Deconstruyendo la Ley de Delitos Informáticos

Miguel MORACHIMO RODRÍGUEZ*

RESUMEN

Tras la promulgación de la Ley de Delitos Informáticos, el autor del presente artículo nos presenta un análisis detallado del proceso de gestación de esta norma, criticando que ninguno de los proyectos de ley de los que se originó haya tomado en cuenta las estadísticas existentes en materia de criminalidad informática. Asimismo, nos presenta un valioso aporte al proponer cinco modificaciones que buscan salvaguardar el principio de legalidad penal, al establecer con mayor precisión la configuración de los tipos penales.

En este artículo me propongo realizar una crítica constructiva a la recientemente aprobada Ley Nº 30096, Ley de Delitos Informáticos. Sobre la base del marco jurídico aplicable en sede nacional e internacional, propongo cinco cambios críticos que podrían realizarse a la ley ya aprobada con la finalidad de convertirla en una auténtica herramienta de lucha contra los delitos informáticos. Los cambios propuestos no pretenden desnaturalizarla sino, por el contrario, dotarla de efectividad y evitar que plantee conflictos con el ejercicio de derechos fundamentales.

Para fines de este trabajo, debemos entender como delito informático a todo delito cometido utilizando tecnologías de la información. En esta definición incluyo a los delitos que afectan computadoras y sistemas informáticos y también aquellos delitos tradicionales como el fraude, la usurpación de identidad o la estafa cuando se llevan a cabo usando un medio informático.

En la primera sección hago un recuento de los antecedentes de la regulación de los delitos informáticos en Perú, incluyendo indicadores estadísticos sobre su incidencia. La segunda parte está dedicada a describir la trayectoria de los diferentes proyectos de ley que terminaron componiendo la Ley de Delitos Informáticos, así como su debate y posterior aprobación por parte del Poder Ejecutivo. Finalmente, la tercera parte está orientada a proponer reformas puntuales a la ley ya aprobada, identificando los problemas de la versión vigente.

I. ¿DELITOS INFORMÁTICOS EN EL PERÚ?

Perú no era un país ajeno a la problemática de la regulación del uso criminal de la tecnología. Por el contrario, nuestro Código Penal ya tenía desde el año 2000 tres artículos especiales sobre delitos informáticos. Sin embargo, estos no eran los únicos "delitos informáticos" reconocidos en nuestro Código Penal. Si entendemos como delitos informáticos, como lo entiende la

* Director de la ONG Hiperderecho, organización sin fines de lucro dedicada a facilitar el entendimiento público de las interacciones entre el Derecho y la tecnología.

nueva Ley, a aquellos delitos que se cometen usando la tecnología podemos ampliar el espectro. Hasta antes de la promulgación de la nueva Ley de Delitos Informáticos, también teníamos tipificados los delitos de apología del delito a través de tecnologías de la información (artículo 316) y elusión de medidas de protección tecnológicas (artículo 220 y siguientes). Además de estos delitos que incorporaban específicamente un elemento tecnológico, debe de señalarse también la existencia de otros delitos como los de infracción a los derechos de autor (artículo 217), difamación (artículo 148-A), violación de la intimidad (artículo 154), violación de correspondencia (artículo 161), entre otros, que también eran posibles de cometerse usando medios tecnológicos.

Sin embargo, es poco lo que sabemos sobre la forma en la que se han venido aplicando estos artículos a lo largo del tiempo o sobre qué tan frecuentes son estos delitos en nuestro país. La estadística sobre el tema es dispersa, no está estandarizada o no proporciona el nivel de detalle suficiente. Uno de los pocos lugares donde encontramos información de varios años es en la página web del Ministerio Público, en cuyas memorias anuales listan los casos que se investigan por región y por tipo de delito. El siguiente cuadro muestra la evolución de la incidencia de casos de delitos informáticos investigados, e incluye los casos en los que la investigación se archivó y también aquellos en los que se dispuso iniciar un proceso.

Cuadro 1
Casos de delitos informáticos investigados por las fiscalías de lima

	2005	2006	2007	2008	2009	2010	2011	2012
Número de casos investigados	60	39	44	52	96	154	243	220
Porcentaje del total de casos investigados ese año	0.4 %	0.2 %	0.28 %	0.32 %	0.47 %	0.6 %	0.7 %	0.79 %

Fuente: Ministerio Público. Elaboración propia.

