09 de setiembre del 2019
MICITT-DM-OF-612-2019

Señores
Comisión Permanente Especial de Seguridad y Narcotráfico
Asamblea Legislativa de la República de Costa Rica

Estimados señores:

Reciba un cordial saludo. En atención a su oficio N° AL-21187-CPSN-OFI-0064-2019 de fecha 04 de julio del 2019, en el cual solicita al Ministerio de Ciencia, Tecnología y Telecomunicaciones enviar las observaciones al proyecto de ley N° 21.187, denominado: "*LEY PARA COMBATIR LA CIBERDELINCUENCIA"*.

Al respecto, y de acuerdo con lo indicado por el señor Jorge Mora Flores, Director de Gobernanza Digital, por medio del documento N° MICITT-DGD-MEMO-024-2019, me permito remitir las observaciones de índole jurídico-técnico, de los artículos del proyecto donde existan observaciones que consideramos necesario tomar en consideración:

***ARTÍCULO 1- Definiciones:***

En muchos de los casos las definiciones son confusas, al ser términos técnicos los cuales, para ser establecidos de manera correcta, no se definen de esa forma. Se presentan definiciones de áreas del conocimiento ajenas al ámbito criminal, que se generan confusión, por citar algunos problemas. Entre estas definiciones están datos tráfico, datos de localización, datos informáticos, datos de abonado, que deben ser definiciones técnicas pero la forma en que están planteadas hace que colisionen entre sí.

Igualmente, las definiciones de delito informático, cibercrimen, delito computacional, siendo de naturaleza igual los definen de manera distinta. Asimismo, se presentan problemáticas en materia de definiciones de datos sensibles que no refiere a la normativa existente en el país en materia de protección de datos.

Consideramos que en su totalidad las definiciones deben ser revisadas, y para las que corresponden a materia técnica, debe buscarse la definición correcta, de manera que

correspondan a una definición como lo establece la ciencia y el arte en estos campos. Las definiciones de términos del ámbito criminal deben revisarse para no generar confusión entre los diferentes conceptos, además que las mismas sean concordantes con el marco normativo nacional existente.
También se recomienda que su construcción de estas sea acompañada por expertos en informática en el campo de la ciberseguridad y expertos en el ámbito del derecho penal y protección de datos para lograr definiciones óptimas.

***ARTÍCULO 2- Difusión de información de interés público:***

**Para efectos de aplicación de la presente ley y los tipos penales informáticos contenidos en el Código Penal, no constituirá delito:**

***3- La publicación reiterada e insistente de reportajes o denuncias de interés público***

El inciso 3 del artículo 2 no parece necesario, siendo que el inciso 1 señala que:

> *1- La publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.*

Por lo que dicha excepción a la información de interés público se encuentra contemplada en el inciso 1 de la propuesta, no siendo necesario esta reiteración.

Se recomienda corregir para que quede claro:

*Para efectos de aplicación de la presente ley y los tipos penales informáticos contenidos en el Código Penal, no constituirá hecho ilícito:*

1. *Buscar, investigar, recibir, y difundir por cualquier medio y de cualquier forma, informaciones o ideas de toda índole o sobre cualquier tema o situación sobre las que la sociedad pueda tener algún interés.*

2. *La búsqueda, recepción, difusión o transmisión de informaciones u opiniones de interés público. Tampoco la difusión o transmisión de hechos o documentos que previamente hayan sido de conocimiento público o que hayan sido previamente difundidos por cualquier medio o de cualquier otra forma.*
3. *La búsqueda, recepción o difusión de documentos públicos, datos contenidos en registros públicos o de bases de datos públicos.*

*No se podrá impedir o restringir el acceso irrestricto de todas las personas a la información en poder del Estado; o relativa al Estado, o sobre la que la población tenga interés. Tampoco se podrá impedir o restringir por cualquier vía, el derecho irrestricto de las personas a indagar y cuestionar, exponer y reaccionar, a coincidir y discrepar, y al derecho de confrontar, publicar y transmitir información sobre cualquier hecho de relevancia pública, o que concierna a funcionarios públicos o a personajes públicos.*

***ARTÍCULO 3- Investigación criminal:***

***Para efectos de aplicación de la presente ley y los tipos penales informáticos contenidos en el Código Penal, no constituirá delito:***

