HIPER DERECHO

Tecnología como libertad

Lima, 16 de julio de 2020

Sr./Sra. Congresista de la República del Perú
Comisión Justicia y Derechos Humanos
Congreso de la República
Presente.—

Asunto: **Comentarios al Proyecto de Ley N 05630/2020-CR, Seguridad Informática y Represión de los Delitos Informáticos**

Hiperderecho es una asociación civil peruana sin fines de lucro dedicada a investigar y promover el respeto de los derechos humanos en entornos digitales, conformada por abogados y especialistas en tecnología. Como parte de nuestro trabajo, estudiamos todas las iniciativas de política pública que puedan impactar el ejercicio de derechos y libertades en estos ámbitos.

Hemos revisado con detenimiento el Proyecto de Ley 05630/2020-CR (en adelante, "el Proyecto"), el cual tiene como objeto: a) Establecer medidas de seguridad informáticas a ser adoptadas por el Estado Peruano; b) Impulsar el comercio electrónico y proteger a sus usuarios; y c) Derogar la Ley de Delitos Informáticos con el fin de reemplazarla por una norma acorde al Convenio de Ciberdelincuencia o Convenio de Budapest, que el país ha ratificado recientemente

Consideramos valioso el interés de su despacho en proponer iniciativas en estos ámbitos. En atención a ello, le hacemos llegar nuestros comentarios sobre el particular, que se centran principalmente en la naturaleza multipropósito del proyecto y la idoneidad y proporcionalidad de las medidas propuestas para combatir los delitos informáticos.

1. Sobre el ámbito de aplicación del Proyecto

Desde el artículo 1, observamos que el ámbito de aplicación del Proyecto es sumamente amplio. Los tres elementos que conforman el Objeto de la Ley, aunque aparentemente relacionados, históricamente han sido legislados de forma diferenciada y sus normativas de desarrollo no siempre conversan entre sí o son siquiera interoperables. Para ejemplificar esta situación basta señalar que la normativa de comercio electrónico vigente es del año

2000[1], mientras que la ley que regula la seguridad digital es de 2018.[2] En el primer caso, las entidades llamadas a accionar frente a posibles conflictos son el Indecopi y las cortes civiles, mientras que en el segundo es la Secretaría de Gobierno Digital (SEGDI), todas entidades de diferente jerarquía y naturaleza.

Esta amplitud presenta diferentes complicaciones, pero queremos centrarnos en las dos que consideramos más graves. En primer lugar, al intentar abarcar un campo tan amplio, el Proyecto pierde profundidad. Así pues, elementos como la seguridad digital en el Estado, que efectivamente necesita ser reforzada a la luz de los últimos casos de vulneraciones informáticas, apenas si se aborda a través de la obligación formalista de contar con certificaciones ISO (Artículos 2 y 3).

En segundo lugar, existe el riesgo de que varias de las disposiciones del Proyecto ya estén contempladas en otras leyes, lo que además puede crear conflictos de competencia. Por ejemplo, en lo relativo al comercio electrónico y la protección al consumidor, detectamos que gran parte del texto ya está recogido en otros dispositivos legales actualmente vigentes, siendo algunos de ellos el Código Civil, el Código de Protección y Defensa del Consumidor y la Ley de Protección de Datos Personales (Artículos 5-8). Tal vez la única excepción a esta crítica es la parte del texto referida a los delitos informáticos (Artículos 9-24), pues tiene el propósito de reemplazar a otra norma ya existente.

Así pues, sin ahondar todavía en la problemática específica de cada una de las reformas propuestas, queremos invitar a su despacho a considerar la decisión de proponer que el Proyecto se decida por contemplar la regulación de uno solo de los elementos descritos en el párrafo anterior: Seguridad Digital en el Estado, comercio electrónico o delitos informáticos. Esto con el fin de poder desarrollar en mayor amplitud la iniciativa y evitar la duplicidad de normas.

2. Sobre las medidas propuestas de seguridad digital en el Estado

La seguridad digital en el ámbito público es un componente muy importante dentro del proceso de modernización del Estado que en la última década ha sido apuntalado por el uso cada vez más intensivo de las Tecnologías de Información y Comunicación. Como se afirma en la Exposición de Motivos, desde hace casi dos décadas existen diferentes esfuerzos por mejorar el estándar de seguridad digital, entre ellos la adopción gradual de normativa ISO de Seguridad de la Información, la publicación de planes de Gobierno Electrónico, entre otros.