Aunque la información obtenida se circunscribe a Lima, puede servir como un indicador para adelantar algunas lecturas. La primera es que se investigan pocos casos de delitos informáticos ante el Ministerio Público, pese a tener desde el año 2000 varios artículos exclusivamente referidos a delitos informáticos. Aunque se puede apreciar una tendencia el crecimiento, todavía no representan ni el 1% de los delitos que investiga la fiscalía. Siguiendo la tendencia estadística de las Fiscalías Provinciales de Lima en el año 2012[1], el número de casos en los que se llega a formalizar una denuncia es cercano al 30 % de los casos estudiados. Por ende, el número de procesos que se llevan a cabo por delitos informáticos en Lima debe de ser alrededor de 60. Tampoco he encontrado estadísticas de cuántas sentencias condenatorias se emiten por la comisión de este tipo de delitos pero el número debe de ser aún menor.

La segunda lectura que podemos ensayar es que el aumento de usuarios de tecnología en nuestro país, que ha sido muy acelerado entre el 2005 y 2012, no necesariamente ha significado un aumento a igual ritmo de las denuncias por delitos informáticos. Aquí es importante comparar el porcentaje del total de casos investigados que representaban los delitos informáticos en el 2005 (0.4 %) con el porcentaje que representaron el 2012 (0.79 %). Si bien se investigan más casos actualmente, la proporción que esos casos representan del total de hechos potencialmente delictivos

1 MINISTERIO PÚBLICO. *Anuario Estadístico 2012*. Ministerio Público, Lima, 2012. Disponible en: <http://www.mpfn.gob.pe/estadistica/anuario_est_2012.pdf>, consultado el 12 de noviembre de 2012.

investigados ha aumentado solo un 50 %. En paralelo, el número de hogares que cuentan con al menos una computadora ha aumentado en el mismo periodo de tiempo en un 240 % según las cifras del Instituto Nacional de Estadística e Informática[2].

Sería incorrecto utilizar estas cifras para afirmar que los delitos informáticos no son un peligro para la sociedad. Pero sí considero apropiado empezar el debate teniendo a la vista la problemática en su real dimensión y contexto. Una lectura alternativa que podríamos hacer de estas estadísticas es que hay muchos delitos informáticos que se cometen sin que nadie llegue a dar parte de ellos al Ministerio Público, ya sea por desconocimiento o desinterés de las víctimas.

Ninguno de los ocho proyectos de ley que se han condensado para dar origen a la Ley de Delitos Informáticos ha tomado en cuenta estadísticas nacionales. Solo se mencionan estadísticas aisladas de la comisión de ciertos delitos como clonación de tarjetas. Pero ninguno ha hecho una evaluación crítica de cómo se han venido aplicado los artículos sobre delitos informáticos ya contenidos en nuestro Código Penal, ni tampoco ha mencionado casos o jurisprudencia en las que se evidencie la carencia de determinados tipos penales en nuestra legislación.

II. EL LARGO CAMINO A LA LEY DE DELITOS INFORMÁTICOS

La Ley de Delitos Informáticos que fue publicada a fines de octubre de 2013, realmente empezó a gestarse desde agosto de 2011. Fueron ocho los proyectos de ley que se unificaron, al menos formalmente, para dar origen a esta ley. Esta sección describe a grandes rasgos la trayectoria legislativa que la nueva ley tuvo.

1. Proyectos de ley iniciales

La primera iniciativa legislativa para regular los delitos informáticos fue el Proyecto de Ley Nº 34/2011-CR de agosto de 2011 presentado por Juan Carlos Eguren (Alianza por el Gran Cambio). El proyecto abarcaba una serie de delitos que iban desde intrusismo informático, violación del secreto de las telecomunicaciones, varios delitos relacionados con medios de pago y suplantación hasta pornografía infantil.

La segunda iniciativa fue el Proyecto de Ley Nº 307/2011-CR de setiembre de 2011 presentado por el congresista Octavio Salazar (bancada fujimorista). Esta propuesta estaba más enfocada en asuntos procedimentales, con una serie de artículos relacionados a la investigación fiscal e incluía la controvertida idea de excluir del ámbito de protección constitucional del secreto de las telecomunicaciones a los datos de IP de un usuario conectado a Internet.

