las tecnologías que ellos usen para suministrar sus servicios, sujeto a los requerimientos necesarios para satisfacer los intereses legítimos de política pública. Este principio de **"neutralidad tecnológica"** es también recogido en nuestra Ley General de Telecomunicaciones, en su Art. 3, inciso h), que lo define como la posibilidad que tienen los operadores de redes y proveedores de servicios de telecomunicaciones para escoger las tecnologías por utilizar, siempre que estas dispongan de estándares comunes y garantizados, cumplan los requerimientos necesarios para satisfacer las metas y los objetivos de política sectorial y se garanticen, en forma adecuada, las condiciones de calidad y precio a que se refiere la Ley.

15. Continuando con el impacto que tiene la aplicación de este Reglamento en el operador que desee desplegar la tecnología 5G, se encuentra el hecho de que el mismo debe enfrentarse a tomar una decisión: puede utilizar los elementos de red que sabe que serán limitados con el Reglamento, pero tendrá que cambiarlos, en el mejor de los casos, en una ventana de 5 años. Este cambio tendrá un costo importante y desde este momento implica un riesgo: ¿Cuál será el soporte y compromiso real que tenga un proveedor de equipamiento que ya sabe que su negocio no puede seguir en el país? Otra decisión que se enfrenta es arrancar con la mayor cantidad de elementos de red, con uno o varios proveedores que no están prohibidos de acuerdo con el Reglamento. Pero esto implica: a) asumir un costo financiero que no estaba previsto y, b) el plazo del proyecto de cambiar estos elementos de red. **De lo anterior, es indudable que el despliegue de 5G tendrá un costo mayor con la entrada en vigor del Reglamento y que también se requerirá de tiempo adicional para el despliegue.**

16. Costa Rica es un país con ARPU´s bajos y con tendencia decreciente en el mercado móvil. Para 2022, la SUTEL estima que el ARPU promedio es de 4.689 colones, menos de US$9. En EEUU, se

estima que el ARPU promedio está arriba de los $35. La realidad es que los ingresos del sector móvil siguen decreciendo a partir de esta misma tendencia de precios, lo que condiciona las inversiones futuras en nuevas tecnologías (como 5G) y futuros despliegues. Si a esta realidad de presión financiera introducimos además una presión adicional tanto en CAPEX como en OPEX por: a) migración forzada de elementos de red y, b) un eventual incremento de precios en equipamiento ante la salida de proveedores más agresivos en precio; **tenemos un entorno que pone en peligro la sostenibilidad del sector, en momentos en que se requiere más bien asegurar las condiciones para que el país siga adelante en el despliegue de red 5G.**

17. La **SUTEL**, basándose en su "**Guía para la Evaluación de la Regulación desde la Perspectiva de la Competencia",** realizó el análisis de la propuesta de Reglamento, encomendado por el MICITT, y emitió el informe de fecha 17 de agosto del 2023, 06900-SUTEL-CS-2023. En cuanto al análisis de la razonabilidad y proporcionalidad de las restricciones encontradas, la **SUTEL** indicó que **varios de los artículos del Reglamento, no cumplían con criterios de predictibilidad, proporcionalidad, transparencia y eficacia**. Concluyó, entre otros puntos, lo siguiente:

- *La normativa propuesta tiene el potencial de limitar la posibilidad de ciertos tipos de operadores o proveedores de telecomunicaciones para prestar sus servicios, al condicionar la asignación de concesiones para uso y explotación del espectro radioeléctrico para redes y servicios de telecomunicaciones 5G, así como establecer características específicas, no estrictamente de índole comercial, que deberán adoptar los operadores y proveedores de telecomunicaciones al dotarse de bienes y servicios requeridos en la implementación de sus redes 5G.*

- *La normativa propuesta tiene el potencial de elevar los costos de todos operadores o proveedores basados en la tecnología 5G, producto de la aplicación de estándares establecidos en la normativa, así como de eventuales sustituciones de equipos, productos y servicios.*

- *La normativa propuesta tiene el potencial de propiciar la reducción de los incentivos de las empresas para competir, al no establecer criterios claros y libres de ambigüedades conducentes a la presentación de los resultados de los análisis de riesgos y la clasificación de estos como altos, además de no detallar el procedimiento y cualquier otro elemento con el fin de ordenar la ejecución de auditorías de ciberseguridad con cargo al auditado.*

III. Petitoria:

1. Por lo expuesto anteriormente, es que **INFOCOM solicita la atención de las observaciones anteriormente expuestas**, tal como le indicamos en nuestra reunión previa, con el ánimo de construir y procurar una normativa justa y conveniente para el desarrollo de la industria de telecomunicaciones que representamos.

2. **Solicitamos conformar las mesas de trabajo o talleres** con el propósito de analizar las posibles modificaciones que podrían implementarse en el reglamento vigente. Esta solicitud se fundamenta en la necesidad de mitigar los posibles efectos negativos que podrían derivarse de las estipulaciones planteadas, tal como se detalló en los puntos anteriores. Esta iniciativa persigue dos objetivos fundamentales que consideramos de vital importancia en este contexto:

   2.1. En primer lugar, buscamos garantizar la tutela efectiva de los derechos constitucionales de participación ciudadana en la toma de decisiones que puedan incidir en los intereses del colectivo y en la industria de las telecomunicaciones en su conjunto. **La industria de las telecomunicaciones desempeña un papel transversal en el desarrollo económico de nuestra nación y, como tal, es crucial que los cambios regulatorios se realicen de manera participativa y transparente.**

   2.2. En segundo lugar, nuestra petición también tiene como objetivo identificar los parámetros técnicos adecuados que sean acordes a nuestro entorno. Esto permitirá que podamos elevar los niveles de ciberseguridad en el país de manera efectiva y con un enfoque más integral, sin que ello suponga un obstáculo para el desarrollo de las nuevas tecnologías, las cuales son esenciales en la coyuntura actual. Lo anterior se explica en que **es necesario dotar de una mayor seguridad jurídica y técnica** para la industria y los operadores de telecomunicaciones, para que pueda tenerse certeza de las implicaciones y efectos que tendrá este Reglamento.

Agradecemos de antemano, su atención a las consideraciones expresadas y petitoria realizada.

Su respuesta y cualquier notificación futura sobre este tema, puede ser dirigida al correo electrónico: presidencia@infocom.cr, a la atención del suscrito, con copia a: aramirez@infocom.cr, a nuestra Directora Ejecutiva, Ana Lucía Ramírez.

Atentamente,

MARIO ALBERTO MONTERO CUEVAS (FIRMA)

Digitally signed by MARIO ALBERTO MONTERO CUEVAS (FIRMA)
Date: 2023.09.27 16:48:58 -06'00'

MARIO MONTERO CUEVAS
PRESIDENTE
CÁMARA DE INFOCOMUNICACIÓN Y TECNOLOGÍA (INFOCOM)

c.c. Sr. Federico Chacón. Presidente del Consejo Directivo. SUTEL
Sr. Hubert Vargas. Viceministro de Telecomunicaciones. MICITT
Junta Directiva. INFOCOM
Comisión de Entorno Regulatorio y Competencia. INFOCOM
Comisión de Ciberseguridad. INFOCOM
Archivo