Sin embargo, como acertadamente señalan los proponentes del Proyecto, nada de esto parece haber sido suficiente para que hoy en día se cuente con un estándar aceptable de seguridad digital en las instituciones públicas. Como parte de nuestro trabajo de investigación, Hiperderecho ha reportado en los últimos tres años diferentes brechas de

[1] Nos referimos específicamente a dos normas:
a) Ley 27291, "Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica", promulgada el 24 de junio del año 2000; y b) Ley 27269, "Ley de Firmas y Certificados Digitales", promulgada el 17 de julio del año 2000.
[2] Nos referimos al Decreto Legislativo N 1412, "Ley de Gobierno Digital", que es la primera de su tipo que otorga rango legal al Marco de Seguridad Digital del Estado.

seguridad y fallos en los productos informáticos del Estado, algunos de ellos muy graves.[3] Es pues una necesidad reforzar el trabajo en esta materia.

En ese sentido, la propuesta del Proyecto es que sea obligatorio para todas las entidades públicas la implementación de normativas ISO de seguridad de la información, y que la SEGDI proponga un plazo para que esta exigencia se extienda también a las personas y empresas que contratan con el Estado. Estos cambios buscarían elevar el estándar de seguridad mencionado en el mediano y largo plazo. No obstante, nuestra opinión es que esta vía no es la más idónea para lograr dicho objetivo. Pasamos a explicar el porqué.

La implementación exitosa de las normas ISO 17799 y 27001 son un indicador de que una entidad ha adoptado ciertos niveles de seguridad en el manejo de la información, pero por sí mismas no son una garantía de mayor seguridad digital. Por ejemplo, desde el año 2004 es obligatoria la implementación de la ISO 17799 en todas las instituciones que conforman el Sistema Nacional de Informática[4] y desde 2012 ocurre lo mismo con la ISO 27001.[5] Para efectos prácticos, dicho Sistema abarca casi la totalidad del Estado, lo que incluye a los organismos más importantes como RENIEC, ONPE, INDECOPI, todos los Ministerios, el Poder Judicial y Legislativo, los gobiernos regionales y municipales, entre otros.[6]

Sin dejar de notar que la mayor parte de la Administración Pública ya está legalmente obligada a implementar estas normas ISO desde mucho antes, nuestro principal argumento en contra de esta propuesta es que esta solución no es una garantía de una gestión informática más segura. Como debe ser de su conocimiento, a finales de mayo del presente año se hizo público que el sistema de entrega del Bono Familiar Universal había sido vulnerado, con la probable pérdida de millones de soles destinados a este subsidio, a manos de delincuentes informáticos.[7] Dos de las entidades involucradas en la gestión de este

---

[3] Véase:
Carlos Guerrero, “La encuesta virtual LGBTI 2017 pone en riesgo a todos”, 17 de mayo de 2017. Hiperderecho. Enlace:
https://hiperderecho.org/2017/05/la-encuesta-virtual-lgbti-2017-pone-riesgo-todos/
Miguel Morachimo, “RENIEC negó que haya existido un filtrado de datos personales. Nosotros lo confirmamos”, 19 de junio de 2018. Hiperderecho. Enlace:
https://hiperderecho.org/2018/06/reniec-nego-que-haya-existido-un-filtrado-de-datos-personales-nosotros-lo-confirmamos/
Diego Escalante, “ONPE filtró los datos personales de millones de peruanos durante más de medio año”, 17 de julio de 2018. Hiperderecho. Enlace:
https://hiperderecho.org/2018/07/onpe-filtrado-datos-hackaton

[4] Resolución Ministerial Nº 224-2004-PCM, “Aprueban uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la gestión de la Seguridad de la Información”. Enlace:
https://repositorio.indecopi.gob.pe/bitstream/handle/11724/3063/RM.224-2004-PCM.pdf?sequence=5&isAllowed=y

[5] Resolución Ministerial Nº 129-2012-PCM, “Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información en todas las entidades integrantes del Sistema Nacional de Informática”. Enlace:
https://cdn.www.gob.pe/uploads/document/file/303765/RM_129_2012PCM.pdf

[6] Decreto Legislativo N 604, Ley de organización y funciones del Instituto Nacional de Estadística e Informática”. Enlace: http://m.inei.gob.pe/media/archivos/5073_1.pdf

[7] Carlos Neyra, “Hackers vulneraron plataforma del Bono Familiar Universal para apropiarse de dinero”, 30 de mayo de 2020. Diario El Comercio. Enlace:

sistema son RENIEC y el Ministerio de Desarrollo e Inclusión Social, las que irónicamente ya tienen implementadas ambas normas ISO en sus procesos de gestión.

