

“Ley de Regulación de Programación de Espionaje Cibernético”

Ley Núm. 165 de 6 de agosto de 2008

Para establecer la “Ley de Regulación de Programación de Espionaje Cibernético” (“Spyware”); tipificar como delito conducta constitutiva de espionaje; establecer penas; y para otros fines.

EXPOSICION DE MOTIVOS

No obstante los avances significativos que representa el nuevo Código Penal, adoptado mediante la [Ley Núm. 149 de 18 de junio de 2004](#), la realidad es que todavía quedan áreas de la conducta humana no reguladas o tipificadas en el mismo y cuyas conductas pueden lacerar y afectar derechos sustanciales de los ciudadanos.

Esta Asamblea Legislativa debe tomar acciones afirmativas y decididas para identificar estas áreas de la conducta humana y establecer medidas de diferente clase y enfoque para evitar que se perpetúe dicha conducta que tanto daño causa a los ciudadanos. Una de las áreas que mayor reto presenta a las autoridades para regular la conducta es la industria de las computadoras y la red de “Internet”. Con el desarrollo del computador en un artículo necesario y un bien de consumo, las ventas de computadoras personales se han multiplicado exponencialmente. Los dueños de computadoras con acceso a “Internet” cada vez es más alto y abarca casi todos los sectores socioeconómicos.

Al convertirse en un bien de consumo y al establecerse como mecanismo de trabajo, estudio y comunicación, las computadoras se han convertido en depósito esencial de gran parte de la información personal confidencial e íntima de los ciudadanos. En ellas se guarda información económica, crediticia, educativa, médica y personal. Toda esta información está disponible para ser obtenida por personas inescrupulosas que, valiéndose de mecanismos y programas cibernéticos, pueden acceder, sin permiso del dueño de la computadora, los archivos y demás contenido de la misma.

Para lograr tales fines, se han diseñado programas de espionaje cibernético llamados “Computer Spyware”, que permiten a su instalador acceder una computadora, tomar control de la misma, retirar información o simplemente, espiar lo que el dueño de la computadora realiza en la misma. Como resultado de la amplia distribución de estos programas, un estudio en los Estados Unidos de las firmas “America Online” (“AOL”, por sus siglas en inglés) y “National Cyber Security Alliance”, reflejó que para octubre de 2004 un ochenta por ciento de las computadoras personales evaluadas estaban infectadas por “Spyware” y 88% de los usuarios afectados desconocían que sus equipos estaban infectados.

Como resultado de éste y otros estudios, diversos gobiernos estatales, al igual que el gobierno federal, se han dado a la tarea de intentar regular y detener la práctica de infectar los equipos de computadoras con este tipo de programación. En el año 2004, el estado de California fue de los primeros en establecer legislación para proteger a ciudadanos de este tipo de programación con el “Consumer Protection Against Computer Spyware Act”. Dicha Ley prohibió la instalación a sabiendas de programación en una computadora ajena al programador para: tomar

control del ordenador; modificar ciertos controles relacionados al acceso o uso de la “Internet” en el ordenador; obtener a través de una interceptación de la computadora u ordenador, información personal del usuario; prevenir los intentos del usuario autorizado a desactivar o intervenir con la programación de “Spyware”; lograr interferir con la computadora u ordenador para que refleje que se eliminó el programa sin que ello sea cierto; e, intencionalmente lograr inhabilitar programación antiespionaje electrónico, anti-virus o cualquier otra similar en el ordenador. La Ley estableció penalidades y creó una causa de acción particular para cualquier persona afectada por espionaje en la computadora u ordenador.

Actualmente Arizona, Arkansas, Iowa, Georgia, Utah, Virginia y Washington han adoptado legislación similar. Además, aunque al presente el Congreso Federal no ha aprobado legislación sobre el particular ha considerado varias medidas dirigidas a regular este tipo de programación. Por ejemplo, el H.R. 29, conocido como “The Spy Act”, prohibiría prácticas injustas y engañosas relacionadas a la programación conocida como “Spyware”. También, el H.R. 744, conocido como “Spyware Prevention Act of 2005”, criminalizaría el acceso intencional no autorizado a una computadora u ordenador, entre otras medidas que dispone para controlar la proliferación de la penetración no autorizada en las computadoras u ordenadores.

Decrétase por la Asamblea Legislativa de Puerto Rico:

Artículo 1. — Título. (10 L.P.R.A. § 218)

Esta Ley se conocerá como “Ley de Regulación de Programación de Espionaje Cibernético”, (“Spyware”).

Artículo 2. — Declaración de Política Pública. (10 L.P.R.A. § 2181 nota)

La Política Pública del Estado Libre Asociado de Puerto Rico es proteger a los consumidores del uso y abuso de la programación cibernética conocida como “Spyware” (en el idioma inglés) y de cualquier subterfugio electrónico que permita a un tercero el acceder sin autorización la información contenida en un programador que no le pertenece.