***1- La ingeniería social por parte de las autoridades en el marco de una investigación criminal.***
***2- La comisión de una acción típica contenida en un tipo penal informático presente en el Código Penal o esta ley, si la misma ha sido realizada con la autorización de un juez penal.***
***3- La captación de datos de ubicación geográfica obtenidos en el desarrollo de los actos y procedimientos de carácter policial o judicial llevados a cabo en el marco o en el transcurso de investigaciones de naturaleza informática, electrónica o telemática, mediante el uso necesario de herramientas electrónicas, programas o aplicaciones informáticas, aparatos electrónicos o sistemas de telecomunicaciones.***

El artículo 3 inciso 1 puede incluir actividades que ingresan dentro del tema de delito experimental por medio de agente provocador y agente encubierto. Es de recordar que en nuestro ordenamiento no es admisible realizar mecanismos para tentar a las personas a cometer hechos delictivos, y menos provocar su consumación en circunstancias en que

la persona inducida no se había planteado esta posibilidad; por lo que permitir o diseñar la posibilidad de generar ingeniería social para la investigación criminal puede generar un conflicto en materia de agente provocador, y que las investigaciones puedan verse afectadas, se recomienda revisar si la normativa existente en materia procesal penal permite tener las herramientas necesarias para investigar sin necesidad de contemplar el indicar directamente acciones de ingeniería social.

***ARTÍCULO 4- Comisión Nacional de Lucha contra la Ciberdelincuencia:***

En este caso crear una comisión por ley imposibilitaría la actualización e inclusión de instituciones de manera ágil, que puedan incorporarse al trabajo de una comisión en esta materia. No es una práctica recomendada crear comisiones por ley. Se recomienda no incluir este artículo y que, en su defecto, se genere por medio de una directriz u otra figura desde el Poder Judicial que permita formar la comisión, pero no por ley.
En dado caso que se quiera mantener dicho artículo no se encuentra en la lista de instituciones el Colegio de Profesionales en Informática y Computación, ni representantes del sector privado, ni de sociedad civil en materia de tecnologías y ciberseguridad.

***ARTÍCULO 5- Protocolos de cooperación en la investigación de delitos informáticos con proveedores extranjeros:***

***La Comisión Nacional de Lucha contra la Ciberdelincuencia convocará a representantes de los proveedores esenciales de servicios electrónicos, sean nacionales o extranjeros, con el fin de crear de forma conjunta protocolos de cooperación para la investigación de delitos informáticos o cualquier otro delito que sea cometido con la ayuda de las nuevas tecnologías o donde exista evidencia digital en control del proveedor de servicio.***
***Deberá crearse un protocolo especial para cooperación en casos de urgencia, por estar en peligro las evidencias digitales, la vida, la salud o la integridad física de una o más personas.***

En este artículo no queda claro que son proveedores esenciales a nivel nacional e internacional. Se recomienda revisar el alcance de este artículo siendo que podría ser

imposible convocar a todos los representantes esenciales a nivel mundial de servicios electrónicos, además de definir claramente qué se entiende por proveedores esenciales.

***ARTÍCULO 6- Cooperación de los proveedores de servicios electrónicos en el marco de una investigación de delitos informáticos:***

***Todo proveedor de servicios electrónicos u operador de telecomunicaciones se encuentra obligado a: (…)***

Se recomienda consultar a la Superintendencia General de Telecomunicaciones (SUTEL), como entidad encargada en materia de Telecomunicaciones sobre las obligaciones que se están incluyendo para los operadores de servicios en telecomunicaciones en este artículo.

***ARTÍCULO 7- Remoción de contenido en casos de Acoso Cibernético o Pornografía infantil:***

***Dentro de un máximo de 24 horas posteriores a la interposición de la denuncia por los delitos de acoso cibernético o pornografía infantil, a solicitud del Ministerio Público, un juez deberá resolver la solicitud de remoción del contenido publicado o difundido en la ejecución del delito informático, dirigida al proveedor de servicios electrónicos o al ofensor en cualquier medio que tenga bajo su control.***

***El juez deberá valorar que, a través de esta medida, no se pueda generar una afectación irreparable a la libertad de expresión y/o al derecho de acceso a la información.***
***El juez podrá conceder la remoción parcial del contenido, como puede ser la eliminación de datos específicos de un documento o contenido, si considera que con esto se logra un balance entre la protección de los derechos de la víctima y la libertad de expresión.***

En este artículo existe una confusión de conceptos, el proveedor de servicios de internet (o proveedor de servicios electrónicos como lo definen en el artículo) no es el que hospeda el contenido de una página web, por lo tanto, no está en sus capacidades técnicas la remoción de contenido web. Se recomienda modificar el artículo para que se

haga referencia a la empresa o persona que brinda el hospedaje web. Además, es importante valorar si la remoción en el plazo de 24 horas no afecta información valiosa para la investigación criminal que pueda interferir con el proceso.