El razonamiento anterior aplica también para el extremo de la propuesta que busca establecer la misma obligación para quienes ofrecen productos y servicios al Estado. Además, en este caso también es necesario valorar en qué casos esta exigencia es necesaria y proporcional para lograr un mayor estándar de seguridad digital. Por ejemplo, ¿resulta idóneo exigirle la implementación de estas normas a proveedores de alimentos y bebidas, vestimenta o a quienes ofrecen servicios personales de consultoría? Aún cuando esta no parece ser la lógica del Proyecto, su texto no hace ninguna distinción entre proveedores, por lo que sugerimos que se realice una modificación que precise que la obligación de contar con la normativa ISO está sujeta a condiciones, de forma que esto se pueda desarrollar mejor en el Reglamento.

3. Sobre las medidas propuestas para el comercio electrónico

Respecto de las medidas propuestas para regular el comercio electrónico, tenemos la impresión de que los proponentes asumen que existe un vacío regulatorio que amerita ser llenado y por lo tanto proponen esta regulación "mínima", que debería complementarse con la regulación actual de protección del consumidor. No obstante, queremos señalar que esta concepción está equivocada pues el comercio electrónico en el país ya responde a diferentes regulaciones, incluidas las del consumidor.

A nivel societario, las empresas domiciliadas en el país que ofrecen sus productos y servicios a través del comercio electrónico están sujetas a las mismas reglas que aquellas que lo hacen por vías más tradicionales. Del mismo modo ocurre con la tributación, pues sin importar la modalidad bajo la cual se obtengan las rentas, siempre que estas sean de fuente peruana, las personas naturales y empresas están obligadas a declarar y pagar impuestos. Finalmente, respecto al cumplimiento de la normativa de consumidor, el Código de Protección y Defensa del Consumidor ya es enteramente aplicable pues solo se requiere probar la existencia o preexistencia de una relación de consumo y la calidad de proveedor y consumidor de las partes. Es más, ya existen en INDECOPI diferentes resoluciones que corroboran el nivel de cumplimiento de estas disposiciones.[8]

Dicho esto, los artículos 5, 6 y 8 del Proyecto duplican lo ya dispuesto por el Código de Protección y Defensa Consumidor y los lineamientos de INDECOPI en materia de Publicidad, además de lo que ha venido desarrollando esta entidad a través de sus resoluciones administrativas en la materia. Por este motivo, consideramos que este apartado es innecesario y por lo tanto proponemos que sea retirado del Proyecto. Quizás la única excepción a ello sería lo dispuesto en el artículo 7, pero estas exigencias también están previstas en otro cuerpo normativo: La Ley de Protección de Datos Personales y su Reglamento, que ya establece obligaciones de consentimiento, medidas de seguridad y mecanismos de acción para los titulares de datos personales, no solo en relación a la

https://elcomercio.pe/lima/sucesos/coronavirus-en-peru-hackers-vulneraron-plataforma-del-bono-familiar-para-apropiarse-de-dinero-noticia

[8] Melissa Zupan, "Regulación sobre e-commerce", IUS 360. Enlace: https://ius360.com/privado/regulacion-sobre-e-commerce/#_ftnref18

información de sus datos bancarios sino en general, pudiendo abarcar nombres, dirección, sexo, estado civil, etc.

4. Sobre las medidas contra los delitos informáticos

Posiblemente la parte más sustantiva del Proyecto es la referente a los delitos informáticos, pues propone derogar la norma actual y reemplazarla por su propio catálogo de delitos informáticos, donde se incluyen algunos nuevos, además de añadir procedimientos al proceso penal en materia de investigación y procesamiento. Sobre este apartado, tenemos varios comentarios de forma y fondo, que vamos a enumerar a continuación:

4.1. La necesidad de dotar de mayor formalismo al Proyecto

Consideramos que si el Proyecto desea modificar la actual Ley de Delitos Informáticos, debería respetar la misma formalidad que las anteriores normas que han tenido este propósito desde su primera regulación en el año 2000.[9] Esto es, que el Proyecto se refiera única y exclusivamente a la modificación de esta materia, lo que incluye el catálogo de delitos informáticos y las modificaciones de índole procesal penal que correspondan, dejando fuera cualquier mención a la seguridad digital en el Estado y al comercio electrónico, por no ser pertinentes.