El tercer Proyecto de Ley involucrado fue el Nº 1136/2011-CR presentado en mayo de 2012 por el congresista Tomás Zamudio (Gana Perú). Este Proyecto era menos ambicioso en alcance y solo proponía incluir el delito de robo de identidad virtual y una forma agravada para los tres delitos ya existentes en el Código Penal.

Estos tres proyectos de ley fueron elevados a la Comisión de Justicia y Derechos Humanos del Congreso para su análisis y dictamen durante el año 2012.

2. Dictamen de la Comisión de Justicia

La Comisión de Justicia y Derechos Humanos, entonces presidida por Alberto Beingolea, acordó unificar los tres proyectos de ley sobre delitos informáticos y aprobó un texto sustitutorio incorporándolos. Este texto sustitutorio tomaba buena parte de la propuesta de Juan Carlos Eguren y Octavio Salazar. Su aprobación y posterior publicación provocó una serie de comentarios negativos por parte de abogados, especialistas en tecnología y usuarios de Internet. Dicho texto pasó a ser conocido como Ley Beingolea, a pesar de que dicho

2 INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA. Hogares que tienen al menos una computadora, por años, según ámbitos geográficos. Disponible en: <http://www.inei.gob.pe/media/MenuRecursivo/Cap11005.xls>, consultado el 12 de noviembre de 2012.

congresista no fue el autor de ninguno de los proyectos. Quizás uno de los extremos más criticados de este proyecto era la exclusión de los datos de los números IP del ámbito de protección del secreto de las telecomunicaciones y autorizaba a que cualquier fiscal o policía lo solicite a la empresa operadora sin necesidad de intervención judicial.

> "El principio de legalidad penal existe pero no puede llevarnos a regular tecnologías en sí mismas, que están sujetas a un cambio constante."

Sin embargo, y pese a las críticas que recibió, el texto del Dictamen de la Ley de Delitos Informáticos nunca fue retirado aunque el propio Beingolea reconoció ante la prensa las carencias de su proyecto. Desde mediados de 2012, el Proyecto estuvo esperando su debate y a inicio de 2013 fue incluido en la agenda del pleno luego de sendas solicitudes de premura enviadas por escrito a la Mesa Directiva del Congreso de los congresistas Juan Carlos Eguren y Tomás Zamudio. En el ínterin, se presentaron otros proyectos que tratan delitos informáticos en específico o que están relacionados con el uso de la tecnología, incluyendo un proyecto integral elaborado por el Ministerio de Justicia y enviado al congreso con las firmas del Presidente de la República y el Primer Ministro.

3. Proyectos de ley posteriores

Luego del dictamen de la Comisión de Justicia, se presentaron cinco nuevos proyectos de ley que estaban relacionados con el tema de delitos informáticos. Estos proyectos también fueron decretados a la misma Comisión de Justicia, pero nunca llegaron a debatirse ni recibieron dictamen. Por el contrario, fueron directamente acumulados al dictamen anterior por el propio Juan Carlos Eguren el mismo día en el que se debatía en el Pleno del Congreso.

El primero de este grupo fue el Nº 1257/2011-CR, también presentado por Tomás Zamudio (Gana Perú) en junio de 2012. Este proyecto de ley pretendía agravar las sanciones para la interceptación de las comunicaciones, a la luz de los recientes escándalos de escuchas telefónicas en Perú. Sobre el punto, proponía introducir tres nuevos artículos en el Código Penal referidos a la inviolabilidad del secreto de las telecomunicaciones, la responsabilidad de la empresa de comunicaciones y penas para la tenencia ilegal de equipos de interceptación.

El segundo proyecto que no alcanzó a discutirse en comisión fue el Nº 2112/2012-CR presentado en abril de 2013 por Renzo Reggiardo (Concertación Democrática). Este proyecto estaba enfocado en reprimir el uso no autorizado de sistemas de telefonía y señales de cable, aunque también incluía un artículo sobre fraude informático.