Se recomienda eliminar el párrafo final del artículo 7 por ambiguo y porque constituye una forma de censura previa radicalmente prohibida

***ARTÍCULO 8- Acceso transfronterizo a datos alojados en el extranjero:***

***Las autoridades judiciales, dentro del marco de una investigación judicial y por las vías diplomáticas que correspondan, podrán:***

***1- Tener acceso o recibir datos informáticos almacenados en otro país, si se obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos.***
***2- Tener acceso a datos informáticos almacenados que se encuentren disponibles desde nuestro territorio, con independencia de la ubicación geográfica de dichos datos.***

Se recomienda revisar este artículo con relación al Convenio de Ciberdelincuencia, el cual busca evitar los procesos tradicionales y engorrosos de solicitudes de información en el caso de delitos informáticos, todo con el fin de evitar retrasos en los procesos de investigación; este artículo podría no estar acorde a lo que el Convenio establece sobre cooperación con la red 24/7, al establecer los procesos tradicionales diplomáticos para estos casos.

*Se recomienda agregar:*

*De ninguna forma o por cualquier vía se podrá tener acceso o se podrá restringir el derecho de los comunicadores sociales a la reserva de sus fuentes de información. Tampoco se podrá tener acceso o restringir de cualquier forma el derecho de los comunicadores sociales a la reserva de contenido de sus apuntes, de la información en su poder, de sus archivos personales y profesionales.*

***ARTÍCULO 9- Reformas al Código Penal. Refórmanse los artículos 7, 167, 167 bis, 173, 173 bis, 174, 194, 194 bis, 196, 196 bis, 198, 209, 217 bis, 223, 229 bis, 229 ter, 230, 231, 232, 233, 234 236, 263 y 281 del Código Penal No.4573 de 4 de mayo de 1970, cuyos textos dirán: (…)***

En este caso se realizan las siguientes observaciones:

- Ya existe el artículo 7.
- Se recomienda eliminar el inciso 3 del artículo 167 por ser amplio y ambiguo, al presentar conceptos jurídicos indeterminados, como *las observaciones de actos eróticos o sexuales de cualquier índole,* de igual forma la palabra obsceno. De igual forma esta situación se presenta en el inciso 4 del artículo 167 bis.
- En el artículo 196, 196 bis y 198 se recomienda incluir las excepciones indicadas del artículo 2 y el artículo 8
- Se recomienda eliminar el artículo 236 en razón que ya existe y el mismo agrava sobre la base de un peligro y por motivos de ambigüedad, además de atentar contra la libertad de expresión.

***Artículo 229 ter- Sabotaje informático:***

***c) El sabotaje afecte infraestructura crítica de Costa Rica o un país extranjero.***

En este caso se recomienda valorar si debe incluirse la protección de infraestructuras de otros países, debido al alcance jurisdiccional de la normativa y la problemática práctica de lograr una investigación efectiva en otras jurisdicciones.

***Artículo 232- Instalación o propagación de programas informáticos maliciosos:***

***d) A quien distribuya herramientas informáticas diseñadas para la creación de programas informáticos maliciosos****.*

En este caso existe una problemática técnica-jurídica. Las herramientas informáticas de creación para programas informáticos maliciosos son las mismas herramientas con las que se generan programas “buenos”; estos son los lenguajes de programación. En este caso, la redacción estaría penando la distribución de lenguajes de programación. Se

recomienda que se modifique la redacción del artículo de forma tal que se indique que se pena la distribución de herramientas informáticas maliciosas que puedan generar la creación de programas informáticos maliciosos.

***Artículo 233- Suplantación de páginas electrónicas:***

***Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de otra persona, suplante sitios legítimos de la red de Internet.***

***La pena será de dos a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet, capture información confidencial de una persona física o jurídica para beneficio propio o de otra persona.***

En este caso el delito no incluye personas jurídicas, siendo estas las más afectadas en el tema de suplantación de páginas electrónicas. Se recomienda incluir tanto a personas físicas como a personas jurídicas.

***Artículo 234- Facilitación del delito informático:***

***Siempre que no constituya delito con una pena superior, se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito informático o del cibercrimen.***
La redacción es confusa debido a los conceptos definidos en el artículo 1, que buscan intentar separar la definición de delitos informático o de cibercrimen. Se recomienda corregir el problema conceptual en el artículo 1 y dejar en la redacción de este artículo solamente el concepto de delitos informáticos.

