

# Expertos creen que Ley de Delitos Informáticos

debe ser equilibrada en aspectos jurídicos y técnicos

21 AGO 2012 Ciencia y Tecnología



El Lic. Roberto Lemaitre Picado, es abogado e ingeniero informático especialista en ciberdelitos. Además, es el representante de Costa Rica para la Red Iberoamericana de Derechos Informáticos y labora como abogado en el área de informática jurídica en la Facultad de Derecho de la Universidad de Costa Rica (foto Laura Rodríguez).

Costa Rica necesita una legislación sobre delitos informáticos que sea actual y equilibrada en aspectos técnicos y jurídicos para proteger a los usuarios y la información de la ciberdelincuencia. Esta fue una de las principales conclusiones de la mesa redonda *Reflexiones en torno a la nueva Ley de Seguridad Informática*, organizada recientemente por el Programa Sociedad de la Información y el Conocimiento de la Universidad de Costa Rica (Prosic).

La actividad tenía como objetivo ser un espacio para intercambiar ideas sobre la Ley de Delitos Informáticos 9048, la cual fue firmada el mes pasado por la Presidencia de la República. El abogado e ingeniero informático, Lic. Roberto Lemaitre Picado, explicó que el país necesitaba una nueva ley de delitos informáticos, pues **la sociedad costarricense cada vez más tiene acceso a las nuevas tecnologías con lo cual exponen su información e identidad** en diferentes redes locales y globales gracias a Internet. La última legislación vigente en esta materia era del 2001.

“Comprendamos que la sociedad de Costa Rica ha cambiado. Vivimos en lo que ahora denominamos la *cibersociedad*, que presenta la información como bien y como actividad”. Por ejemplo, mencionó que **Costa Rica se encuentra entre los primeros 10 países de Latinoamérica que más genera ataques maliciosos hacia la red.**

El abogado explicó que la persecución de un delito informático suele ser muy compleja debido a la forma en la que se transmiten los datos y porque **las evidencias son muy sensibles a sufrir cambios**, lo que dificulta delatar al autor de un ataque.

Con la Ley 9048 de Delitos Informáticos se establecen reformas y modificaciones al Código Penal, con lo cual se establecen nuevos tipos penales como suplantación de identidad, suplantación de páginas electrónicas e instalación o propagación de programas informáticos maliciosos. También se contemplan otros delitos como la violación de correspondencia y datos personales, extorsión, estafa informática, daño informático y espionaje. Con lo anterior, se busca no sólo la protección de personas físicas, sino también de personas jurídicas.



El M.Sc. Francisco Salas Ruiz es abogado especialista en delitos informáticos y profesor de la Facultad de Derecho de la Universidad de Costa Rica. Participó como experto en la formulación del proyecto de ley que dio origen a la Ley 9048 de Delitos Informáticos (foto Laura Rodríguez).

Otra novedad de la ley es que las penas son más altas para las personas que sean encargadas de administrar o dar soporte a un sistema o red informática y comentan un

delito, dado su conocimiento técnico y el acceso que poseen a la información.

## Seguridad informática y libertad de expresión

Si bien la nueva legislación de delitos informáticos presenta reformas importantes en el tema de ciberseguridad, también contiene artículos que han causado **polémica y dudas sobre su aplicación**. Además, la velocidad con la que se desarrollan las tecnologías se vuelve un obstáculo para mantener una legislación actualizada y sin vacíos legales, coincidieron los expertos participantes en la actividad.

El M.Sc. Francisco Salas Ruiz, quien es abogado especialista en delitos informáticos y profesor de la Facultad de Derecho de la UCR, expuso que la formulación y aprobación en Plenario Legislativo de la Ley 9048 de Delitos Informáticos fue **un proceso largo que requirió de la asesoría de técnicos especialistas** en el tema. Incluso, el proyecto de ley fue revisado por un representante del Consejo de Europa, que es la instancia internacional más reconocida que ha dictado estándares a nivel mundial sobre ciberdelincuencia.

El M.Sc. Ruiz fue tajante al explicar que el artículo 288 sobre espionaje informático, **no fue formulado con fines políticos o para atentar contra la libertad de expresión y la labor periodística**. Dicho artículo plantea: "Será reprimido con prisión de cuatro a ocho años al que procure u obtenga indebidamente informaciones secretas políticas o de los cuerpos de policía nacionales o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la nación, o afecte la lucha contra el narcotráfico o el crimen organizado".



El Dr. Marlon Mora es periodista y académico especializado en desigualdades e intervención social. Participó en la mesa redonda como representante del Colegio de Periodistas (foto Laura Rodríguez).

Según el especialista, la prensa ha **malinterpretado e incomprendido** la legislación y no ha consultado la opinión experta de los técnicos que ayudaron a redactar la ley. Tampoco se

ha tomado en cuenta que la figura de informaciones secretas políticas está contemplada en el Código Penal desde 1970.