Artículo 3. — Definiciones. (10 L.P.R.A. § 2181)

A los fines de esta Ley, los siguientes términos tendrán el siguiente significado:

(a) **Anuncio** — significa cualquier comunicación, cuyo fin primordial es el promover comercialmente un producto comercial o servicio, incluyendo el contenido de un portal en la “Internet” a estos fines.

(b) **Computadora** — significa cualquier computadora, ordenador, servidor de computadora o dispositivo electrónico, como por ejemplo, celulares y teléfonos móviles, asistentes personales digitales, juegos de video que acceden al “Internet”; y dispositivos que coleccionan información biométrica, como lectores de retina y huellas digitales.

(c) **Consentimiento Informado** — significa el consentimiento prestado por una persona a quien se le ha avisado de manera clara, concisa, conspicua y no ambigua que se está instalando o

ejecutando un programa en su computadora, así como un aviso de su función y efectos. Además, deberá informársele de la forma que dicho producto puede ser removido de su computadora.

(d) Daño — significa cualquier impedimento o efecto adverso sobre la integridad del ordenador, la programación del ordenador, su sistema operativo o la información que contiene el ordenador.

(e) Persona — significa todo individuo, sociedad, corporación o cualquier otro tipo de organización con capacidad jurídica.

(f) Programa — significa una secuencia de instrucciones escritas en cualquier lenguaje de programación que es ejecutado en un ordenador.

(g) “Spyware” o Programa de Espionaje Cibernético — cualquier programa que:

i. corra o ejecute funciones en una computadora sin el consentimiento informado del dueño o usuario autorizado de la computadora; y

ii. obtenga o utilice, de cualquier manera, cualquier información que esté en tal computadora, o información que sea obtenida o provista por tal computadora a cualquier otra computadora, servidor de computadoras o dispositivo electrónico, a través de cualquier tipo de comunicación.

Esta definición no incluye las funciones de investigación del estado que se realizan conforme a la Constitución del Estado Libre Asociado de Puerto Rico y de los Estados Unidos de América, y las leyes y reglamentación estatales y federales.

(h) Usuario Autorizado — significa cualquier persona que sea dueño o esté autorizado por el dueño o arrendador del ordenador para su uso.

(i) Virus — significa cualquier programa o secuencia de instrucciones que está diseñado para degradar el funcionamiento del ordenador o para inhabilitar el ordenador o la red de ordenadores, que está diseñado de forma que se reproduce espontáneamente en los ordenadores o redes de ordenadores sin autorización del dueño o usuario autorizado.

Artículo 4. — Información Personal Confidencial. (10 L.P.R.A. § 2182)

A los efectos de esta Ley, se considerará información confidencial personal toda aquella que se encuentre en una computadora u ordenador o redes de computadoras u ordenadores, según a continuación se expresa:

(a) Nombres, apellidos e iniciales de cualquier persona.

(b) Números de tarjetas de débito o crédito.

(c) Cualquier código secreto que se utilice para acceder la información detallada en este Artículo o para acceder información financiera.

(d) Números de Seguro Social.

(e) Balances bancarios, de crédito, historial de pagos a instituciones financieras, información sobre sobregiros o cheques sin fondos.

(f) Historial de páginas visitadas en la “Internet”.

(g) Historial de compras en la Internet.

(h) Direcciones postales o físicas.

(i) Expedientes médicos.

(j) Expedientes académicos.

Artículo 5. — Conducta Prohibida. (10 L.P.R.A. § 2183)

Se prohíbe el uso o instalación de “Spyware” en una computadora, para cualquier propósito, a no ser que medie el consentimiento informado y expreso del dueño o usuario autorizado de ésta.

El uso prohibido de Spyware o Programación de Espionaje Cibernético incluye, pero no se limita a:

(a) Modificar, a través de cualquier forma de engaño o treta cualesquiera de las funciones de la computadora u ordenador, incluyendo, pero no limitado acceso a la computadora u ordenador, la página cibernética donde la computadora u ordenador activa su sistema de navegación en la Internet y las marcas o “bookmarks” que el usuario autorizado o dueño han registrado en la computadora u ordenador.

(b) Recolectar, a través del uso de cualquier forma de engaño o treta, información personal confidencial del usuario autorizado o dueño, incluyendo cuando dicha acción se realiza a través de uso de un dispositivo que graba todos los usos del teclado de un usuario autorizado y transfiere tal información a otro ordenador o persona; cuando dicha acción se realiza a través de acceder sin autorización el historial de páginas de la “Internet” visitadas por el usuario autorizado y cuando dicha acción se realiza extrayendo del disco duro del ordenador información sin la autorización expresa del usuario autorizado o dueño.

