

San José, 18 de Setiembre de 2024

**Señora
Johana Obando Bonilla
Diputada de la Asamblea Legislativa de Costa Rica
PRESENTE**

Asunto: Consulta Proyecto Expediente N.º 23292

Redactan:

Lic. Olger Ernesto Rodríguez Calvo - Especialista en Derecho Digital y Tecnologías Emergentes

Lic. Miguel Rodríguez Espinoza – Master en Derecho de las Telecomunicaciones y Tecnologías de la Información

Estimada doña Johana:

En atención a la audiencia sobre el proyecto del proyecto de ley, denominado, "*Ley De Ciberseguridad de Costa Rica*", tramitado bajo expediente legislativo número 23292, se manifiesta lo siguiente:

En la actualidad, producto de la excesiva cantidad de normativa oscura o ambigua, es misión de los operadores jurídicos completar la labor del legislador y son ellos quienes en última instancia terminan expresando lo que el juez o cualquier otro operador jurídico desea, intuye o interpreta; esto, desafortunadamente es el resultado de un acto de delegación de la facultad que tiene el Legislador.

Por ende, previo a la emisión de normativa se debe tomar en cuenta la sistematización de esta de conformidad al entorno normativo en la que debe desenvolverse, como señala GARCIA ESCUDERO, la estructura o sistematización de la ley determinada por criterios de orden lógico, tiene como finalidad, facilitar la localización de cada precepto en el conjunto del texto normativo. (*García-Escudero Márquez, Piedad, "Manual de Técnica Legislativa", editorial Aranzadi, S.A, Navarra, 2011, p. 97*)

I. CONSIDERACIONES DE FORMA

Desde este punto, es claro, que una mejor formulación del texto jurídico le permite al legislador integrar aspectos fundamentales de la realidad social, política y económica que se requieren previamente a la hora de preparar los proyectos de ley, siendo necesario mejorar la propuesta:

- Encabezado. Va precedido por el título: PROYECTO DE LEY, que es invariable, asimismo con las justificaciones necesarias que dan vida a la propuesta normativa.
- Articulado. La unidad básica de un proyecto de ley debe determinar de forma clara el objeto o fin de la propuesta, ámbito de regulación (que va a regular), definiciones si así es necesario, y si es un cuerpo normativo extenso determinar un capitulado que sea claro, y entendible para las personas lectoras, desarrollando de manera amplia procesos y subprocesos en los cuales es aplicable la regulación propuesta
- Transitorios: Cuando la normativa viene a modificar situaciones jurídicas consolidadas. (ultraactividad de la norma)

En este punto, al ser normativa que establece un ámbito que nos interesa mejorar, deben darse procesos y subprocesos de regulación, así como sanción por incumplimiento.

II. CONSIDERACIONES DE FONDO

En el entorno disruptivo en el que nos desarrollamos, nos es difícil pensar en un mundo sin conectividad, a tal punto que ha influido en cuanto a la nueva concepción de derechos fundamentales que ha sido tutelados con el denominado “constitucionalismo multinivel”.

En ese orden de ideas, es interesante observar que, en los últimos años, que a nivel constitucional y convencional se ha dado un reconocimiento al acceso a internet como un derecho humano fundamental, de acuerdo con el modelo de interacción laboral, educativo, familia, negocios, y otros aspectos, han mutado a un ecosistema digitalizado, volviendo de primera necesidad la interconexión y determinar un entorno seguro.

Los adelantos tecnológicos como lo ha sido la conexión de internet ha marcado el nuevo paradigma de ser omnipresentes en actividades que ya son habituales, como la utilización del correo electrónico, las redes sociales, plataformas de compra, son manifestaciones que marcan una nueva forma de visualizar los derechos fundamentales cambiando su ejercicio, acceso a la información, libertad de asociación, libertad de expresión y pensamiento, el derecho a la educación, la salud, eso sí demostrando gran vulnerabilidad en el derecho a la intimidad de las personas.

En ese orden de ideas, un servicio universal que todos los Estados deben garantizar a sus ciudadanos a través de inversiones estatales, políticas, sociales y educativas, elecciones de gasto público. Diferentes fuentes reconocidas, como la UIT, GSMA Intelligence y Eurostat, informan que ha incrementado la cantidad de personas que utilizan tecnologías conectadas, alrededor de 5.44 billones a principios de abril de 2024, lo que equivale al 67,1 % de la población mundial.

La Asamblea General de la Organización de las Naciones Unidas (ONU) en el año 2011 declaró el acceso a internet como un derecho humano siendo una herramienta que fortalece el crecimiento y el progreso de la sociedad en su conjunto. (Ver informe denominado tendencias claves y los desafíos que enfrenta el acceso a internet como derecho universal) La posibilidad de que exista una cuarta generación de derechos humanos relacionada con el mundo digital se encuentra condicionada al cumplimiento por parte del Estado de promover las ventajas y beneficios que representa para cada persona, sociedad, entidades públicas y privadas Estado la interconectividad como acceso ahora al quehacer diario.

