Congreso de la República

Proyecto de Ley N° 3105/2013-CR

CONGRESO DE LA REPUBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
18 DIC. 2013
RECIBIDO
Firma: Hora: 12:36 p.m.

PROYECTO DE LEY QUE MODIFICA LA LEY N° 30096, LEY DE DELITOS INFORMÁTICOS.

Los Congresistas de la República que suscriben, integrantes del Grupo Parlamentario Perú Posible, ejerciendo su derecho funcional de presentar propuestas de ley que le confiere el artículo 107° de la Constitución Política, concordado con lo establecido en el artículo 76° del Reglamente del Congreso de la República; y a iniciativa de la Congresista CARMEN OMONTE DURAND, presentan el siguiente Proyecto:

1. EXPOSICIÓN DE MOTIVOS.

La globalización y las transformaciones económicas que la explican han hecho posible la aparición, desarrollo y masificación de las nuevas tecnologías de la información. Paralelamente, el desarrollo tecnológico ha traído de la mano nuevas formas delictuales que tienen por medio o finalidad los sistemas informáticos e Internet. Las peculiaridades de estos nuevos tipos exigen un tratamiento conjunto y coherente, y del mismo modo, su problemática particular involucra a elementos transnacionales, lo que obliga a la utilización de la cooperación internacional para la adopción de medidas globales. Mediante esta técnica es posible lograr una armonización del Derecho sustantivo, así como en el ámbito procesal, que redunda definitivamente en un alivio de la singular incertidumbre que rodea los tipos ciberdelictuales. Para lograrlo, la cooperación internacional, que se materializa principalmente a través de convenios internacionales, deberá reunir unos requisitos mínimos cualitativos. El Convenio sobre la Cibercriminalidad del Consejo de Europa se presenta como la solución internacional existente para el tratamiento de la cuestión ciberdelictual, convirtiéndose en una adecuada herramienta para la armonización legislativa interestatal y la lucha contra el ciberdelito.

Ahora, técnicamente, se consideran Tecnologías de la Información y Comunicación tanto al conjunto de herramientas relacionadas con la transmisión, procesamiento y almacenamiento digitalizado de información, como al conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software)[1]. Se trata de instrumentos que

[1] http://www.recursoseees.uji.es/fichas/fc10.pdf

nos permiten estar informados prácticamente al instante de lo que ocurre en el mundo, comunicarnos en menos de un segundo con cualquier persona de la tierra.

Dichas tecnologías aparecen plasmadas en distintos soportes físicos que todos conocemos, como son el teléfono –fijo y móvil-, el ordenador, la televisión, etc. Todos ellos continúan desarrollándose y evolucionando día a día, llegando incluso a mezclarse, y apareciendo híbridos de éstos. Como sabemos, es gracias a dispositivos como los enunciados que pueden crearse las redes, que son un conjunto de equipos informáticos conectados entre sí que pueden intercambiar información[2].

Ahora, la especificidad de Internet como medio de comunicación ha originado lo que es conocido como "ciberdelincuencia". Por su singularidad con respecto a la delincuencia tradicional, este fenómeno exige una consideración especial por parte del Derecho Penal, puesto que la mayor parte de los métodos clásicos, como se advertirá, no sirven.

Cometer delitos informáticos es mucho más sencillo de lo que pudiera parecer. En primer lugar requieren escasos recursos por parte del delincuente (apenas un ordenador conectado a la Red) y pueden cometerse desde cualquier lugar del mundo. Pero además, puede ser extremadamente sencillo hacerlo, hasta el punto que una persona con escasos conocimientos de informática sería hipotéticamente capaz de lograrlo, diferenciando entre los distintos tipos delictivos, puesto que las grandes estafas informáticas o la creación de complejos programas destructores no pueden ser llevadas a cabo por personas con limitado conocimiento de sistemas informáticos. Sin embargo, existen otros delitos, aparentemente simples, que sí admiten su comisión por cuasi-ignaros informáticos. Así, a modo de ejemplo, es posible enviar virus creados por otros (con relativa facilidad) o sabotear programas informáticos mediante cracks, generadores de claves o similares que se encuentran en la World Wide Web sin demasiada dificultad[3].

---

[2] REAL ACADEMIA ESPAÑOLA, Diccionario de la Lengua Española, Espasa Calpe, Madrid, 2001 (22° edición).

[3] El envío de "virus", si produce daños. Por otro lado, un crack es un programa utilizado para alterar el software original sin el consentimiento del propietario. Ello permite, entre otras cosas, la copia de programas, el acceso y la utilización de éstos sin necesidad de adquirirlos o la eliminación de las restricciones establecidas por los fabricantes. La facilidad de comisión es increíble y se trata de una práctica muy extendida entre los usuarios de Internet y las nuevas tecnologías.

