De Budapest al Perú:

ANÁLISIS SOBRE EL PROCESO DE IMPLEMENTACIÓN DEL CONVENIO DE CIBERDELINCUENCIA

IMPACTO EN EL CORTO, MEDIANO Y LARGO PLAZO

* **Carlos Guerrero Argote**

Esta investigación fue producida en el marco del proyecto "Grupo de trabajo sobre Ciberseguridad en América Latina", gracias al trabajo conjunto de las organizaciones Hiperderecho (Perú), IPANDETEC (Panamá), Fundación Karisma (Colombia), Red en Defensa de los Derechos Digitales (México) y TEDIC (Paraguay), bajo la coordinación de Derechos Digitales, y gracias al apoyo de Ford Foundation.

Grupo de trabajo sobre Ciberseguridad en América Latina
Coordinación: Marianne Díaz, *Derechos Digitales*

Investigación:
Martín Borgioli y Carlos Guerrero, *Hiperderecho*
Sara Frati, Lía Hernández y Diego Morales, *IPANDETEC*
Juan Diego Castañeda y Amalia Toledo, *Karisma*
Danya Centeno, *R3D*
Maricarmen Sequera y Marlene Samaniego, *TEDIC*

Edición: Marianne Díaz
Portada: Violeta Cereceda
Diagramación: Constanza Figueroa
Junio 2018.

3

INTRODUCCIÓN

Una de las primeras normas publicadas en el Perú relacionadas al uso de las computadoras fue el el Decreto Legislativo N° 681, que estableció en 1991 la validez legal de ciertas técnicas de archivo de documentos a través de medios informáticos. En ese mismo año, la recién creada Red Científica Peruana envió el primer correo electrónico a través de Internet y se creó la primera cabina de acceso público, un modelo que en los próximos años ayudaría a conectar masivamente a toda la población. En un país convulsionado por la crisis económica y la guerra contra el terrorismo, estos hitos permitían ver con esperanza el futuro, un futuro en donde las tecnologías de información y comunicación (TICs) impulsarían el desarrollo de la sociedad peruana.

Veintisiete años después, el contexto social y la forma cómo ha evolucionado Internet en el país obliga a pensar de forma más realista sobre lo avanzado en este tiempo. Superado el espejismo del solucionismo tecnológico, las TICs se han convertido efectivamente en pilares fundamentales del desarrollo, pero también han servido de plataforma para que viejos problemas se repliquen y aparezcan otros nuevos. Uno de ellos, quizás el más apremiante de nuestro siglo, es la proliferación de la criminalidad en el ciberespacio, que reta el poder de los sistemas de justicia nacionales y la seguridad de usuarios y entidades en todo el mundo.

El presente informe toma la situación antes descrita como punto de partida para analizar de forma crítica la inminente suscripción del Convenio sobre Ciberdelincuencia o Convenio de Budapest por parte del Perú, el más reciente esfuerzo por hacer frente al problema del crimen informático. El contexto histórico en el cual se enmarca este análisis es el de un país que ha construido su ecosistema digital (tecnología, normativa y gobernanza) en base a los modelos y concepciones predominantes en los países desarrollados, a los cuales les ha introducido elementos adaptativos que han hecho viable su apropiación en el corto, mediano y largo plazo. Teniendo en cuenta esto, el desarrollo del análisis se divide en dos ejes principales: el primero enfocado en el proceso de implementación del Convenio y el segundo en medir el impacto que dicha implementación tendrá en el país.

El primer eje empieza con un recuento histórico del desarrollo Convenio de Budapest y cómo luego de su creación, este ha interactuado en varias oportunidades con el ecosistema digital peruano, por ejemplo en el caso de la creación de normas y procedimientos sobre delitos informáticos. Luego se aborda de lleno la implementación, en donde se busca responder algunas preguntas: ¿Qué es lo que debe implementarse? ¿Qué ya ha sido implementado? ¿Qué es lo que falta? ¿Qué no es posible implementar? Finalmente, se propone una serie de acciones consideradas esenciales para que la implementación del Convenio de Budapest sea exitosa.

El segundo eje mide el impacto de la implementación del Convenio en tres

aspectos relevantes: las políticas públicas, los actores y sus roles y los derechos humanos. A partir de las acciones que se identificaron en el primer eje, este apartado contiene una proyección de lo que podríamos esperar como consecuencia de su implementación y ejecución en el corto, mediano y largo plazo. Estas proyecciones, que proponemos ocurrirán en un horizonte de tiempo de diez años, tienen diferentes niveles de probabilidad. Por ejemplo, en el caso de políticas públicas, una proyección muy probable es que se inicie la redacción de una Política Nacional de Ciberseguridad. Por otro lado, en el caso de los actores y sus roles, una proyección poco probable es que se creen nuevas entidades para la implementación del Convenio y se deje de lado al actor principal que es actualmente la Secretaría de Gobierno Digital.

Finalmente, las conclusiones son un recuento de los puntos más importantes del desarrollo de ambos ejes y contienen también una declaración de intención sobre este proceso, del cual este informe aspira a ser un primer acercamiento.

1. IMPLEMENTANDO EL CONVENIO DE BUDAPEST

El Convenio de Budapest es un tratado internacional creado por los países miembros del Consejo de Europa con el fin de hacer frente a los delitos informáticos a través de mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y cooperación internacional. La redacción del Convenio inició en 1995 y la versión final fue aprobada en 2001, entrando en vigencia tres años después. A la fecha, ha sido suscrito por 56 países y actualmente existe una larga lista de posibles adherentes, especialmente entre los países de América Latina y El Caribe.

Con la masificación de Internet, son cada vez más los países que deben lidiar con diferentes escenarios de amenaza en el ciberespacio, los cuales afectan no solo su capacidad de gobierno sino también la seguridad de sus ciudadanos, de sus sistemas y del ecosistema digital en general. En ese contexto, la adhesión al Convenio de Budapest se suele ver como un elemento importante de cualquier estrategia de ciberseguridad. En principio, el Convenio ofrece a los países interesados un corpus amplio de términos y tipificaciones relacionados a los delitos informáticos que buscan crear un marco penal común. También pretende fijar un estándar mínimo de procesos que hagan viable la persecución penal y la acumulación de pruebas. Pero quizás el mayor atractivo es la posibilidad de formar parte de un club en donde los miembros tienen, al menos en teoría, la obligación de compartir información y cooperar entre sí.

Sin embargo, no todos los países consideran que el Convenio de Budapest es beneficioso para sus intereses. Existe actualmente un bloque conformado por Brasil, Rusia, India y China (BRICS) que han denunciado el tratado como un instrumento para legitimar prácticas de vigilancia como las ejercidas por Esta-

dos Unidos y sus aliados europeos1 y por ello se han negado a suscribirlo. En la misma línea se encuentra la Organización de Cooperación de Shanghai (OCS) que además de los países euroasiáticos de BRICS agrupa a: Kazajistán, Kirguistán, Tayikistán, Uzbekistán y Pakistán. Todos ellos, con excepción de Brasil, poseen una visión del ciberespacio profundamente ligada a la soberanía, que se contrapone al modelo europeo y la hace incompatible con los mecanismos que propone el Convenio.