(c) Prevenir, a través del uso de cualquier forma de treta o engaño, el que un usuario autorizado pueda detectar que su ordenador ha sido intervenido, se le ha insertado programación o se ha sustraído información sin su autorización.

(d) Representar, intencionalmente, de forma electrónica, que la computadora u ordenador ha eliminado un programa de espionaje cibernético o un virus, a sabiendas que dicha información es falsa.

(e) Intencionalmente o a través de treta o engaño lograr inutilizar el sistema de seguridad, anti-espionaje cibernético o antivirus en una computadora.

Artículo 6. — [10 L.P.R.A. § 2183 Inciso (3)]

Ninguna persona, excepto un usuario autorizado o dueño de la computadora u ordenador, podrá:

(a) Inducir a un usuario autorizado a instalar un programa o componente del mismo a través de treta o engaño, representando falsamente que dicho programa es necesario para garantizar la seguridad de la computadora u ordenador o para que la computadora u ordenador pueda abrir cierto expediente, programa o archivo.

Artículo 7. — Penalidades. (10 L.P.R.A. § 2184)

Toda persona que, con la intención de defraudar o de causar daño económico o de otra naturaleza, a sabiendas e intencionalmente, viole cualesquiera de las disposiciones incluidas en los Artículos 4 y 5 de esta Ley, incurrirá en delito grave de cuarto grado y se le aplicará la pena dispuesta en el [Código Penal](#) del Estado Libre Asociado de Puerto Rico, según enmendado, para tal clase de delitos.

Toda persona que por su imprudencia y al no observar el debido cuidado viole cualesquiera de las disposiciones incluidas en los Artículos 4 y 5 de esta Ley, incurrirá en delito menos grave y se le aplicará la pena dispuesta en el [Código Penal](#) del Estado Libre Asociado de Puerto Rico, según enmendado, para tal clase de delitos.

Artículo 8. — Reserva de Derecho. (10 L.P.R.A. § 2185)

Nada de lo dispuesto en esta Ley se interpretará como una limitación al derecho de las compañías proveedoras de servicio de acceso a la “Internet”, en cualesquiera de sus modalidades, a monitorear su red; interactuar con sus suscriptores; y realizar cualquier otra acción relacionada al sistema de seguridad del proveedor, reparaciones al sistema, actualizaciones de equipo y programas y sobre cualquier programa de detección o prevención de uso no autorizado, fraudulento o ilegal, del sistema de acceso a la “Internet” provisto por el proveedor.

Artículo 9. — Separabilidad. (10 L.P.R.A. § 2181 nota)

Si cualquier cláusula, inciso, artículo, sección, título o parte de esta Ley fuere declarada inconstitucional por un Tribunal competente, la sentencia a tal efecto dictada no afectará, perjudicará, ni invalidará el resto de la Ley.

Artículo 10. — Vigencia. Esta Ley comenzar a regir inmediatamente después de su aprobación.

Nota. Este documento fue compilado por personal de la [Oficina de Gerencia y Presupuesto](#) del Gobierno de Puerto Rico, como un medio de alertar a los usuarios de nuestra Biblioteca de las últimas enmiendas aprobadas para esta Ley. Aunque hemos puesto todo nuestro esfuerzo en la preparación del mismo, este no es una compilación oficial y podría no estar completamente libre de errores inadvertidos; los cuales al ser tomados en conocimiento son corregidos de inmediato. En el mismo se han incorporado todas las enmiendas hechas a la Ley a fin de facilitar su consulta. Para exactitud y precisión, refiérase a los textos originales de dicha ley y a la colección de Leyes de Puerto Rico Anotadas L.P.R.A.. Las anotaciones en letra cursiva y entre corchetes añadidas al texto, no forman parte de la Ley; las mismas solo se incluyen para el caso en que alguna ley fue derogada y ha sido sustituida por otra que está vigente. Los enlaces al Internet solo se dirigen a fuentes gubernamentales. Los enlaces a las leyes enmendatorias pertenecen a la página web de la [Oficina de Servicios Legislativos](#) de la Asamblea Legislativa de Puerto Rico. Los enlaces a las leyes federales pertenecen a la página web de la [US Government Publishing Office GPO](#) de los Estados Unidos de Norteamérica. Los enlaces a los Reglamentos y Ordenes Ejecutivas del Gobernador, pertenecen a la página web del [Departamento de Estado](#) del Gobierno de Puerto Rico. Compilado por la Biblioteca de la Oficina de Gerencia y Presupuesto.

Véase además la [Versión Original de esta Ley](#), tal como fue aprobada por la Legislatura de Puerto Rico.

⇒ ⇒ ⇒ Verifique en la Biblioteca Virtual de OGP la **Última Copia Revisada** (Rev.) para esta compilación.

Ir a: www.ogp.pr.gov ⇒ Biblioteca Virtual ⇒ Leyes de Referencia—SEGURIDAD INFORMÁTICA.