“Esto es un trabajo bastante técnico. No será perfecto, por supuesto que no, pero yo creo que las personas que hemos participado, quienes lo han revisado y le han dado el visto bueno, son personas que tienen absolutamente toda la credibilidad en esta materia, porque es sumamente especializada. No se trata de un tema político”, dijo el MSc. Ruiz.

**El abogado añadió que el delito de espionaje se configura en el momento en el que se da la apropiación de la información, por lo que no se coarta la libertad de expresión, porque no es necesario revelar ciertos datos para cometer un delito.**

Por su parte, el periodista y académico Dr. Marlon Mora, planteó desde una reflexión personal que **la ley de delitos informáticos es necesaria, pero requiere cambios importantes.** Además, como representante del Colegio de Periodistas (Colper), también expuso la posición de dicha organización.

“La ley de delitos informáticos en varios apartados no solamente tiene afectación para los periodistas, sino para los comunicadores, que pueden ser todos y todas”, mencionó el Lic. Mora. El periodista cuestionó que si ninguna persona ha sido acusada por la obtención de informaciones secretas políticas, ¿por qué es necesario mantener ese término en la ley?, además apuntó que este hecho no descarta que en el futuro alguien pueda ser sancionado.



El Lic. José Adalid Medrano es abogado consultor en temas de ciberseguridad y fundador de la plataforma ticoblogger, la cual alberga blogs de usuarios costarricenses (foto Laura Rodríguez).

Para el Dr. Mora, Costa Rica es un país democrático donde **el uso de los secretos de Estado debería ser limitado para asegurar la transparencia política.** Además, la Ley de Delitos

Informáticos debería armonizar el término de informaciones secretas políticas con el de secretos de Estado que se presenta en la Constitución Política.

“A mí me preocupa muchísimo que al final una interpretación que hacen los comunicadores al respecto de la ley, permita que nosotros apliquemos una autocensura y un temor a seguir investigando sobre temas específicos en el caso que caigan en esas tres palabras (informaciones secretas políticas)”, mencionó el periodista.

### ¿Cómo enfrentar la delincuencia informática?

Para combatir la ciberdelincuencia de forma efectiva, los especialistas participantes en la mesa redonda coincidieron en que es necesaria la **educación del usuario** y también **voluntad política** para emitir una legislación equilibrada en lo técnico y jurídico.

El abogado y consultor sobre ciberdelincuencia, Lic. José Adalid Medrano, explicó que la educación es necesaria para asegurar la protección de los usuarios y su información, pues no basta con tener una ley.



El público asistente mostró interés por conocer sobre los detalles de la Ley 9048 de Delitos Informáticos, especialmente en temas como el resguardo de la identidad e información personal foto Laura Rodríguez).

“Generalmente la principal vulnerabilidad de un sistema informático viene a ser la falta de conocimiento que tienen los mismos usuarios de las nuevas tecnologías o de las tecnologías en general”.

En este punto también coincidió el Lic. Lemaitre, quien dijo que los usuarios suelen ignorar de la **importancia de actualizar los programas antivirus y los equipos** para disminuir vulnerabilidades.

La **formación jurídica e informática** también debe incluir a los abogados y jueces para comprender mejor los delitos y aplicar la justicia. “Los jueces y abogados ocupan formarse

en términos técnicos también para que comprendan este tipo de delitos. Si sólo se mantienen en el tema jurídico no van a comprender cómo ocurren estos delitos, qué es lo que hay detrás”, dijo el Lic. Lemaitre.

El Lic. Medrano mencionó que la voluntad política también es clave para lograr una legislación contra la ciberdelincuencia efectiva. Según el abogado, en la legislación que fue firmada recientemente, **los asesores legislativos ignoraron recomendaciones** que hicieron los técnicos especialistas y eso se traduce en **errores y vacíos legales**. Por ejemplo, es necesario que se contemple en la ley **la colaboración transfronteriza** para que los delitos informáticos no queden impunes, pues la ciberdelincuencia es una realidad mundial que no se limita a Costa Rica.

Recientemente se presentó ante la Asamblea Legislativa un **nuevo proyecto de ley** que pretende corregir los **vicios y vacíos legales** que se considera tiene la Ley 9048 de Delitos Informáticos. Se espera que el proyecto entre a la corriente legislativa este mes para su discusión y posterior aprobación.

[Anna Georgina Velásquez Vásquez](#)  
Periodista Oficina de Divulgación e Información  
[anna.velasquez@ucr.ac.cr](mailto:anna.velasquez@ucr.ac.cr)

**Etiquetas:** [ciberseguridad](#), [ciberdelincuencia](#), [delincuencia informatica](#), [ataques informaticos](#), [malware](#), [seguridad informatica](#), .