Ello pone de manifiesto, una vez más, las insólitas dimensiones que presentan los nuevos delitos, que juegan en un ámbito que invita a la comisión de ilícitos.

Teniendo en cuenta lo dicho, la novedad y el dinamismo de la nueva sociedad de la información, y la necesidad de proteger a las personas de nuevas conductas perniciosas a través de la Red, es indudable que el Derecho Penal está experimentando una nueva expansión. De hecho, cualquier propuesta de solución de problemas, cualquier intento de mejora de las legislaciones, pasa inevitablemente por una ampliación de las conductas delictivas. Ésta parece ser la única alternativa a la protección de los bienes jurídicos que se vulneran en las distintas modalidades de delitos informáticos.

El expansionismo del Derecho Penal es un fenómeno global que ha penetrado forzosamente en todos los países y en la mayoría de las jurisdicciones penales[4]. Pero en el ámbito informático quizás se agrava y se hace necesario, dada la aparición de modernos bienes jurídicos y del surgimiento de nuevos riesgos. Así el Convenio de Budapest, es un buen ejemplo de esta tendencia. Sin embargo, se debe tener cuidado con el incremento desproporcionado de los tipos delictivos; siempre hay que tener en mente el carácter subsidiario y el esencial principio de *ultima ratio* del Derecho Penal. De este modo debemos preguntarnos a la hora de incriminar una nueva conducta si es realmente necesario, o si no bastaría una regulación administrativa o civil que estableciera su desvalor.

No hace falta decir que el Derecho Penal sólo debería utilizarse en los ataques más importantes. Y nos consta, sin ánimo de especificar, que algunos de los delitos informáticos presentes en las diferentes legislaciones no responden en absoluto a estos principios. Por ello, algunos autores advierten que se corre el peligro de ir hacia un Derecho Penal del Enemigo en materia de delincuencia informática. Vale decir que la tendencia preferible es la reducción progresiva de la presencia punitiva, pues definitivamente no toda conducta irregular relacionada con la informática ha de incluirse en el ámbito penal.

[4] MORILLAS CUEVA, LORENZO, "Nuevas tendencias del Derecho Penal: Una reflexión dirigida a la cibercriminalidad", en Cuadernos de Política Criminal, N° 94, 2008, págs. 18 ss.

En definitiva, es innegable que hay un punitivismo ampliamente desarrollado en relación con la cibercriminalidad, pero también debemos tener en cuenta que estamos ante uno de los temas más necesitados de protección penal. Será necesario equilibrar la balanza introduciendo los principios garantistas propios del Estado Social y Democrático de Derecho.

Lo cierto es que tanto en materia de Derecho Informático como de cooperación internacional en general, la legislación europea se presenta como adalid indiscutible de las nuevas formas de colaboración entre Estados.

Llamamos informalmente "Convenio de Budapest" al Convenio sobre la Cibercriminalidad hecho en Budapest, en el seno del Consejo de Europa[5]. Este convenio supone en cierto modo la plasmación positivizada de muchas de las ideas aquí vertidas, la mayor maximización de la cooperación en materia de delitos informáticos existente hoy en día en el plano internacional. En efecto, se trata del primer y único instrumento internacional existente hasta la fecha en esta materia con auténtica importancia.

Es en relación a todo lo anteriormente definido que el presente Proyecto de Ley tiene por finalidad modificar la ya promulgada Ley N° 30096, Ley de Delitos Informáticos, incluyendo agravantes y supuestos de exclusión de responsabilidad; así como supuestos de hecho y elementos en los distintos tipos penales; a fin de adicionarle ciertos criterios tomados en cuenta en el Convenio de Budapest, dada la tendencia irrefrenable que muestra la tecnología y el gran acogimiento por parte de la población de las nuevas TIC's.

Así, la aparición de nuevos dispositivos con acceso a la Red, la reducción de la brecha digital y el imparable crecimiento de Internet son hechos irrebatibles. El aumento del número de delitos informáticos, como se dijo al principio, también. Así las cosas, se pretenden normas que tengan por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos

[5] Convenio sobre la Cibercriminalidad de 23 de noviembre de 2001 del Consejo de Europa.

cometidos en las variedades existentes contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías.

2. ANÁLISIS COSTO – BENEFICIO

Se destaca que las modificaciones contenidas en el presente Proyecto no originan gasto alguno al erario nacional, contrariamente, al cumplirse dicha normatividad, el perjuicio económico, tanto de la sociedad como del Estado, se verían reducidas.