1.1 EL CONTEXTO PERUANO

El Perú no ha sido ajeno al desarrollo de normativa para encarar los desafíos que suponen las nuevas relaciones creadas a partir de las tecnologías de las TICs. Entre los años 80 e inicios de los 90, se expidieron muchas normas de organización interna para regular el uso de las computadoras y otros dispositivos electrónicos, que comenzaban a jugar un papel importante en la modernización del Estado. Asimismo, en 1991 se publicó el Decreto Legislativo N° 681, "Uso de Tecnologías Avanzadas en Materia de Archivo", una norma pionera en la región que otorgaba validez legal a los archivos reproducidos por medios informáticos. En un claro signo del cambio de los tiempos, esta ley declaraba expresamente su intención de fomentar la inversión privada a partir del uso de la tecnología.2

En lo que respecta a Internet, la primera conexión estable se realizó también en 1991 gracias a la Red Científica Peruana (RCP) y en los siguientes años el acceso se expandió debido principalmente a un elemento adaptativo exitosamente aplicado: las cabinas públicas de Internet.3 Este modelo hizo posible conectar a una mayor cantidad de personas y sortear la valla de los altos precios que inicialmente tenían las conexiones domésticas. A finales de la década, la masificación de esta tecnología empezó a producir las mismas demandas que ya había producido en otros países: mejores condiciones de conexión, regulación sobre el comercio, protección de derechos, entre otros.

A partir del año 2000 estas demandas empezaron a ser atendidas por el Estado a través de la vía de la regulación. Por un lado, se empezó a construir un marco jurídico para el uso de las TICs en el gobierno (gobierno electrónico) y por el otro, se desplegaron sin mucho orden diferentes normas para resolver problemas de sectores específicos. En este último caso se encuentran las modificaciones del Código Civil a través de la Ley N° 27291 que otorga validez a las transacciones electrónicas (2000), la Ley de firma y certificados digitales

1 "Revelaciones sobre la red de vigilancia mundial (2013-2015)", Wikipedia, La enciclopedia libre, https://goo.gl/eYmLzK

2 En su exposición de motivos, el Decreto Legislativo N° 681 señala "(...) Que es conveniente, para otorgar facilidades a las empresas, regular el uso de las tecnologías avanzadas en materia de archivos de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras..."

3 Historia de Internet en el Perú, Red Científica Peruana, http://www.rcp.net.pe/historia.html

(2000), la Ley de transparencia y acceso a la información pública (2002), la creación de organismos de seguimiento como la Comisión para el Desarrollo de la Sociedad de la Información - CODESI, (2003), la Ley contra el SPAM (2005), la Ley de protección de datos personales (2011), entre otras.

En materia de crimen informático, el Perú adoptó tempranamente normas penales específicas sobre los denominados delitos informáticos, pero sin ahondar en su concepción, evitando también la distinción entre estos y los delitos cometidos a través de medios informáticos. En el 2000, un año antes de que se publique la versión final del Convenio de Budapest, se aprobó la Ley N° 27309 que introdujo dos nuevos delitos al Código Penal peruano: el intrusismo informático y el cracking. Entre 2004 y 2010 se aprobaron también otras modificaciones referidas a los delitos de explotación sexual, pornografía infantil y propiedad intelectual relacionados al uso de la TICs. Posteriormente, en 2013 se aprobó la Ley N° 30096 que introdujo nuevas modificaciones al Código Penal e incorporó un grupo numeroso de delitos informáticos y medidas procesales. Finalmente, en 2014 se aprobó la Ley N° 30171 que modificó a esta última y es el texto vigente sobre delitos informáticos en el país. Cabe decir que todas estas normas estuvieron inspiradas en mayor o menor medida en el Convenio, pero innovando en ciertos casos con el fin de introducir elementos adaptativos o yendo más allá de Budapest como en el caso de la regulación del grooming. Así mismo, ninguna de estas modificaciones fue ajena a la controversia, pues en su momento organizaciones de la sociedad civil protestaron no solo por los textos propuestos para la redacción de las leyes sino por la poca transparencia en el debate para su aprobación.4

Además de normas penales, el Estado peruano empezó a engendrar a partir de 2003 un conjunto de entidades que, por sus atribuciones, jugaron y juegan un rol importante respecto de los delitos informáticos. En el escalón más alto se encuentra la Secretaría de Gobierno Digital (SEGDI), órgano rector del Sistema Nacional de Informática ubicado dentro de la Presidencia del Consejo de Ministros y que funciona como una oficina de creación de políticas públicas en materia de gobierno electrónico. Después se encuentran un grupo de instituciones que crean normas de estandarización para los procesos informáticos como el Instituto Nacional de Estadística e Informática (INEI) y el Instituto Nacional de Calidad (INACAL). Luego están las entidades de primera línea como el Centro de Emergencia y Respuesta Temprana (PeCERT), la División de Delitos de Alta Tecnología de la Policía Nacional (PNP-DIVINDAT), las fiscalías y juzgados especializados y, finalmente, las oficinas dentro de los ministerios encargadas de gestionar el uso de las TICs.

Pese a la existencia de todos estos elementos que parecen acercar al Perú a los estándares de los países que forman parte del Convenio de Budapest, en general no existe una consciencia muy grande en el país con relación a la seguridad

4 Miguel Morachimo, “En qué quedó la Ley de Delitos Informáticos”, 2014, https://goo.gl/SgNqvq

informática y la cultura digital es deficitaria en casi todos los niveles. Esto se agrava en la medida que la oferta educativa y de formación de capacidades en materia de ciberseguridad es mínima y ni siquiera los operadores de justicia y otros actores involucrados directamente están debidamente capacitados para poder actuar frente a los nuevos escenarios que crea el crimen informático. Un estudio conducido en 2016 por el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA) refleja bien esta situación, señalando que el principal problema en el Perú es la ausencia de concientización entre los actores, malas prácticas en la gestión de la infraestructura y la ausencia de una cultura de la seguridad digital.5

1.2 SOBRE LA IMPLEMENTACIÓN

El Convenio de Budapest tiene tres objetivos declarados: La creación de un marco común de derecho penal sustantivo, la estandarización de procesos penales y la cooperación internacional. Teniendo en consideración el contexto presentado en el punto anterior, queda claro que el proceso de implementación del Convenio no será uniforme, lo que influirá considerablemente en el cumplimiento de sus objetivos. En ese sentido, cabe preguntarse: ¿Qué es lo que ya se ha implementado? ¿Qué es lo que falta? ¿Qué no es posible implementar? Para contestar estas y otras preguntas, a continuación se ha dividido el análisis a partir de los tres objetivos mencionados.

1.2.1 MARCO COMÚN DE DERECHO PENAL SUSTANTIVO

El Convenio de Budapest incorpora en el Primer Capítulo de su texto una serie de artículos destinados a crear un marco común de derecho penal sustantivo. Allí se proponen cuatro grandes categorías dentro de las cuales se desarrollan diferentes tipos penales. Las categorías son: Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, delitos informáticos, delitos relacionados con el contenido y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Las dos primeras categorías son la más robustas en cuanto a definiciones, proponiendo inclusive textos modelo, mientras que las dos últimas son definidas de forma más genérica, dándole a los miembros mayor libertad para definir las conductas punibles en base a su propia legislación.