Otros dos que tampoco alcanzaron a discutirse fueron el Proyecto de Ley Nº 2398/2012-CR presentado por Gustavo Rondón (Solidaridad Nacional) en junio de 2013 y el Nº 2482/2012-CR presentado por Julia Tévez (Gana Perú) en julio de 2013. Ambos proyectos de ley tenían un texto muy similar y proponían incluir como un nuevo tipo penal el delito informático de proposición con fines sexuales a menores a través de Internet (*grooming*).

Finalmente, el proyecto de ley más reciente del grupo fue el Nº 2520/2012-PE enviado directamente por el Poder Ejecutivo a fines de julio de 2013. Este proyecto de ley planteaba un texto alternativo llamado Ley de Represión de la Cibercriminalidad y propone incluir una serie de nuevos delitos y agravantes en nuestro Código Penal, para casos en los que se afecte la integridad de los sistemas informáticos o se use un sistema informático para cometer un delito. La primera mitad del proyecto se inspiraba en la controvertida Convención de Budapest, mientras la otra mitad del proyecto iba más allá del marco internacional, agregaba delitos completamente novedosos como *grooming* y modificaba otros artículos como los de discriminación. La versión que finalmente conocemos de la Ley de Delitos Informáticos es casi idéntica a este último proyecto de ley, pese a que no alcanzó a ser debatido ni dictaminado por ninguna Comisión antes de ser discutido en el Pleno.

4. Presiones externas

El otro antecedente directo de la Ley de Delitos Informáticos es la reunión de técnicos de la Conferencia de Ministros de Justicia de Iberoamérica (COMJIB), que se llevó a cabo en Lima a fines de junio. Este grupo de trabajo lleva discutiendo hace varios meses la necesidad de adoptar un marco común a los países de Iberoamérica para la persecución de delitos informáticos, inspirado en la Convención de Budapest. Se sabe que en la última reunión de Lima se avanzó sobre la redacción de un convenio sobre ciberdelincuencia para la región, que ha pasado a evaluación y espera ser firmado por todos los países antes de que termine el 2013.

5. Debate en el Pleno

Luego de más de un año de que el dictamen de la Ley de Delitos Informáticos que aprobó la Comisión de Justicia entrara a agenda, finalmente se discutió en el Pleno el 12 de setiembre de 2013. Fue una discusión por momentos desordenada y en la que apenas se mencionaron algunos de los problemas del dictamen que tanto se comentaron el año pasado. Durante el debate, un grupo de congresistas aprovecharon para mencionar que ellos también tenían sus propias leyes que tocaban delitos informáticos. Al final del debate, Juan Carlos Eguren, autor del primer proyecto de ley y actual presidente de la Comisión de Justicia, pidió un receso para tomar en cuenta las sugerencias de los demás congresistas. Eran las 11 a.m.

A las 4 p.m. se reanudó la sesión del Pleno y para esa hora el congresista Eguren anunció que ya tenía un nuevo texto. Un nuevo texto que, ahora sabemos, no se trataba de una modificación menor al dictamen materia de debate, sino que había reemplazado íntegramente al texto original. Eguren señaló que esta nueva versión de la Ley de Delitos Informáticos ya había sido revisada y consultada con los congresistas, e incluso con representantes del Poder Ejecutivo. Entonces, en un debate de unos pocos minutos se introdujeron un par de precisiones y el proyecto de ley quedó aprobado por el voto unánime de todos los congresistas presentes (por 79 votos a favor y ninguno en contra). Se le dispensó de segunda votación y el texto final de la ley solo se publicó en la página web del Congreso en los días posteriores. Hasta antes de ello, nadie, salvo los congresistas y sus asesores, tuvo acceso al texto.

Pese a que fue aprobado el 12 de setiembre, recién fue remitido al Poder Ejecutivo para su promulgación el 27 del mismo mes. El Presidente de la República, pese a todas las críticas y cartas que recibió durante esos días, terminó aprobando la Ley de Delitos Informáticos al borde del plazo que tenía legalmente para hacerlo. Así fue como el Congreso cambió radicalmente el texto de un dictamen para reemplazarlo por un proyecto de ley que no fue debatido en ninguna comisión y terminó convirtiéndolo en la Ley de Delitos Informáticos.

