REPÚBLICA ORIENTAL DEL URUGUAY

CÁMARA DE REPRESENTANTES

**SECRETARÍA**

**COMISIÓN DE CONSTITUCIÓN, CÓDIGOS, LEGISLACIÓN GENERAL Y ADMINISTRACIÓN**

REPARTIDO Nº 1359
JUNIO DE 2014

CARPETA Nº 2819 DE 2014

# DELITOS INFORMÁTICOS

## T i p i f i c a c i ó n

*XLVIIa. Legislatura*

PODER EJECUTIVO

Montevideo, 16 de mayo de 2014

Señor Presidente de la Asamblea General:

El Poder Ejecutivo tiene el honor de dirigirse a ese Cuerpo, a efectos de someter a su consideración el presente proyecto de ley, en virtud de la necesidad de legislar sobre la comisión de delitos informáticos, no pretendiendo abarcar todos los delitos informáticos que pueden llegar a cometerse, sino de un elenco mínimo y necesario para brindar certezas jurídicas en un plazo breve.

Estamos en conocimiento del proyecto de Reforma de Código Penal y la inclusión de las herramientas tecnológicas a las figuras tradicionales, pero entendemos que es necesaria la tipificación, en forma rápida, de las figuras que se describen a continuación y que no necesariamente quedan incluidas en los delitos tradicionales realizados por medios electrónicos.

Se tipifican, entonces, con precisión algunas conductas marcadamente lesivas de bienes jurídicos cuya vulnerabilidad de grado mayor siempre ha estado en la mira del Derecho Penal (la fe pública, los derechos fundamentales, entre otros), pero que al ser ejecutadas contra, o por medio de un sistema informático, hoy día requieren de renovadas previsiones legales.

Está comprobado que el potencial lesivo de una conducta criminal que pudiera considerarse como tradicional, se ve amplificado cuando intervienen las tecnologías, donde el medio u objeto afectados caracterizan de modo sustancial el iter delictivo.

Entran en esta apreciación desde un simple acceso no autorizado a un sistema informático, hasta el daño infringido al sistema. Con efectos de menoscabo que pueden llegar a extenderse en cascada, incluso, a los bienes o servicios que dependen del sistema afectado. Además, se consideran las acciones basadas en engaños tendientes a sustraer, obtener o falsificar información (por ejemplo: phishing, clonación de tarjetas magnéticas).

Un ámbito que ha ido adquiriendo rápida relevancia para la comisión de esta clase de delitos son las redes sociales. Su fácil y rápido efecto viral, aunado a su utilización masiva, resultan factores propicios para el ejercicio de conductas merecedoras de punición penal como son las suplantaciones de identidad.

Desde el ángulo de los incidentes de seguridad informática, resulta necesario contar con tipos penales que actualicen los existentes, para sumar instrumentos en el combate y represión de aquellas acciones que atentan contra sistemas informáticos, en especial contra los activos de información críticos del Estado y otras organizaciones que involucran programas y conjuntos de datos de alto valor estratégico (ejemplo los afectados a la seguridad nacional, salud pública, entre otros).

Se protege también el derecho humano a la intimidad y a la privacidad, con fundamento en el artículo 72 de la Constitución de la República y regulado por la Ley Nº 18.331, de 11 de agosto de 2008, la cual prevé un elenco de sanciones administrativas, que hoy en día son insuficientes para disuadir a

personas y empresas de la realización de tratamientos de datos de carácter personal, a través de medios engañosos, abusivos o extorsivos. La doctrina internacional entiende que al ser los datos personales la moneda de oro de la sociedad de la información amerita regular la violación de este derecho por vía penal.

El proyecto de ley puesto a consideración a través del presente texto aborda los objetivos enunciados buscando suministrar a Jueces, Fiscales y operadores de la Justicia en general, una herramienta más fina, sensible y eficaz que aquélla con la que se cuenta actualmente (Código Penal, algunas leyes especiales conexas al tema), por fuerza más adaptada al vertiginoso y complejo mundo de la sociedad y economía digitales, donde la delincuencia nacional e internacional han hecho del medio electrónico un elemento recurrente y preferido para la comisión de sus acciones.

El Poder Ejecutivo saluda a ese Cuerpo con su mayor consideración.