Teniendo en cuenta este marco penal propuesto, la pregunta inminente es: ¿Cuántos de estos delitos se encuentran tipificados actualmente en el Código Penal peruano? ¿Son equivalentes a los del Convenio? ¿Qué tan relevante han sido su creación para nuestro ecosistema digital? En el siguiente cuadro vamos a comparar las definiciones del Convenio de Budapest principalmente con los delitos creados por la Ley N° 30096, sus posteriores modificaciones y otras normas relacionadas:

5 Ciberseguridad 2016: ¿Estamos preparados en América Latina y el Caribe?, BID/OEA, 2016, https://goo.gl/nSf5j1

Tipo	Código Penal Peruano	Convenio de Budapest
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	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 queel 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 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 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)	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 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.
	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.
	Atentado a la integridad de sistemas informáticos: El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa. (Fuente: Ley N° 30096 modificada por Ley N° 30171)	Ataques a la integridad del sistema (Art. 5): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
	Abuso de mecanismos y dispositivos informáticos: El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa." (Fuente: Ley N° 30096 modificada por Ley N° 30171)	Abuso de los dispositivos (Art. 6): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegìtimade los siguientes actos: a) laproducción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: (i)un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artìculos 2 a 5; (ii)una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artìculos 2 a 5; y b)la posesión de alguno de los elementos contemplados en los anteriores apartadosa(i) o (ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artìculos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

Delitos informáticos	Falsedad ideológica: El que inserta o hace insertar, en instrumento público, declaraciones falsas concernientes a hechos que deban probarse con el documento, con el objeto de emplearlo como si la declaración fuera conforme a la verdad, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de tres ni mayor de seis años y con ciento ochenta a trescientos sesenticinco días-multa. El que hace uso del documento como si el contenido fuera exacto, siempre que de su uso pueda resultar algún perjuicio, será reprimido, en su caso, con las mismas penas. (Fuente: Art. 428 CP)	Falsificación informática (Art. 7): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.
	Fraude informático: El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado afines asistenciales o a programas de apoyo social. (Fuente: Ley N° 30096 modificada por Ley N° 30171)	Fraude Informático (Art. 8): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) cualquier introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.
Delitos relacionados con el contenido	Pornografía infantil: El queposee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:1. El menor tenga menos de catorce años de edad.2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36. (Fuente: Art.183-A CP modificado por la Ley N° 30096)	Delitos relacionados con la pornografía infantil (Art: 9): Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a) la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático; b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático; c) la difusión o transmisión de pornografía infantil por medio de un sistema informático, d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona; e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.2. A los efectos del anterior apartado 1, por pornografía infantil se entenderá todo material pornográfico que contenga la representación visual de: a) un menor comportándose de una forma sexualmente explícita; b) una persona que parezca un menor comportándose de una forma sexualmente explícita; c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita. 3. A los efectos del anterior apartado 2, por menor se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años. 4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Delitos contra los derechos intelectuales: Artículo 216: Copia o reproducción no autorizada; Artículo 217: Reproducción, difusión, distribución y circulación de la obra sin la autorización del autor; Artículo 218: Formas agravadas; Artículo 219: Plagio; Artículo 220: Formas agravadas; Artículo 220-A: Elusión de medida tecnológica efectiva; Artículo 220-B: Productos destinados a la elusión de medidas tecnológicas; Artículo 220-C: Servicios destinados a la elusión de medidas tecnológicas; Artículo 220-D: Delitos contra la información sobre gestión de derechos; Artículo 220-E: Etiquetas, carátulas o empaques; Artículo 220-F: Manuales, licencias u otra documentación, o empaques no auténticos relacionados a programas de ordenador (Fuente: Art. 216 al 220 del CP)	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (Art. 10): 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artìsticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. 2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. 3. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo.

Como se aprecia en el cuadro, en todos los casos en los que el Convenio de Budapest ha hecho propuestas de tipificación, se han creado o modificado normas en el país relacionadas con el mismo objetivo. En la mayoría de los casos, las normas peruanas tienen una redacción similar, incluyendo aspectos clave como la necesidad de que los delitos sean cometidos “deliberada e ilegítimamente” e incluso empleando los mismos verbos rectores (infringir, producir, difundir, alterar, suprimir, etc.). En realidad, lo que se observa es más bien una ampliación de términos pues en varios delitos se agregan acciones más allá de lo sugerido por el Convenio (introducir, clonar, etc.). Además, la Ley N° 30096 introduce en la categoría de delitos informáticos otras conductas que no estuvieron contempladas en el texto final de Budapest, pero que han sido desarrolladas posteriormente a través de sus protocolos. Este es el caso de: Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (grooming), tráfico ilegal de datos personales y la modificación de los artículos 162 (Interferencia telefónica) y 323 (Discriminación e incitación a la discriminación) del Código Penal para que incluyan como agravante el uso de medios informáticos o Internet. Esto último no está exento de cierta polémica, pero en términos prácticos no afecta en nada la futura implementación del Convenio, toda vez que entre los actuales adherentes se discuten protocolos

para tipificar nuevos delitos como el discurso de odio y la xenofobia a través de medios informáticos.

Podría decirse entonces que la creación de un marco común de derecho penal sustantivo es una tarea bastante avanzada en el Perú, pero haber llegado a dicha situación ha requerido superar varios obstáculos. Por lo menos desde 2010, el interés por regular las situaciones relacionadas a los delitos informáticos produjo múltiples iniciativas legislativas que fueron materia de grandes debates entre los actores del ecosistema digital. La definición misma de "delitos informáticos" es problemática en tanto que no existe consenso en si esta debería abarcar solo a los delitos en donde el bien jurídico es la información o bien informático o incluir también a los delitos comunes cometidos mediante medios informáticos. El producto final de dichas discusiones, la Ley N° 30096 publicada en 2013, se decantó por la definición más amplia, pero recibió muchas críticas de forma y de fondo. Por ejemplo, no en todos los casos se había cuidado la redacción y se castigaba conductas comunes en Internet como la creación de bases de datos o acciones inofensivas y potencialmente beneficiosas como el ethical hacking. Diferentes expertos criticaron estos problemas en su momento y señalaron la distancia que existía en perjuicio del país entre dicha norma y el estándar propuesto por el Convenio de Budapest. Recién con las modificaciones introducidas por la Ley N° 30171 publicada en 2014 se mejoró la redacción y se modificaron o eliminaron las disposiciones problemáticas. El cuadro presentado refleja estos últimos cambios.