III. CINCO CAMBIOS A LA LEY Nº 30096

Esta propuesta no busca desnaturalizar la ley aprobada. Por el contrario, los cambios propuestos obedecen a tres objetivos: (i) lograr una mayor precisión en los tipos penales, en cumplimiento de la regla de "ley cierta" o taxatividad penal que es parte del principio de legalidad aplicable en materia penal; (ii) evitar que ciertos tipos penales penalicen el ejercicio regular de un derecho; y, (iii) evitar que ciertas conductas criminales tengan una pena mayor cuando se realicen usando la tecnología.

En esta línea, los cambios propuestos no se apartan del estándar internacional fijado por la Convención de Budapest y se sustentan en los propios documentos emitidos del Consejo de Europa, ente autor del Convenio.

1. Precisar la tipificación de los delitos contra la integridad de datos y sistemas informáticos (artículos 3 y 4)

En los ocho delitos contemplados en el Convenio de Budapest (artículos del 2 al 9 del mismo) se recomienda a los países firmantes delimitar los tipos penales a los casos en los que las conductas se llevan a cabo intencionalmente (*intentionally*) y sin derecho (*without right*). En el caso peruano, no resulta necesario establecer el requisito de intencionalidad porque la infracción culposa solo es punible en los casos expresamente establecidos

por ley[3]. Sin embargo, en el caso del requisito de actuar sin derecho o indebidamente, la Ley Nº 30096 solo ha seguido esta recomendación en su artículo 2 (acceso ilícito) y ha omitido hacerla para otros artículos como los artículos 3 y 4.

Por ende, debe otorgarse un tratamiento legislativo estándar a estos casos, añadiéndose el requisito de actuar sin autorización o "indebidamente" (siguiendo un término utilizado con frecuencia en nuestro Código Penal para los casos en los que se actúa sin autorización o fuera del amparo de un derecho). De lo contrario, podrían terminar entendiéndose como ilícitas una serie de actividades que involucran el procesamiento o la alteración de datos y corresponden al ejercicio regular de un derecho, al campo de la investigación académica, la informática recreativa o al ejercicio de una profesión, y que no necesariamente están cubiertas por el artículo 20 del Código Penal[4].

Además, conforme lo propone el propio Convenio de Budapest, es apropiado que se precise en el artículo 3 de la Ley que solo se incurrirá en este delito cuando se ocasionen daños que puedan calificarse como graves. Es necesario acoger esta recomendación del Convenio con la finalidad de respetar la condición de última ratio del Derecho Penal y aplicarlo solo a los casos que ocasionen un daño grave para la sociedad. Cabe precisar, además, que efectuar esta precisión a dicha regla no afectará la posibilidad de que quien se sienta dañado pueda recurrir a la vía civil para buscar reparación por los daños generados.

Redacción actual	Redacción propuesta
Artículo 3.- Atentado contra la integridad de datos informáticos El que, a través de las tecnologías de la información o de la comunicación, 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.	Artículo 3.- Atentado contra la integridad de datos informáticos El que, a través de las tecnologías de la información o de la comunicación, *indebidamente* introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, *siempre que cause un daño grave* será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.
Redacción actual	**Redacción propuesta**
Artículo 4.- Atentado contra la integridad de sistemas informáticos El que, a través de las tecnologías de la información o de la comunicación, 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.	Artículo 4.- Atentado contra la integridad de sistemas informáticos El que, a través de las tecnologías de la información o de la comunicación, *indebidamente* inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios *siempre que cause un daño grave*, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

3 Código Penal
Artículo 12.- "Las penas establecidas por la ley se aplican siempre al agente de infracción dolosa. El agente de infracción culposa es punible en los casos expresamente establecidos por la ley".

4 Sobre la validez de remitirse a los excluyentes de responsabilidad penal del artículo 20 del Código Penal, resulta sintomático que la propia Ley de Delitos Informáticos incluya un artículo que autoriza a la Policía a almacenar pornografía infantil en sus servidores cuando también podría entenderse que ese comportamiento está exceptuado de responsabilidad en los términos del artículo 20.

2. Precisar los alcances del delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (artículo 5)

El delito de proposiciones a niños, niñas y adolescentes por medios tecnológicos es de muy reciente concepción en el mundo. En virtud de este artículo, se penaliza a quien contacta a un menor de catorce años para: (i) solicitar u obtener de él material pornográfico, o (ii) llevar a cabo actividades sexuales con él. Esta práctica (también denominada *grooming*) está regulada en muy pocos países en el mundo y su tipificación y aplicación ha sido muy polémica.