4.2. Sobre el bloqueo de dominios

En el artículo 13 del Proyecto se establece que el fiscal puede autorizar el bloqueo del Domain Name Service, DNS, (presuntamente cuando el dominio esté involucrado en la comisión de un delito informático) durante las investigaciones y dentro del proceso mismo. Consideramos esta medida desproporcionada pues la normativa actual de Neutralidad de la Red en el Perú exige que para solicitar el bloqueo de sitios web o aplicaciones legales, se requiere una norma legal expresa o en su defecto, un mandato judicial.[10]

En el mismo sentido, la Declaración Conjunta Sobre Libertad de Expresión e Internet, suscrita por, entre otros, el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión y la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión, reconoce a la neutralidad de red como un principio estrechamente vinculado al derecho a la libertad de expresión e información. Dicho

---

[9] Perú ha contado hasta ahora con dos leyes especiales que regulan los delitos informáticos, a saber; la Ley N 27309 promulgada en julio del año 2000, la que fue derogada posteriormente por la Ley N 30096, que a su vez ha sufrido modificaciones por parte de la Ley N 30171.

[10] Resolución de Consejo Directivo Nº 165-2016-CD/OSIPTEL, Reglamento de Neutralidad de la Red:
(...)
Artículo 12.- Tipos de medidas permitidas relativas a la neutralidad de red
El Operador de Telecomunicaciones podrá implementar una medida relativa a la Neutralidad de Red, cuando:
1. El presente Reglamento la califica expresamente como una medida autorizada relativa a la Neutralidad de Red.
2. Se trata de una medida ante situación de emergencia relativa a la Neutralidad de Red.
3. Se trata de una medida implementada por mandato judicial.
Enlace:
https://busquedas.elperuano.pe/normaslegales/reglamento-de-neutralidad-en-red-resolucion-no-165-2016-cdosiptel-1467489-1/

documento define a la neutralidad de red como el principio a través del cual "[e]l tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación.[11] También, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos ha indicado que "[e]l principio de neutralidad es un principio de diseño de Internet, por el cual se maximiza la utilidad de las redes, tratando a todos los 'paquetes de datos' en forma igualitaria sin distinción alguna".[12]

Así pues, el bloqueo de un sitio web o aplicación es tal vez una de las medidas más graves que vulneran el libre flujo de datos en la red, lo que en ciertos casos resulta equiparable incluso al cierre de una radio o de un periódico. Por ello, consideramos que es un retroceso que se flexibilice su aplicación, toda vez que ya existe un procedimiento que cuenta con las garantías suficientes para lograr ese fin: Que el fiscal solicite al juez dicha actuación y que este, luego de la valoración correspondiente, otorgue o no la medida y esta sea ejecutada por los proveedores de servicios de telecomunicaciones.

Si faltara una razón más para postular que esta no es una propuesta acertada, bastaría con decir que el procedimiento de bloqueo no está exento de cierta complejidad. A nivel tecnológico, no siempre es posible efectuar un bloqueo efectivo de nombres de dominio. Por ejemplo, tratándose de contenidos almacenados en páginas web que usen conexiones cifradas (ej. Facebook, Youtube, Twitter), solo podrá bloquearse el dominio completo y no una dirección web en particular.

4.3. Deficiente adecuación al Convenio de Budapest

En la Exposición de Motivos, los proponentes del Proyecto afirman que la modificación de la Ley de Delitos Informáticos es necesaria para adaptar nuestra legislación penal al estándar del Convenio de Ciberdelincuencia o Convenio Budapest, un tratado multilateral que el Perú recientemente ha ratificado.[13] No obstante, respecto del apartado donde se modifican o crean nuevos delitos (17-24), encontramos que estas tienen varias deficiencias, las cuales no están presentes en la norma actual que se quiere cambiar. Pasamos a enumerarlas:

a) En el caso de "Intrusismo informático" y "Perturbación informática", notamos que su redacción adolece del mismo problema que adolecían las primeras normas penales que sancionaban esta conducta; esto es: Se impone la pena sobre una conducta, sin tener como requisito que la forma de ejecución sea deliberada (es decir, con dolo) e ilegítima y que sea

[11] Relator Especial de las Naciones Unidas (ONU) sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión, y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), 1 de junio de 2011, Punto 5 (a). Enlace: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2

[12] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. Estándares para una Internet Libre, Abierta e Incluyente, 15 de marzo de 2017, párrafo 21.