¿Significa esto que contamos con una legislación acorde al estándar de Budapest? En el papel, la respuesta es que sí, pero consideramos que el nivel de aplicación efectivo por parte de los operadores del sistema de justicia es incierto. En principio, no existe información pública disponible sobre la ocurrencia de este tipo de delitos, salvo por la contínua y constante aseveración de actores privados de que existe un peligro inminente y que buscan ofrecer productos de seguridad. Consecuentemente tampoco se conoce el número de causas que superan la investigación policial y se formalizan en un proceso penal, llegan a juicio y reciben una sentencia. Menos aún se sabe si la ciudadanía conoce que puede encauzar estas situaciones a través de la justicia. Al no existir cifras públicas ni otros medios para conocer el escenario actual, existe la sensación de que los diferentes actores interesados trabajan a ciegas o de forma descoordinada, pese a contar con una legislación adaptada al uso internacional. Prueba de ello son las diferentes iniciativas sectoriales que son impulsadas actualmente y que, en la mayoría de los casos, son contradictorias entre sí. Peor aún, existen otras que ya han reclamado la vulneración de diferentes derechos con el fin de facilitar la tarea de sus operadores ignorando procesos anteriores largamente consensuados. Por ejemplo, pese a que existe desde hace varios años un protocolo en el Código Procesal Penal para la intervención legal de las comunicaciones, en 2015 se aprobó el Decreto Legislativo N° 1182 que creó un mecanismo por fuera de esta ley, que permitía a la policía acceder a datos

de geolocalización sin orden judicial.6 Esto último compromete la legalidad de ciertas medidas de acceso y retención y precariza la posición peruana frente a la implementación del Convenio.

1.2.2 ESTANDARIZACIÓN DE PROCESOS PENALES

Junto con la normas penales, en su Segundo Capítulo el Convenio de Budapest propone diferentes medidas procesales con el fin de viabilizar la persecución penal y facilitar la informática forense, es decir la acumulación de pruebas que permitan demostrar la comisión de los delitos informáticos, identificar a sus autores y conducirlos a juicio. Estas medidas se pueden dividir en propuestas sobre garantías procesales y propuestas sobre obligaciones de vigilancia. Las primeras son: el ámbito de aplicación del marco penal común, las condiciones y salvaguardias y los límites a la jurisdicción. Las otras abarcan diferentes obligaciones de conservación de datos informáticos, la revelación de dicho datos en tiempo real, su interceptación y los procedimientos para el registro y confiscación.

Siguiendo el ejemplo del punto anterior, se va a emplear un cuadro para comparar las propuestas del Convenio de Budapest con la legislación peruana en materia procesal aplicable a los delitos informáticos:

6 "Cinco claves para entender la Ley de Geolocalización", Diario La República, 2015, https://goo.gl/Meevzz

Tipo	Código Procesal Peruano	Convenio de Budapest
Disposiciones comunes	Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles: 1. El Fiscal, cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad y la intervención sea absolutamente necesaria para proseguir las investigaciones, podrá solicitar al Juez de la Investigación Preparatoria la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación. Rige lo dispuesto en el numeral 4) del artículo 226. 2. La orden judicial puede dirigirse contra el investigado o contra personas de las que cabe estimar fundadamente, en mérito a datos objetivos determinados que reciben o tramitan por cuenta del investigado determinadas comunicaciones, o que el investigado utiliza su comunicación. 3. El requerimiento del Fiscal y, en su caso, la resolución judicial que la autorice, deberá indicar el nombre y dirección del afectado por la medida si se conociera, así como, de ser posible, la identidad del teléfono u otro medio de comunicación o telecomunicación a intervenir, grabar o registrar. También indicará la forma de la interceptación, su alcance y su duración, al igual que la dependencia policial o Fiscalía que se encargará de la diligencia de intervención y grabación o registro. El Juez comunicará al Fiscal que solicitó la medida el mandato judicial de levantamiento del secreto de las comunicaciones. La comunicación a los concesionarios de servicios públicos de telecomunicaciones, a efectos de cautelar la reserva del caso, será mediante oficio y en dicho documento se transcribirá la parte concerniente. 4.Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento. Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos y software, se encontrarán obligados a mantener la compatibilidad con el sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú. 5. Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente. 6. La interceptación no puede durar más de sesenta días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal y decisión motivada del Juez de la Investigación Preparatoria. (Fuente: Art. 230, NCPP modificado por Ley N° 30096)	Ámbito de aplicación de las medidas de derecho procesal (Art. 14): 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos. 2. Salvo disposición en contrario, prevista en el artículo 21, los Estados podrán aplicar los poderes y procedimientos mencionados en el párrafo 1: a) a las infracciones penales establecidas en los artículos 2 a 11 del presente Convenio; b) a cualquier otra infracción penal cometida a través de un sistema informático; y c) a la recogida de pruebas electrónicas de cualquier infracción penal. 3. a) Los Estados podrán reservarse el derecho de aplicar la medida mencionada en el artículo 20 a las infracciones especificadas en sus reservas, siempre que el número de dichas infracciones no supere el de aquellas a las que se aplica la medida mencionada en el artículo 21. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de la medida mencionada en el artículo 20. b) Cuando un Estado, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del presente Convenio, no esté en condiciones de aplicar las medidas descritas en los artículos 20 y 21 a las comunicaciones transmitidas en un sistema informático de un prestador de servicios que: i. es utilizado en beneficio de un grupo de usuarios cerrado, y ii. no emplea las redes públicas de telecomunicación y no está conectado a otro sistema informático, público o privado, ese Estado podrá reservarse el derecho de no aplicar dichas medidas a tales comunicaciones. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.
	Legitimidad de la prueba: 1. Todo medio de prueba será valorado sólo si ha sido obtenido e incorporado al proceso por un procedimiento constitucionalmente legítimo 2. Carecen de efecto legal las pruebas obtenidas, directa o indirectamente, con violación del contenido esencial de los derechos fundamentales de la persona. 3. La inobservancia de cualquier regla de garantía constitucional establecida a favor del procesado no podrá hacerse valer en su perjuicio. (Fuente: Artículo VIII del Título Preliminar del NCPP)	Condiciones y garantías (Art. 15): 1. Los Estados velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad. 2. Cuando ello sea posible, en atención a la naturaleza del poder o del procedimiento de que se trate, dichas condiciones y garantías incluirán, entre otras, la supervisión judicial u otras formas de supervisión independiente, la motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión. 3. Los Estados examinarán la repercusión de los poderes y procedimientos de esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros, como exigencia dimanante del interés público y, en particular, de una correcta administración de justicia.