La principal objeción a esta figura es que penaliza el mero contacto con un menor, sin necesidad de que se lleve a cabo ninguna acción posterior. Esto, en principio, plantea el problema de penalizar un acto preparatorio en sí mismo. Además, también resulta muy difícil de fiscalizar y probar ya que para acreditar el "contacto" tendría que recurrirse a la interceptación de las comunicaciones del presunto infractor.

Hace unos meses, en Argentina se debatió un proyecto de ley muy similar que fue duramente criticado por organizaciones como la Asociación por los Derechos Civiles, porque consideraban que tenía "numerosos problemas de compatibilidad con los principios esenciales que deben regir una legislación penal respetuosa de las garantías constitucionales"[5].

Si es que se ha tomado la decisión política de incluir un delito de este tipo en nuestra legislación, nuestra recomendación es precisar sus alcances con la finalidad de que fiscales y jueces puedan reconocerlo e individualizarlo adecuadamente respecto de otros delitos.

En ese sentido, la Convención sobre Explotación Infantil del Consejo de Europa[6] propone penalizar el delito de *solicitation of children for sexual purposes* siempre y cuando la propuesta esté seguida de actos materiales que conduzcan a concretar el encuentro (*where this proposal has been followed by material acts leading to such a meeting*). Por ende, creo necesario modificar la redacción actual del artículo 5 de la Ley Nº 30096 con la finalidad de que lo que se penalice sean los actos mismos de proposición y no el mero contacto o la tentativa.

Redacción actual	Redacción propuesta
Artículo 5.- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	Artículo 5.- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos
El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.	El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años y solicita u obtiene de él material pornográfico, o le propone llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.
Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.	Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

5 RABINOVICH, Eleonora. "Los problemas del proyecto de ley sobre *grooming* en Argentina". En: *Digital Rights Latin America & The Caribbean*. Nº 1. Disponible en: <http://www.digitalrightslac.net/es/los-problemas-del-proyecto-de-ley-sobre-grooming-en-argentina/>, consultado el 12 de noviembre de 2013.

6 CONSEJO DE EUROPA. *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*. Disponible en: <http://www.conventions.coe.int/Treaty/EN/treaties/Html/201.htm>, consultado el 25 de octubre de 2007.

Adicionalmente, debe de analizarse la posibilidad de modificar los delitos de seducción (artículo 175) y de actos contra el pudor en menores (artículo 176-A) del Código Penal con la finalidad de que sus penas sean consistentes a las del delito de proposiciones con fines sexuales por medios tecnológicos. No debe permitirse que cualquier acoso a una niña, niño o adolescente realizado en persona tenga una pena menor que los casos cuando este acoso se lleve a cabo a través de medios tecnológicos.

3. Mejorar la redacción del delito de tráfico de datos para penalizar exclusivamente el tráfico (artículo 6)

La actual redacción del artículo 6 de la Ley es demasiado amplia, al punto que comprende cualquier uso de bases de datos. Se entiende que el objetivo del artículo, como lo anuncia su sumilla, es reprimir aquellas conductas que involucren el traspaso de bases de datos de información personal sin autorización. Por ello, sugiero una redacción que esté directamente orientada a reprimir las conductas que constituyen tráfico en sí mismo y no cualquier uso de una base de datos. Además, el criterio de cuándo el uso de datos personales es debido o indebido debe de estar directamente vinculado con lo dispuesto por la Ley de Protección de Datos Personales y su Reglamento por ser más detallada y tomar en cuenta las particularidades del problema.

4. Eliminar los agravantes para los delitos de interceptación telefónica y de datos que no son parte del Convenio de Budapest (artículos 7 y 162 del Código Penal)

Con la finalidad de incluir el delito de interceptación de datos, se ha estandarizado su redacción respecto del delito ya existente de interceptación telefónica. Sin embargo, encuentro innecesaria la consignación de los dos grupos de agravante que se añaden. En principio, porque no son parte del texto de la Convención de Budapest y su consignación nos aleja de ese estándar y de lo planteado por el propio Ministerio de Justicia.