JOSÉ MUJICA
ÓSCAR GÓMEZ
JORGE POLGAR
ELEUTERIO FERNÁNDEZ HUIDOBRO
ENRIQUE PINTADO
EDGARDO ORTUÑO
JOSÉ BAYARDI
LEONEL BRIOZZO
ENZO BENECH
LILIAM KECHICHIAN
FRANCISCO BELTRAME
DANIEL OLESKER

_____

PROYECTO DE LEY

Artículo 1º. Definiciones.- Se entenderá por:

a. Activos de información: aquellos datos o información que tienen valor para una organización.

b. Activos de información críticos del Estado: aquellos activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios vitales para la operación del gobierno y la economía del país.

c. Activos de información críticos de entidades privadas: aquellos activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios esenciales de las entidades privadas.

d. Dato personal: información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.

e. Datos sensibles: datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

f. Servicios vitales para la operación del gobierno y la economía del país: son aquéllos referidos a la salud, orden público, servicios de emergencia, energía, telecomunicaciones, transporte, suministro de agua potable, ecología y ambiente, agroindustria, servicios públicos, banca y servicios financieros o cualquier otro que afecte a un sector significativo de la población, considerado desde un punto de vista cualitativo o cuantitativo.

g. Sistema informático: aquellos dispositivos electrónicos y redes de comunicación electrónica así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.

h. Tratamiento de datos: operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Artículo 2º. Acceso no autorizado.- El que en forma no autorizada, infringiendo o no medidas de seguridad, acceda a todo o parte de un sistema informático, será castigado con la pena de seis meses de prisión a tres años de penitenciaría y multa de 160 a 3.200 Unidad Reajustables.

Constituye agravante especial la revelación o difusión a terceros de la información accedida en forma no autorizada.

Artículo 3º. Daño informático.- El que en forma no autorizada dañe, borre, altere, deteriore o suprima datos o sistemas informáticos, o inutilice, obstaculice o distorsione el funcionamiento de éstos, será castigado con la pena de seis meses de prisión a seis años de penitenciaría y multa de 160 a 3.200 Unidad Reajustables.

Artículo 4º. Estafa informática.- El que, mediante el uso de tecnologías, se valiere de cualquier manipulación engañosa de sistemas informáticos o de información en ellos contenida, para procurarse a sí mismo o a un tercero un provecho injusto en daño de otro,

será castigado con la pena de seis meses de prisión a cuatro años de penitenciaría y multa de 160 a 3.200 Unidades Reajustables.

Artículo 5º. Suplantación de identidad.- El que, mediante la utilización de tecnologías, suplante la identidad de una persona física, aún fallecida, con la finalidad de cometer una actividad penada por la ley, o de la cual resulte un perjuicio injustificado, será castigado con la pena de dieciocho meses de prisión a ocho años de penitenciaría y multa de 160 a 3.200 Unidades Reajustables.

Artículo 6º. Protección de datos personales.- El que, a través de medios engañosos, abusivos o extorsivos, efectúe cualquier tipo de tratamiento de datos personales, será castigado con la pena de tres meses de prisión a seis años de penitenciaría y multa de 160 a 3.200 Unidades Reajustables.

Artículo 7º .Agravantes.- Se consideran circunstancias agravantes de los delitos tipificados en esta ley, las siguientes:

1. Que el daño provocado sea irreparable o fuere imposible retornar al estado original de la información o de los sistemas informáticos afectados.
2. Que el ilícito se cometa para obtener un beneficio económico o de cualquier otra naturaleza, para sí o para un tercero.
3. Que la acción criminal recaiga sobre activos de información críticos del Estado o activos de información críticos de entidades privadas.
4. Que la víctima sea una persona menor de edad o con discapacidad.
5. Que la acción criminal recaiga sobre datos personales sensibles.

Montevideo, 16 de mayo de 2014

ÓSCAR GÓMEZ
JORGE POLGAR
ELEUTERIO FERNÁNDEZ HUIDOBRO
ENRIQUE PINTADO
EDGARDO ORTUÑO
JOSÉ BAYARDI
LEONEL BRIOZZO
ENZO BENECH
LILIAM KECHICHIAN
FRANCISCO BELTRAME
DANIEL OLESKER

=