Conservación inmediata de datos informáticos almacenados	Art. 230, NCPP modificado por Ley N° 30096 y; DECRETO LEGISLATIVO QUE REGULA EL USO DE LOS DATOS DERIVADOS DE LAS TELECOMUNICACIONES PARA LA IDENTIFICACIÓN, LOCALIZACIÓN Y GEOLOCALIZACIÓN DE EQUIPOS DE COMUNICACIÓN, EN LA LUCHA CONTRA LA DELINCUENCIA Y EL CRIMEN ORGANIZADO: (...) Disposiciones Complementarias Finales: Primera.- Implementación: Para los efectos de la entrega de los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas o privadas relacionadas con estos servicios, implementan mecanismos de acceso exclusivo a la unidad especializada de la Policía Nacional del Perú. Segunda.- Conservación de los datos derivados de las telecomunicaciones: Los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas relacionadas con estos servicios deben conservar los datos derivados de las telecomunicaciones durante los primeros doce (12) meses en sistemas informáticos que permitan su consulta y entrega en línea y en tiempo real. Concluido el referido período, deberán conservar dichos datos por veinticuatro (24) meses adicionales, en un sistema de almacenamiento electrónico.La entrega de datos almacenados por un periodo no mayor a doce meses, se realiza en línea y en tiempo real después de recibida la autorización judicial. Para el caso de los datos almacenados por un periodo mayor a doce meses, se hará entrega dentro de los siete (7) días siguientes a la autorización judicial, bajo responsabilidad(...) (Fuente: Decreto Legislativo N° 1182)	Conservación inmediata de datos informáticos almacenados (Art. 16): 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación. 2. Los Estados adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos --que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente--durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente. 3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno. 4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.
	Art. 230, NCPP modificado por Ley N° 30096 y; Decreto Legislativo N° 1882	Conservación inmediata y divulgación de datos de tráfico (Art. 17): 1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para: a. procurar la conservación inmediata de los datos de tráfico, cuando uno o más prestadores de servicio hayan participado en la transmisión de dicha comunicación; y b. asegurar la comunicación inmediata a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido. 2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.
Mandato de comunicación	Art. 230, NCPP modificado por Ley N° 30096 y; Decreto Legislativo N° 1882	Mandato de comunicación (Art. 18): 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar: a. a una persona presente en su territorio que comunique los datos informáticos especificados, en posesión o bajo el control de dicha persona, y almacenados en un sistema informático o en un soporte de almacenaje informático; y b. a un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, que comunique los datos en su poder o bajo su control relativos a los abonados y que conciernan a tales servicios; 2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15. 3. A los efectos del presente artículo, la expresión «datos relativos a los abonados» designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido, y que permite establecer: a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio; b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y el pago, disponibles por razón de un contrato o de un alquiler de servicio; c. cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un alquiler de servicio.

Registro y decomiso de datos informáticos almacenados	Art. 230, NCPP modificado por Ley N° 30096; Decreto Legislativo N° 188; y Diligencia de secuestro o exhibición: 1. Obtenida la autorización, el Fiscal la ejecutará inmediatamente, contando con el auxilio policial. Si no se perjudica la finalidad de la diligencia, el Fiscal señalará día y hora para la realización de la diligencia, con citación de las partes. Al inicio de la diligencia se entregará copia de la autorización al interesado, si se encontrare presente. 2. Los bienes objeto de incautación deben ser registrados con exactitud y debidamente individualizados, estableciéndose los mecanismos de seguridad para evitar confusiones o alteración de su estado original; igualmente se debe identificar al funcionario o persona que asume la responsabilidad o custodia del material incautado. De la ejecución de la medida se debe levantar un acta, que será firmada por los participantes en el acto. Corresponde al Fiscal determinar con precisión las condiciones y las personas que intervienen en la recolección, envío, manejo, análisis y conservación de lo incautado, asimismo, los cambios hechos en ellos por cada custodio. 3. Sin perjuicio de lo anterior, si se trata de incautación de bienes muebles se procederá de manera que se tomen bajo custodia y -si es posible- se inscribirá en el registro correspondiente. Si se trata de bienes inmuebles o de un derecho sobre él, adicionalmente a su ocupación, se operará de manera que se anote en el registro respectivo dicha medida, en cuyo caso se instará la orden judicial respectiva. 4. Lo dispuesto en los dos numerales anteriores es aplicable cuando la exhibición o incautación es realizada por la Policía o el Fiscal en los casos previstos en el artículo 216.2 5. La Fiscalía de la Nación, a fin de garantizar la autenticidad de lo incautado, dictará el Reglamento correspondiente a fin de normar el diseño y control de la cadena de custodia, así como el procedimiento de seguridad y conservación de los bienes incautados. (Fuente: Art. 220 NCPP)	Registro y decomiso de datos informáticos almacenados (Art. 19): 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para registrar o acceder de un modo similar: a. a un sistema informático o a una parte del mismo, así como a los datos informáticos que están almacenados; y b. a un soporte de almacenamiento que permita contener datos informáticos en su territorio. 2. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para procurar que, cuando sus autoridades registren o accedan de un modo similar a un sistema informático específico o a una parte del mismo, conforme al párrafo 1 (a), y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son igualmente accesibles a partir del sistema inicial o están disponibles a través de ese primer sistema, dichas autoridades estén en condiciones de ampliar inmediatamente el registro o el acceso y extenderlo al otro sistema. 3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para decomisar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en aplicación de los párrafos 1 o 2. Estas medidas incluyen las prerrogativas siguientes: a. decomisar u obtener de un modo similar un sistema informático o una parte del mismo o un soporte de almacenaje informático; b. realizar y conservar una copia de esos datos informáticos; c. preservar la integridad de los datos informáticos almacenados pertinentes; y d. hacer inaccesibles o retirar los datos informáticos del sistema informático consultado. 4. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a cualquier persona, que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione todas las informaciones razonablemente necesarias, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2. 5. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.
Recogida en tiempo real de datos informáticos	Art. 230, NCPP modificado por Ley N° 30096 y; Decreto Legislativo N° 1882	Recogida en tiempo real de datos de tráfico (Art. 20): 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para: a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio a través de un sistema informático. 2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio. 3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto. 4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.
	Art. 230, NCPP modificado por Ley N° 30096 y; Decreto Legislativo N° 1882	Interceptación de datos relativos al contenido (Art: 21): 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes respecto a infracciones consideradas graves conforme a su derecho interno para: a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; y b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos relativos al contenido de concretas comunicaciones en su territorio, transmitidas a través de un sistema informático. 2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos relativos al contenido de concretas comunicaciones transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio. 3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto. 4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Jurisdicción	Artículo 19: Determinación de la competencia; Artículo 20: Efectos de las cuestiones de competencia; Artículo 21: Competencia territorial; Artículo 22: Delitos cometidos en un medio de transporte; Artículo 23: Delito cometido en el extranjero; y Artículo 24: Delitos graves y de trascendencia nacional(Fuente: Art. 19 al 24 del NCPP)	Jurisdicción (Art. 22): 1. 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido: a. en su territorio; b. a bordo de una nave que ondee pabellón de ese Estado; c. a bordo de una aeronave inmatriculada en ese Estado; d. por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado. 2. Los Estados podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones específicas, las reglas de competencia definidas en los párrafos 1b a 1d del presente artículo o en cualquiera de las partes de esos párrafos. 3. Los Estados firmantes adoptarán las medidas que se estimen necesarias para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1 del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición. 4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno. 5. Cuando varios Estados reivindiquen una competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución.

Como se aprecia en el cuadro, a diferencia del Código Penal, las disposiciones del Código Procesal Penal aplicables a los delitos informáticos evidentemente no fueron pensadas teniendo al Convenio de Budapest como referente. Por el contrario, la reforma del anterior Código Procesal Penal que condujo a la redacción y aprobación en 2004 del Nuevo Código Procesal Penal (NCPP) estuvo casi exclusivamente enfocada en renovar el sistema de acusación penal e introducir instituciones nuevas con el fin de adecuar y limitar los roles de los actores en todas las etapas del proceso penal. No obstante, por su misma naturaleza, este corpus de normas también es susceptible de modificaciones a través de leyes específicas.