En el caso de la información que compromete la defensa, la seguridad o la soberanía nacionales, creo que esos escenarios ya están cubiertos por el delito de espionaje cuyas penas son de hasta quince (15) años[7]. En los casos en los que la interceptación se recaiga sobre información clasificada, creo que los fueros penales no son un escenario adecuado para que se interprete la Ley de Transparencia y Acceso a la Información Pública. Estos tipos de evaluaciones regularmente son materia

Redacción actual	Redacción propuesta
Artículo 6.- Tráfico ilegal de datos El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.	Artículo 6.- Tráfico ilegal de datos El que *comercializa, trafica o vende* una base de datos sobre una persona natural o jurídica, identificada o identificable *en incumplimiento de lo previsto por la Ley de Protección de Datos Personales* será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

7 Código Penal
Artículo 331.- "El que espía para comunicar o comunica o hace accesibles a un Estado extranjero o al público, hechos, disposiciones u objetos mantenidos en secreto por interesar a la defensa nacional, será reprimido con pena privativa de libertad no menor de quince años.
Si el agente obró por culpa la pena será no mayor de cinco años".

incluso de procesos de hábeas data dada la complejidad existente en determinar si ciertas informaciones (como informes oficiales o estudios previos a la dación de una norma) tienen o no un interés público que merezca su publicidad. Por ende, creo que ambos grupos de agravantes deben de ser omitidos de los tipos penales de interceptación.

Redacción actual	Redacción propuesta
Artículo 7.- Interceptación de datos informáticos. El que, a través de las tecnologías de la información o de la comunicación, intercepta 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, será reprimido con 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 las normas de la materia. La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.	Artículo 7.- Interceptación de datos informáticos. El que, a través de las tecnologías de la información o de la comunicación, intercepta 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, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
Redacción actual	**Redacción propuesta**
Artículo 162. Interferencia telefónica El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años. Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4. 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 las normas de la materia. La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.	Artículo 162. Interferencia telefónica El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años. Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

5. Eliminar el agravante por uso de tecnologías de la información del delito de discriminación (artículo 323 del Código Penal)

El delito de discriminación ha tenido una historia compleja en nuestro país. Un informe reciente de la Defensoría del Pueblo señala que entre el 2009 y el 2012 solo se han conocido diecinueve (19) procesos por discriminación en el Poder Judicial, de los cuales doce siguen en proceso, cuatro se archivaron y tres tuvieron sentencia[8]. Regularmente,

8 DEFENSORÍA DEL PUEBLO. *Lucha contra la discriminación: avances y desafíos*. Serie Informes de Adjuntía- Informe Nº 008-2013-DP/ADHPD, Defensoría del Pueblo, Lima, 2013. Disponible en: <http://www.defensoria.gob.pe/modules/Downloads/informes/varios/2013/informe-008-2013-DP-ADHPD.pdf>, consultado el 12 de noviembre de 2013.

el Ministerio Público ha aplicado este delito a acciones discriminatorias como la negativa de ingreso a determinado lugar o el acceso a cierta condición.

Ampliar este delito a los casos en los que se lleva a cabo a través de tecnologías de la información o comunicación conforme lo hace la ley resulta problemático porque significa reconocer que es posible castigar el ejercicio regular de la libertad de expresión. Así, un artículo político podría entenderse como una discriminación "política" o una opinión en contra de la unión civil podría denunciarse como una discriminación "por género". Creo que el delito de discriminación debe de dejarse conforme a su redacción anterior y seguir orientado a actos discriminatorios y no a expresiones. Para todos los demás casos, existen soluciones civiles y hasta penales (vía difamación) que pueden utilizar quienes se sientan afectados por un contenido difundido a través de las tecnologías de la información y las comunicaciones.

Esta interpretación es consistente con el Protocolo Adicional a la Convención sobre Cibercrimen de Budapest del Consejo de Europa Nº 189 (CETS 189), sobre la criminalización de actos de racismo y de naturaleza xenófoba cometidos a través de sistemas informáticos[9]. En particular, este Protocolo circunscribe la posibilidad de que los Estados partes criminalicen la discriminación exclusivamente a casos relacionados con raza, color, descendencia u origen étnico. Al mismo tiempo, señala claramente que las partes podrían reservarse el derecho de no criminalizar la distribución de material discriminatorio si es que no promueve el ejercicio del odio o la violencia y si es que ello significaría entrar en conflicto con el ámbito de protección del derecho a la libertad de expresión conforme a su sistema de derechos humanos[10].