3. EFECTO DE LA PROPUESTA SOBRE LA LEGISLACIÓN NACIONAL

De aprobarse el presente Proyecto de Ley, los artículos 3°, 5°, 7° y 10° de la Ley N° 30096, Ley de Delitos Informáticos, serían modificados, incluyendo agravantes y supuestos de exclusión de responsabilidad; así como supuestos de hecho y elementos en distintos tipos penales.

Por otro lado, también se modifica la Cuarta Disposición Complementaria Final de la citada Ley, en tanto se incluyen dependencias estatales especializadas en temas de teleinformática, informática y electrónica, tales como la Pe-CERT (Coordinación de Emergencias en redes Teleinformáticas, dependencia de la PCM) y la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática, dependencia de la PCM) a fin de que se lleva una mejor cooperación en mira a los fines que dicha Disposición persigue.

Finalmente, la Cuarta Disposición Complementaria Modificatoria de la Ley, se vería variada en lo que concierne al delito tipificado en el artículo 162° del Código Penal, referido a la Interceptación Telefónica, modificando el elemento normativo a valorar.

4. VINCULACIÓN DE LA NORMA CON EL ACUERDO NACIONAL

La propuesta legal tiene vinculación con el Acuerdo Nacional, particularmente con la I Política de Estado correspondiente a "Democracia y Estado de Derecho"; en específico con la matriz 7) perteneciente a la Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana; la misma que encuentra como parte de sus objetivos, consolidar políticas orientadas a prevenir, disuadir, sancionar y eliminar aquellas conductas y prácticas sociales que ponen en peligro la tranquilidad, integridad o libertad de las personas; asimismo, propiciar una cultura cívica de respeto a la ley y a las normas

de convivencia, sensibilizando a la ciudadanía contra la violencia y generando un marco de estabilidad social que afiance los derechos y deberes de los peruanos, poniendo especial énfasis en extender los mecanismos legales para combatir prácticas violentas arraigadas, como son el maltrato familiar y la violación contra la integridad física y mental de niños, ancianos y mujeres, garantizando su presencia efectiva en las zonas vulnerables a la violencia, fomentando una cultura de paz a través de una educación y una ética públicas que incidan en el respeto irrestricto de los derechos humanos.

5. FÓRMULA LEGAL

EL CONGRESO DE LA REPÚBLICA:
HA DADO LA LEY SIGUIENTE:

LEY QUE MODIFICA LA LEY N° 30096, LEY DE DELITOS INFORMÁTICOS

Artículo 1.- Modifíquense los artículos 3, 7 y 10 de la Ley N° 30096, Ley de Delitos Informáticos, los que quedaran redactados de la siguiente manera:

Artículo 3.- Atentado a la integridad de datos informáticos

*El que, **de manera ilegítima**, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, **daña**, 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 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, 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 una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de la 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 cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Artículo 10.- Abuso de mecanismos y dispositivos informáticos

El que 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.

No son reprimibles la producción, venta, obtención para la utilización, importación, difusión o cualquiera otra forma de puesta a disposición mencionada en el presente artículo que no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos de la presente Ley, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

Artículo 2.- Modifíquese la Cuarta Disposición Complementaria Final de la Ley N° 30096, Ley de Delitos Informáticos, la misma que quedara redactada de la siguiente manera:

CUARTA.- Cooperación operativa

Con el objeto de garantizar el intercambio de información, equipos de investigación conjuntos, transmisión de documentos, interceptación de comunicaciones, y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Publico, Poder Judicial, ***Pe-CERT, ONGEI*** *y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reforzada en el plazo de treinta días desde la vigencia de la presente Ley.*

Artículo 3.- Modifíquese la Cuarta Disposición Complementaria Modificatoria de la Ley N° 30096, Ley de Delitos Informáticos, la misma que quedara redactada de la siguiente manera:

CUARTA.- Modificación de los artículos 162, 183-A y 323 del Código Penal

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, seguridad o soberanía nacionales.

Está exento de responsabilidad penal, quien difunde comunicaciones privadas con el propósito de proteger un interés público, siempre y cuando no haya tenido intervención en la obtención de dichas comunicaciones.

Lima, 18 de Diciembre del 2013

JOSÉ LEÓN RIVERA
Directivo Portavoz
Grupo Parlamentario Perú Posible

CARMEN OMONTE DURAND
CONGRESISTA DE LA REPÚBLICA

CONGRESO DE LA REPÚBLICA

Lima, 19 de diciembre del 2013

Según la consulta realizada, de conformidad con el Artículo 77° del Reglamento del Congreso de la República: pase la Proposición N° 3105 para su estudio y dictamen, a la (s) Comisión (es) Justicia y Derechos Humanos.

JAVIER ANGELES ILLMANN
Oficial Mayor(e)
CONGRESO DE LA REPÚBLICA