[13] "Perú se adhiere al Convenio de Budapest sobre ciberseguridad y ayuda judicial", 4 de febrero de 2019. Diario Gestión. Enlace: https://gestion.pe/tecnologia/peru-adhiere-convenio-budapest-ciberseguridad-ayuda-judicial-257741-noticia/?ref=gesr

necesario un resultado. En el caso de “Interceptación de datos informáticos”, el contenido necesita estar mejor desarrollado. En todos estos casos, la redacción actual de la Ley de Delitos Informáticos va mucho más acorde con lo propuesto en la sección de delitos del Convenio de Budapest.

Propuesta del Proyecto de Ley	**Ley de Delitos Informáticos actual**	**Convenio de Ciberdelincuencia o Convenio de Budapest**
Intrusismo informático: El que sin contar con autorización o haciendo uso indebido de ella, accede o facilita a otro el al conjunto o una parte de un sistema informático, o se mantiene en el mismo, con la intención de obtener información, datos informáticos, o con cualquier otra intención delictiva, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con treinta a noventa dias multa.	**Acceso ilícito:** El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado. (Fuente: Ley N 30096 modificada por Ley N 30171)	**Acceso ilícito (Art. 2):** Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o partes de un sistema informático.Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.
Interceptación de datos informáticos: El que deliberada e ilegalmente intercepta datos informáticos de terceros, en transmisiones no públicas, dirigidos, originados o efectuados dentro de un sistema informático, incluidas las emisiones electromagnéticas que transporten dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.	**Interceptación de datos informáticos:** El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga	**Interceptación ilícita (Art. 3):** Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas

	sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública. La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales. (Fuente: Ley N 30096 modificada por Ley N 30171)	provenientes de un sistema informático que transporte dichos datos informáticos.Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.
Perturbación informática: El que deliberadamente, valiéndose de cualquier medio, daña, borra, deteriora, altera, suprime, entorpece, hace inaccesible o imposilita el funcionamiento de un sistema será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	**Atentado a la integridad de datos informáticos:** El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.”	**Ataques a la integridad de los datos (Art. 4):** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos. 2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

b) En el caso del delito de “Creación de falsa identidad”, consideramos que esta adición no solo es innecesaria sino que es perjudicial para el ordenamiento legal por diferentes motivos. Decimos que es innecesario pues ninguna ley penal antes ha establecido la prohibición de crear o poseer identidades falsas o seudónimas para el desarrollo de una actividad, en la medida que esta sea lícita y no se requieran formalidades que impidan este ejercicio. Esto es así por la sencilla razón de que, cuando se comete un delito, no importa bajo qué identidad haya actuado su autor para que el sistema penal se active y pueda ir en su persecución, siendo que en muchos casos la investigación debe centrarse precisamente en establecer la identidad real del imputado para poder procesarlo. Dentro del mundo del crimen organizado el uso de alias, disfraces, entre otros elementos de anonimato están ampliamente difundidos, sin que esto haya impulsado la creación de normas que prohíban las máscaras, los pasamontañas u otros elementos de camuflaje. Esto se debe a que el Derecho Penal simplemente no encuentra este hecho relevante y consideramos que lo mismo debería ocurrir en este caso.

Decimos también que es perjudicial porque a partir de esta inclusión innecesaria, se está criminalizado la mera existencia de figuras públicas inventadas que cuentan con perfiles propios o creados por su comunidad en redes sociales; como el dragón Timoteo[14], el tendero Don Pepe[15], entre otros. Se estaría haciendo lo mismo también con las identidades inventadas con propósitos literarios, de ejercicio creativo, parodia, seguridad, trabajo, entre otros. Aunque la redacción del delito consigna diferentes situaciones bajo las cuales resulta delito la creación de una identidad falsa, todas salvo una ya se castigan, independientemente si el autor usa o no una identidad inventada. Es más, la única excepción es tal vez la más preocupante. El Proyecto menciona que se sancionará este delito cuando el objeto de crear la identidad falsa sea "Obtener un beneficio económico para sí o para tercero". La mayoría de los ejemplos anteriormente señalados caen en esta categoría, pese a que no hay nada de ilícito en ello y es más bien una práctica común y facilitada por la forma en que Internet funciona. Sugerimos pues que se retire esta parte de la propuesta por ser potencialmente dañina para los derechos de los usuarios de Internet en el país.