Con respecto a las propuestas sobre garantías procesales no encontramos que sean necesarias grandes modificaciones en la legislación peruana. Las disposiciones comunes del Convenio de Budapest proponen un marco para la aplicación de medidas procesales especiales para los delitos informáticos, un apartado sobre las garantías y finalmente el ámbito de la jurisdicción aplicable. En estos tres aspectos, actualmente se aplican normas del NCPP de orden general relacionadas a la legalidad de la obtención y uso de las pruebas, el debido proceso y el ámbito de la competencia territorial respectivamente. En una evaluación inicial, las normas procesales peruanas vigentes parecen adaptarse bien a lo propuesto por el Convenio de Budapest, al menos en lo esencial, por lo que no parece necesario una reforma sustancial.

Diferente es el caso respecto a las propuestas sobre obligaciones de vigilancia. El Convenio de Budapest propone medidas relacionadas a la recolección, interceptación, disposición y conservación de datos informáticos, lo que incluye no solo la información del tráfico de datos sino también el contenido de los mismos y los dispositivos donde están almacenados, a veces en tiempo real. Este tipo de medidas han sido introducidas principalmente por las modificaciones de la Ley N° 30096 al artículo N° 230 del NCPP relacionado a la intervención de las comunicaciones. Allí se establecen mecanismos de cooperación y obligaciones para los concesionarios de servicios de telecomunicación. No obstante, hasta la fecha no se ha desarrollado de forma específica su modo de aplicación, lo que parece haberse dejado para los manuales y protocolos

de investigación del Ministerio Público, que es el encargado de solicitar estas medidas al Poder Judicial. Sin embargo, existe otra norma habilitante para adoptar estos mecanismos que fue aprobada en 2015: el Decreto Legislativo 1182, que se superpone al NCPP y crea un régimen especial para la geolocalización de dispositivos móviles, además de (volver) a imponer obligaciones de recolección, conservación y entrega a las compañías de telecomunicación. Este Decreto además otorga facultades a la Policía sin requerir un mandato judicial para hacer estos pedidos, lo que pone en riesgo la constitucionalidad de dicha medida y la validez de las pruebas. Debe tenerse en cuenta que esto puede resultar problemático para la implementación del Convenio de Budapest pues la coexistencia de ambas normas pueden producir resultados inválidos.

1.2.3 COOPERACIÓN INTERNACIONAL

Finalmente, en el Tercer Capítulo, el Convenio de Budapest establece una serie de obligaciones mínimas y disposiciones comunes para hacer viable la cooperación entre sus miembros. Estas obligaciones están referidas principalmente a la adaptación de la legislación en materia de extradición, la asistencia mutua y la creación de un aparato de respuesta a emergencias. En el primer caso, la propuesta del Convenio de Budapest es hacer posible la extradición siempre que se cometa un delito informático y los países envueltos lo hayan tipificado en su norma penal. Para ello propone adicionar los delitos informáticos en tratados previos de extradición y, de no existir, emplear el Convenio como base legal para que estos puedan ser ejecutados. En lo que respecta a la asistencia mutua, se propone que los resultados producto de las medidas propuestas en la sección de procesos penales puedan ser compartidos entre los miembros en situaciones específicas, con el fin de ampliar la eficacia de la persecución penal. Finalmente, se propone un modelo de cooperación basado en la designación de puntos de contacto para atender solicitudes de emergencia que pueden o no estar relacionadas al contenido de los pedidos de asistencia mutua.

A la fecha, el Perú no ha suscrito ningún acuerdo o tratado internacional en donde se incluyan cláusulas equivalentes a las propuestas del Convenio de Budapest en materia de cooperación internacional. No obstante, eso no significa que no se cuente con mecanismos análogos, al menos en el caso de la aplicación de la extradición y la cooperación judicial internacional. Por ejemplo, los alcances de la extradición en el Perú están plasmados en un capítulo especial del NCPP (artículos 513 al 527). Lo mismo en el caso de la asistencia mutua judicial, que está regulada también en dicho Código (artículos del 508 al 512 y 528 al 539). No obstante, como su nombre lo indica, esta asistencia abarca solamente al sistema judicial peruano y por lo tanto quedan fuera otros actores como la Policía Nacional. En el caso del modelo de cooperación basado en el punto de contacto, al no haber suscrito el Convenio de Budapest, el Perú no ha construido una red específica para atender esta obligación, pero actualmente participa de redes similares que incluso se retroalimentan con la red de los miembros del Convenio. Una de ellas es el Subgrupo de Delitos de Alta Tecnología que existe dentro del G8, en donde el Perú participa activamente desde hace más de diez

años. Otra es el contacto de Interpol en donde sí está incluida la Policía Nacional y es el actor principal.

1.3 ACCIONES ESENCIALES PARA UNA IMPLEMENTACIÓN EXITOSA

Habiendo analizado la situación en la que se encuentra el país, todo parece indicar que en materia de adecuación, es poco lo que debería modificarse de forma sustantiva para implementar el Convenio de Budapest. No obstante, sí existen algunas medidas que merecen especial atención y sin las cuales el cumplimiento de los objetivos del Convenio no podrán ser abordados de forma exitosa. Estas acciones están principalmente orientadas a viabilizar la implementación del Convenio y explotar sus beneficios, especialmente los relacionados a la adecuación normativa y la cooperación internacional.

Hemos propuesto, a modo de ejercicio didáctico, cuáles serían algunas de estas acciones. En general, el Gobierno debe impulsar desde el nivel más alto un proceso de análisis para comprender las ventanas de oportunidad para aplicar reformas y debe tener en cuenta que la participación de otros actores no estatales es vital para la viabilidad de cualquier propuesta. Tomando como experiencia las leyes de delitos informáticos, debería ser tenido en cuenta que a mayor consenso, son mayores las oportunidades de gestionar un ecosistema de seguridad fuerte y soportado por todos los interesados.

Para una mejor comprensión, las acciones propuestas están ordenadas en función a una secuencia cronológica ideal:

1. REVISIÓN NORMATIVA POSTERIOR A LA RATIFICACIÓN DEL CONVENIO

Mediante Decreto Supremo, el Poder Ejecutivo debe crear un grupo de trabajo multisectorial con el objetivo de evaluar el proceso de implementación del Convenio de Budapest. Este grupo de trabajo debe estar conformado mínimamente por: Un representante de la Secretaría de Gobierno Digital, un representante del Ministerio de Relaciones Exteriores, un representante del Ministerio de Justicia y Derechos Humanos, un representante del Ministerio de Transporte y Comunicaciones, un representante del Ministerio del Interior, un representante del Ministerio de Defensa y otras entidades que se estime conveniente, inclusive fuera del sector público. El objetivo del grupo de trabajo será realizar un análisis de la situación de cara a la implementación del Convenio de Budapest y propondrá reformas en todos los niveles del Estado para lograr una adecuación exitosa.