***Artículo 236-Difusión de información falsa:***

***Será sancionado con pena de uno a cuatro años de prisión a quien fabrique y difunda, a través de medios informáticos, una noticia falsa capaz de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.***
***La misma pena indicada en el párrafo anterior se impondrá a quien fabrique y difunda, a través de medios informáticos, una noticia falsa con el fin***

***de afectar la decisión del electorado en un proceso de plebiscito, referéndum o electoral nacional o extranjero.***
***La pena será de tres a seis años de prisión cuando a raíz de la difusión de la noticia falsa sobreviniere peligro de muerte para una o varias personas.***

Se recomienda en este caso se realice la consulta sobre este artículo al Tribunal Supremo de Elecciones, el cual es el poder de la república encargado de tema electoral, debido a que el mismo prevé sanciones penales por temas electorales y noticias falsas.

Además, se recomienda se analice este artículo con relación a la definición de noticia falsa incluida en el artículo 1 sobre definiciones, la cual señala:

*20- Noticia falsa: Hecho falso, incompleto o inexacto, divulgado con conocimiento de su falsedad y con intención de engañar o hacer incurrir en error al destinatario, diferente a la parodia o al ejercicio periodístico.*

Siendo que un hecho incompleto o inexacto, puede no ser falso, esta definición se presta a confusión, además la misma excluye el ejercicio periodístico, la cual podría generar impunidad de este delito si es realizado por periodistas, porque no estaría contemplado para el tipo penal.

***Artículo 263- Entorpecimiento de servicios públicos:***

***Será reprimido con prisión de seis meses a dos años, a la persona que, sin crear situación de peligro común, impidiere, estorbare o entorpeciere el normal funcionamiento de los transportes por tierra, agua y aire a los servicios públicos de comunicación o de sustancias energéticas.***

En este caso no se incluyen los servicios de telecomunicaciones; recomendamos que se incluya el mismo como parte de los servicios públicos que podrían ser entorpecidos

***Artículo 232 bis- Abuso de dispositivos:***

***Se impondrá pena de prisión de uno a cinco años a quien distribuya, produzca, venda, compre, obtenga para su utilización o importe un dispositivo o programa***

***informático diseñado o adaptado principalmente para la comisión de delitos informáticos.***

***Artículo 233 bis- Ingeniería social:***

***Siempre que no constituya delito con una pena superior, se impondrá pena de prisión de seis meses a dos años a quien, mediante engaño, capture u obtenga datos personales o información confidencial apta para la comisión de un delito informático.***

En ambos casos son actividades que pueden realizarse de manera lícita en el ámbito del hacking ético, tanto la adquisición de herramientas como la ingeniería social, por lo que se recomienda incluir en la excepción de delito la adquisición de herramientas o el uso de ingeniería social dentro del ámbito del hacking ético para que no quede dudas de que dicha actividad no será penada.

***ARTÍCULO 14- Adiciónanse los incisos 3) y 4) al artículo 23 de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones No.7425 de 09 de agosto de 1994, cuyo texto dirá:***

***Artículo 23- Obligaciones de los responsables de las empresas de comunicación***

***Serán obligaciones de los funcionarios responsables de las empresas o instituciones públicas y privadas a cargo de las comunicaciones:***
***[...]***
***3- Conservar los datos de tráfico y datos de localización de las telecomunicaciones, por un periodo mínimo de cuatro años o hasta su prescripción legal.***

En este caso se recomienda consultar con las empresas de telecomunicaciones sobre la capacidad técnica y de almacenamiento para la conservación de los datos de todos sus usuarios por el periodo indicado. Además, se recomienda consultar a la Agencia de Protección de Datos de los Habitantes, en razón que al existir estos registros se estarían creando bases de datos con datos personales de todos los usuarios.

Quedo a sus órdenes para cualquier consulta o información adicional que sea requerida por medio del correo electrónico despacho.ministro@micitt.go.cr.

Atentamente,

EDWIN RICARDO ESTRADA HERNANDEZ (FIRMA)

Firmado digitalmente por EDWIN RICARDO ESTRADA HERNANDEZ (FIRMA)
Fecha: 2019.09.09 11:49:51 -06'00'

**Edwin Estrada Hernández**
**Ministro a.i.**
**DESPACHO MINISTERIAL**

AMM

C: Sr. Jorge Mora Flores, Director de Gobernanza Digital, MICITT.
Archivo