Pero no sólo eso, el Estado debe garantizar que toda persona pueda conectarse a la Internet viéndolo desde el punto de vista universal, para lo cual es insoslayable la determinación de una política pública y legislación, que no crea platonismos jurídicos, sino que pueda ejecutarse acorde al país a desarrollar, que puede ser de manera paulatina para que sea efectiva.

En cuando al ordenamiento jurídico emitido al efecto en España, debemos primeramente artículo 24 de la Constitución Política, nos señala el principio de autodeterminación informativa su aplicabilidad y limitaciones del ciberespacio en cuanto al uso de tecnologías que no respeten dicho derecho.

El derecho de acceso a internet como la base de los derechos digitales que son de un acceso universal, accesible, de calidad y claro la transparencia y no discriminación, esto pensando a todo el colectivo de personas que forma en este caso la sociedad costarricense.

El texto no establece de forma clara los tipos que ámbitos del ciberespacio que pasará a fiscalizar Estado, asimismo es necesario determinar los procesos y subprocesos que tendrá la entidad competente, no debe solamente determinar el ámbito competencial al Gobierno Central, sino en el mundo digital que coexistimos, se debe dar la exigencia del cumplimiento de normas de seguridad de la información por parte de Administración Pública y toda persona física o jurídica que se encuentre en el manejo de información propia y de terceros en todos los niveles.

Si es necesario tomar en cuenta, legislación comparada como el numeral 31 bis sobre la responsabilidad de las personas jurídicas en casos de ciberdelincuencia, así como la obligación de tener Sistemas de Seguridad de Información de acuerdo con los UNE/ISO, que son de implementación necesaria. no solo para atenuar posibles responsabilidades, sino también para mejora continua en combate de la ciberdelincuencia.

Se pudo detectar asimismo que el proyecto en estudio pretende crear una Dirección Nacional de Ciberseguridad que sería un órgano con desconcentración mínima dentro del Poder Ejecutivo, cuyas funciones lejos de ser fiscalizadoras son directivas y con un presupuesto insuficiente para las funciones que se le establecen, lo cual conllevaría un peso adicional e innecesario para el Estado, lo cual va en contra de las políticas de ahorro público; claro está, que si fuera una inversión necesaria se tendría que hacer, sin embargo, por lo que se dirá más adelante no lo es.

El ámbito de aplicación es extremadamente limitado e insuficiente al establecerse para “todos los Ministerios y sus órganos desconcentrados (adscritos)”. En este sentido se debe recordar que el sector público es mucho más amplio que esto y que realmente la mayor necesidad de fiscalización en muchas ocasiones no está en el gobierno central sino en los desconcentrados, por ejemplo, las Municipalidades, órganos desconcentrados, entidades autónomas, etc., así como que estas mencionadas manejan mucho más información y de

mayor sensibilidad que los Ministerios y sus órganos desconcentrados; esto viene a generar una insuficiencia en la aplicación de la normativa que es completamente evitable.

En el mismo sentido del párrafo anterior, se procedió a estudiar la posibilidad de ampliar el ámbito de aplicación para optimizar el alcance de la normativa y se llegó a la conclusión que de la forma que está redactado este proyecto, determinando una “dirección” esto sería legalmente inviable en respeto a la autonomía de las diferentes instituciones y órganos, sin embargo, como se dirá más adelante en las recomendaciones esto es absolutamente evitable cambiando el esquema de uno “director” a uno “fiscalizador”, de tal suerte que cada institución u órgano regulado sería que dirija sus procedimientos bajo un marco normativo y respondiendo a una autoridad fiscalizadora.

III. RECOMENDACIONES

Tomando todo lo anterior en consideración, se recomienda la redacción de un texto sustitutivo, que determine una entidad competente para la emisión de criterios y requisitos de Ciberseguridad, así como la **fiscalización** respectiva de cumplimiento en todos los ámbitos, social, cultural, educativo, fiscal, entre otros, con las atribuciones y obligaciones para cumplir sus fines, considerando que la Dirección propuesta tiene, como ya se indicó, una competencia exageradamente reducida y permanece como dependiente del Gobierno Central, por lo que es necesaria su descentralización de toda entidad estatal, bajo el principio de probidad regulado en LGAP, siendo que la misma Administración Pública es regulada en el tema que nos ocupa.

En ese orden de ideas, es necesario un ente con la especificidad del ámbito regular, con atribuciones legales de exigir a sus regulados, procedimientos de prevención y sanción de prácticas fuera de y determinar las sanciones correspondientes, así como la independencia administrativa para tener mayor objetividad.

Por las razones citadas anteriormente, es de carácter insoslayable, que se reoriente el cuerpo normativo puesto a consideración y se mejore su redacción, siendo de vital inclusión, lo señalado por esta Comisión de Derecho Informático.

Quedamos a sus órdenes para cualquier colaboración que requieran de nosotros.

Atentamente,

Lic. Olger Ernesto Rodríguez Calvo

Lic. Miguel Rodríguez Espinoza

**Por la Comisión de Derecho Informático del Colegio de Abogados y Abogadas de
Costa Rica**