2. APOYO EN ORGANISMOS MULTILATERALES

Como primer acto luego de su creación, el grupo de trabajo multisectorial cursará dos solicitudes formales para obtener asesoría externa en el proceso de análisis y proposición de reformas para la adecuación al Convenio de Budapest. Una estará dirigida a la Oficina del Programa de Cibercriminalidad del

Consejo de Europa y la otra a la Gerencia de Programa de Seguridad Cibernética de la Organización de Estados Americanos. Ambas solicitudes no son excluyentes y ayudarán a obtener una visión más amplia de las necesidades de cada institución dentro del Estado.

3. PARTICIPACIÓN DE MÚLTIPLES PARTES INTERESADAS

Con el fin de enriquecer el debate y validar sus avances, el grupo de trabajo multisectorial propondrá la creación de varias mesas de trabajo abiertas y públicas enfocadas en temas específicos como: reforma de la ley de delitos informáticos, reforma de la ley procesal sobre delitos informáticos, mecanismos de cooperación internacional sobre delitos informáticos, entre otros. Esto con el fin de que las propuestas de reforma incorporen orgánicamente la opinión de los actores interesados del sector privado. Estos grupos pueden o no ser creados formalmente y pueden construirse a partir de mesas de trabajo ya existentes en diferente sectores, como es el caso de la Comisión para el Desarrollo de la Sociedad de la Información que se desarrolla dentro del Ministerio de Transporte y Comunicaciones.

4. PAQUETE DE MEDIDAS IMPULSADAS EN EL MARCO DEL FORTALECIMIENTO DE LA CIBERSEGURIDAD

Una vez concluido el análisis y entregado el informe con la propuesta de reformas, el Poder Ejecutivo elaborará uno o varios proyectos de ley que idealmente deberán ser agrupados en un “paquete” de medidas identificadas como necesarias para la ejecución de los objetivos del Convenio de Budapest. Este paquete eventualmente será derivado a la o las comisiones del Congreso de la República encargadas de su evaluación, las cuales deberán realizar una nueva valoración para perfeccionar aquellos puntos controvertidos e incorporar otros proyectos de ley que sean pertinentes con el fin de que el paquete de medidas sea aprobado de forma íntegra.

5. CREACIÓN DE UN PLAN NACIONAL DE CIBERSEGURIDAD

Una vez aprobado el paquete de medidas, durante el proceso de evaluación en el Congreso o incluso anteriormente, el Poder Ejecutivo creará por Decreto Supremo el Comité para la redacción del Plan Nacional de Ciberseguridad que deberá tener una composición de múltiples actores interesados públicos y privados. Este Comité tendrá como objetivo la redacción del Plan Nacional de Ciberseguridad y adicionalmente supervisará la adecuación de las diferentes entidades para su ejecución, lo que eventualmente hará coincidir sus acciones con la ejecución del paquete legislativo si este es aprobado en el Congreso, especialmente en los aspectos de creación de capacidades e implementación de medidas para la cooperación internacional.

Todas estas acciones constituyen un núcleo mínimo inicial y deben ser ejecutadas de tal forma que no entorpezcan otros procesos o terminen siendo

asimiladas por otras agendas. Escapa del alcance de este informe profundizar en la forma cómo deberían aplicarse y cuál debería ser el rol de las entidades públicas y privadas en su ejecución. Sin embargo, es de esperar que el proceso completo demore varios años y que su perfeccionamiento y puesta en ejecución no sea uniforme y esté llena de obstáculos que los actores deberán superar mediante el consenso y la adaptación al contexto peruano de las mejores prácticas internacionales.

2. IMPACTO EN EL CORTO, MEDIANO Y LARGO PLAZO

La situación actual y las acciones esenciales descritas anteriormente nos dan una idea general de cuál podría ser el impacto en el país luego de que el Convenio de Budapest sea ratificado y empiece el proceso de implementación. Sin embargo, como ha ocurrido ya en otros países, este proceso puede tardar muchos años y retrasarse por diferentes factores. No obstante, aún suponiendo que los avances serán progresivos, es posible proyectar el impacto que tendrán en diferentes ámbitos de la sociedad en los próximos diez años. Este informe se ha planteado tres escenarios relevantes en los cuales dicho impacto debería ser más visible y que se emplean como una primera aproximación a un estudio más integral: las políticas públicas, los actores y roles y los derechos humanos. Algunas proyecciones pueden parecer superpuestas o contradictorias entre sí, debido a que representan diferentes escenarios, algunos más probables que otros.

2.1 POLÍTICAS PÚBLICAS

En el ámbito de las políticas públicas, entendidas como el conjunto de normas, acciones y productos propuestos por diferentes actores pero impulsados principalmente desde el sector público, encontramos factibles diferentes escenarios. Por ejemplo, es altamente probable que tras la ratificación, la incidencia de propuestas de política pública relacionadas a la ciberseguridad sufra un salto cuantitativo. En los últimos años, se han propuesto todo tipo de normas que inciden en esta área y con las nuevas herramientas que pone a disposición el Convenio de Budapest, es de esperar que estas aumenten. Como consecuencia de ello, dependiendo del uso que se les pretenda dar, podrían aumentar los pedidos por adoptar sistemas de vigilancia más intrusivos o, por el contrario, se fortalecerán los medios actuales y la cooperación internacional.

A continuación anexamos un cuadro en donde hemos colocado las proyecciones respecto de políticas públicas que podemos esperar en los próximos diez años:

Período	Medidas	Poco Probable	Probable	Muy probable
Corto Plazo	Creación de un Comité para la implementación del Convenio de Budapest.			x
	Múltiples propuestas para expandir las obligaciones de vigilancia de intermediarios.		x	
Mediano Plazo	Proceso de redacción de un Plan Nacional de Ciberseguridad.			x
	Adquisición de equipos para aumentar la capacidad de respuesta del Estado a emergencias informáticas.		x	
	Capacitación de funcionarios y servidores públicos en materia de ciberseguridad.			x
	Múltiples propuestas para modificar la ley actual de delitos informáticos.			x
	Múltiples propuestas para modificar la ley actual de Protección de Datos Personales.		x	
	Múltiples propuestas para incluir nuevos delitos informáticos como acoso en línea, pornografía de venganza, etc.			x
Largo Plazo	Creación de diferentes planes sectoriales para avanzar en la concientización de la población sobre la ciberseguridad.		x	
	Otras políticas públicas sectoriales que incluyan elementos TICs en sus planes.		x	

2.2 ACTORES Y ROLES

En el caso de los actores y sus roles, como hemos indicado a lo largo de este informe, en cuestión de entidades, el Perú se alinea con las prácticas de los países que ya han implementado el Convenio de Budapest. En principio, quien suponemos jugará un rol importante dentro del proceso de implementación del Convenio de Budapest es la Secretaría de Gobierno Digital. Esta instancia hasta el momento se ha caracterizado por su transparencia y apertura hacia los actores no estatales. Sin embargo, pese a que en teoría es la instancia que debería guiar este proceso, su posición dentro de la jerarquía estatal podría comprometer la efectividad de sus disposiciones frente a otros actores, incluso dentro del Estado.