Redacción actual	Redacción propuesta
Artículo 323.- Discriminación El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas. Si el agente es funcionario o servidor público, la pena será no menor de dos ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36. La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación se ha materializado mediante actos de violencia física o mental, o si se realiza a través de las tecnologías de la información o de la comunicación.	Artículo 323.- Discriminación El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas. Si el agente es funcionario o servidor público, la pena será no menor de dos ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.

9 CONSEJO DE EUROPA. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. Disponible en: <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>, consultado el 28 de enero de 2003.

10 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Article 3.- "Dissemination of racist and xenophobic material through computer systems

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

CONCLUSIONES

La tarea de hacer normas implica buscar soluciones a problemas complejos. Existen soluciones legales muy específicas que responden a problemas concretos o épocas particulares, como las leyes que regulan el hallazgo de tesoros o la tenencia de animales para transporte. Por otro lado, existen otras que han perdurado con el paso del tiempo como muchas instituciones de los derechos reales que existen desde el Derecho Romano (v. gr. la prescripción adquisitiva de dominio). Hay también en estas últimas un sentido de atemporalidad impuesto por sus creadores que las hace tan vigentes hoy como lo eran hace dos mil años.

Creo que la regulación de mercados tan dinámicos como los sustentados en tecnologías, en la medida de lo posible, debe de también tener una visión de futuro. Esta es una tarea muy difícil porque no podemos predecir el futuro. En algunos mercados se pueden identificar tendencias o limitaciones naturales que nos pueden dar una pista de cómo van a evolucionar. En el caso de la tecnología y la Internet en particular, todas las predicciones se agotan en un horizonte de tres o cuatro años. Por ello, resulta imposible que hagamos una regulación capaz de resolver todos los problemas que pueden surgir en el futuro. Sin embargo, sí podemos optar por hacer una regulación que no termine deteniendo la llegada del futuro o alterándolo. Desde mi punto de vista, una regulación "a prueba del futuro" para mercados dinámicos debe de ser clara en sus objetivos, precisa en sus herramientas y estar orientada a permitir la diversidad de ofertantes, de ofertas, de modelos de negocio y de mercados. En contextos como el peruano, donde existen grandes brechas de infraestructura y de alfabetización digital, resulta importantísimo imponer una regulación que facilite el crecimiento del mercado y no lo detenga.

Por eso, al regular delitos informáticos, considero que existen tres ideas que no podemos dejar de tomar en cuenta:

- Nunca vamos a poder ponernos en todos los casos. No podemos esperar que las leyes penales describan con lujo de detalles los procedimientos, circunstancias o herramientas que se llevan a cabo para cometer un delito para recién perseguirlo. El principio de legalidad penal existe pero no puede llevarnos a regular tecnologías en sí mismas, que están sujetas a un cambio constante.
- No podemos penalizar el ejercicio regular de un derecho. Es un principio que está en nuestro propio Código Penal, pero a veces lo olvidamos. Acceder a información pública, escribir un comentario en una red social o en una página web, desarmar un aparato o un programa de computación para ver cómo funciona o usar recreativamente la tecnología son distintos aspectos del ejercicio de nuestros derechos. De la misma manera en la que todos estamos de acuerdo en que se termine la violencia familiar, pero no estaríamos de acuerdo con instalar cámaras dentro de todos los hogares del país. El interés por contar con mejores herramientas para combatir la criminalidad no puede terminar quitándonos nuestras libertades fundamentales a la libre expresión, la privacidad y el acceso a la cultura y el conocimiento.
- Las leyes son una parte de la solución. A menudo, son la parte más pequeña. Si Perú es el "paraíso de la ciberdelincuencia" como repiten los fabricantes de antivirus y tenemos leyes sobre delitos informáticos desde el año 2000, hay una pieza que falta. Como en tantos otros casos, combatir la delincuencia informática también significa preocuparnos por tener fiscales y jueces más preparados, incluso a través de la creación de instancias especiales, que puedan identificar y hacer frente a estos casos.

2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2".