5. Comentarios Finales

Recomendamos a su despacho que valore la posibilidad de recalibrar el enfoque del Proyecto, de tal manera que se dirija exclusivamente a alguno de los tres elementos que pretende regular: Seguridad digital en el Estado, comercio electrónico o delitos informáticos. Esto con el fin de dotar de mayor profundidad y ahondar en la reforma pretendida en cualquiera de estas categorías. Opinamos en contra de que todas ellas sean reguladas bajo el mismo Proyecto, aún cuando eventualmente este sea modificado a partir del debate surgido en la Comisión.

En relación a las **medidas de seguridad digital**, consideramos que las propuestas no son idóneas y en los casos ya explicados resultan ser más bien barreras burocráticas innecesarias para los privados que contratan con el Estado. En ese sentido, vale la pena que la Comisión cuente en esta parte de la propuesta con la opinión de la Secretaría de Gobierno Digital, con el propósito de conocer de primera mano los avances del Ejecutivo en esta materia y así pueda perfeccionarse la propuesta. Opinamos en contra de que se mantenga el texto actual o que se fuerce la adopción de normativa ISO al sector privado de manera genérica y sin admitir excepciones.

En relación a las **medidas de comercio electrónico**, las propuestas del Proyecto duplican la regulación ya existente y por lo tanto son innecesarias. Como en muchos otros Proyectos que buscan regular la innovación tecnológica, se ha perdido de vista que el marco legal de comercio actual ya es enteramente aplicable al comercio electrónico, siendo este marco tan antiguo como el año 2000, cuando se promulgaron reformas al Código Civil y la Ley de Firma y Certificados Digitales para hacerlo posible. Opinamos en contra de que se mantenga el texto actual y proponemos que se lo retire completamente por irrelevante.

Finalmente, en relación a las **medidas sobre delitos informáticos**, observamos que se han propuesto varias incorporaciones de tipo procesal potencialmente peligrosas como la potestad dada al fiscal para solicitar el bloqueo de un dominio, lo que actualmente solo

[14] Ver: https://www.facebook.com/TimoteoDeLaTV
[15] Ver: https://www.facebook.com/LTDDP

puede ser ejecutado por mandato judicial. Respecto al catálogo de delitos, tal como hemos señalado, hay varias redacciones propuestas que se alejan del estándar del Convenio de Budapest, siendo más exactas las redacciones de la norma actual, al menos en tres delitos: Intrusismo informático, interceptación de datos informáticos y perturbación informática. Por otro lado, la incorporación del delito de Creación de falsa identidad no solo es innecesaria sino potencialmente peligrosa pues criminaliza diferentes conductas en Internet que actualmente no son ilegales ni dañinas para la comunidad, y más bien constituyen una forma más del ejercicio de la libertad de expresión. Opinamos que todo el catálogo de delitos propuesto debe revisarse para que las propuestas sean un avance y no un retroceso respecto de la norma actual y se descarte completamente la inclusión de la potestad del fiscal para bloquear dominios y el delito de Creación de falsa identidad.

Por la suma de estos motivos, solicitamos a su despacho tenga a bien recibir esos comentarios y los sume al debate en la Comisión sobre esta iniciativa. Llegado el momento de la votación, sugerimos votar en contra, en la medida en que no se realicen cambios sustantivos al Proyecto. Del mismo modo, si es necesaria alguna precisión o mayores alcances nos ponemos a su disposición para cualquier consulta sobre este Proyecto de Ley o sobre otras iniciativas que la Comisiones respectivas del Congreso requieran.

Sin más, le expresamos nuestros mejores deseos y mayor consideración.

Atentamente,

Miguel Morachimo Rodriguez
Director Ejecutivo

Carlos Guerrero Argote
Director de Políticas Públicas

Asociación Civil Hiperderecho
Av. Benavides 1944, Piso 9, Miraflores, Lima
RUC: 20551193099