Respecto del sector privado, proyectamos que las empresas probablemente apunten a estimular el crecimiento de un mercado interno de la seguridad informática con el fin de encontrar soluciones locales a precios competitivos, las cuales serán vitales en el crecimiento de pqueñas y medianas empresas. Así mismo, la oferta educativa relacionada a las TICs seguramente experimentará también un alza. En cuanto a la sociedad civil organizada podríamos decir que es probable que las organizaciones de derechos humanos empiecen a tomar más atención a estos temas.

A continuación anexamos un cuadro en donde hemos colocado las proyecciones respecto de actores y roles que podemos esperar en los próximos diez años:

Actores	Medidas	Poco Probable	Probable	Muy probable
Gobierno	Modificación de la estructura encargada de Gobierno Digital, pudiendo crecer en número de personal o creándose nuevas oficinas especializadas dentro de la Presidencia del Consejo de Ministros y otros ministerios.		x	
	Creación de una entidad autónoma encargada del desarrollo de las TICs dentro y fuera del Estado.	x		
	Creación del Viceministerio de las Tecnologías de Información y Comunicación, localizado dentro del Ministerio de Transportes y Comunicaciones encargado de las políticas públicas en materia de TICs dirigidas al sector privado.		x	
	Repotenciación del PeCERT y de otros CERT estatales.			
	Creación de fiscalías y juzgados especializadas en delitos informáticos con personal capacitado.		x	
	Recomposición de las oficinas TICs en los ministerios, para mejorar la capacidad de respuesta del Estado a emergencias informáticas.		x	
Sector Privado	Participación más activa de diferentes sectores en la creación de políticas públicas en materia de ciberseguridad.		x	
	Aumento de la inversión en seguridad informática.			x
	Crecimiento del mercado de la seguridad informática a partir de la mayor demanda de las pequeñas y medianas empresas.			x
	Crecimiento de la oferta académica en materia de ciberseguridad, dirigida especialmente a profesionales del sector TIC.			x
	Promoción de CERTs público-privados, especialmente en el sector bancario.			x
	Incentivos del sector para la creación de startups y otros emprendimientos que creen soluciones innovadoras en seguridad informática.		x	
Sociedad Civil y Academia	Implementación progresiva de elementos de derecho informático y ciberseguridad en el currículum de aprendizaje de facultades de Derecho, Ingeniería y otras afines.		x	
	Crecimiento de la demanda de abogados e ingenieros con formación de peritos informáticos o con experiencia en informática forense.			x
	Indiferencia por gran parte de la sociedad civil.			x
	Fomento de la cultura de seguridad digital al interior de organizaciones de derechos humanos y colectivos sociales.		x	
	Falta de representatividad de la sociedad civil en las políticas públicas de ciberseguridad aplicadas por el Estado al no haber sido incluida en el proceso de redacción del Plan Nacional de Ciberseguridad.		x	
	Participación activa de la sociedad civil en las políticas públicas de ciberseguridad aplicadas por el Estado al haber sido incluida en el proceso de redacción del Plan Nacional de Ciberseguridad.		x	

2.3 DERECHOS HUMANOS

Finalmente, en lo que corresponde a los derechos humanos, proyectamos que la forma en que estos serán valorados depende en gran medida de cómo se desarrollen los puntos anteriores y las configuraciones que adopte el ecosistema. Por ejemplo, si las normas sobre vigilancia aumentan, las organizaciones de sociedad civil no actúan y la creación de normas de ciberseguridad pasan a ser competencias de entidades asociadas a las fuerzas armadas, es evidente que se producirá una erosión de los derechos humanos.

En el ámbito de los derechos humanos podemos esperar en los próximos diez años:

Período	Medidas	Poco Probable	Probable	Muy probable
Mediano Plazo	Erosión de los derechos a la privacidad, el secreto de la telecomunicaciones y otros conexos debido a la creación de mayores obligaciones de vigilancia para la implementación de los objetivos del Convenio de Budapest.		x	
	Respeto de los derechos a la privacidad, el secreto de la telecomunicaciones y otros conexos debido a la implementación consensuada de los objetivos del Convenio de Budapest.		x	
	Incremento de acciones de incidencia y litigio estratégico por parte de organizaciones de derechos humanos contra normas, disposiciones internas y tecnologías creadas o adquiridas para implementar los objetivos del Convenio de Budapest, especialmente en lo que se refiere medidas de vigilancia y procedimientos de informática forense.		x	
Largo Plazo	Ecosistema digital tóxico producto de la imposición de normas y disposiciones internas sobre ciberseguridad y tecnologías que afectan los derechos humanos.		x	
	Ecosistema digital saludable producto de la implementación consensual de normas y disposiciones internas sobre ciberseguridad y tecnologías de uso limitado y respetuosas de los derechos humanos.		x	

3. CONCLUSIONES

A partir de los hallazgos de nuestro análisis y de lo descrito hasta este momento, queremos ofrecer las siguientes conclusiones:

3.1 SOBRE LA SITUACIÓN ACTUAL

A grandes rasgos, el Perú posee normas e instituciones similares a las de los países miembros del Convenio de Budapest pues durante muchos años ha interactuado directa o indirectamente con este instrumento internacional para sus propios procesos de reforma. No obstante, pese a ello, en la práctica la incidencia de los delitos informáticos y las amenazas a la seguridad informática aún es baja en el país comparada incluso con sus pares dentro de la región. Esto ha impedido que se mida su robustez, pero es posible que esta se ponga a prueba en los siguientes años. La implementación del Convenio de Budapest es visto como una forma de iniciar un proceso de revisión y modernización del esquema actual.

3.2 SOBRE EL PROCESO DE IMPLEMENTACIÓN

Respecto de los tres objetivos declarados del Convenio de Budapest: Crear un marco común de derecho penal sustantivo, estandarizar los métodos procesales y la informática forense e impulsar la cooperación internacional; y habiendo analizado la situación del país, debemos concluir que la implementación del Convenio no requerirá mayores cambios. Probablemente en donde se presenten las mejores oportunidades de formular políticas públicas en materia de ciberseguridad serán en el ámbito de la cooperación internacional, lo que abrirá la puerta para una inserción mayor del país en los espacios de discusión que el Convenio habilita para sus miembros.

3.3 SOBRE EL IMPACTO DE LA IMPLEMENTACIÓN

El impacto de la implementación del Convenio de Budapest es variable y depende en gran medida de la interacción entre la formulación de políticas públicas, el nivel de involucramiento de los actores y los roles que logren cumplir, así como el nivel de respeto de los derechos humanos involucrados en todas las etapas. En los cuadros de pronóstico que hemos presentado hemos intentando asumir algunos de los escenarios que a veces son positivos, pero también negativos en relación al ecosistema digital peruano.

La forma cómo esto evolucione depende del compromiso que organizaciones de todos los sectores asuman. Es por ello que esperamos que los debates acerca de la implementación se den en espacios abiertos y transparentes.

hiperderecho

@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina