

## Síntesis del módulo 5

En el módulo 5 estuvimos compartiendo materiales y reflexiones sobre el tema de los ciberdelitos y la doctrina de la ciberseguridad. Antes que nada, muchas gracias a todas y todos por hacer la tarea y participar en el foro. Una de las riquezas que tiene este curso es la diversidad de participantes, que venimos de muchos países distintos, con realidades diferentes, lo cual sirve para enriquecer la discusión.

Lo primero que nos llamó la atención es la sensibilidad y empatía compartida hacia Aaron Swartz, esa especie de niño genio que asombró a todo el mundo por su talento como desarrollador y por su militancia firme en favor del acceso libre al conocimiento. Hubo un acuerdo bastante generalizado en torno a que la acusación fue injusta. Pero lo importante para este módulo es que la persecución contra Aaron se hizo aplicando la ley de delitos informáticos de Estados Unidos, una ley hiperpunitiva y cuyos artículos están redactados de forma poco precisa, lo cual habilitó que se presentaran acusaciones por acciones que no deberían ser sancionadas penalmente. Recuerden siempre que uno de los principios del derecho penal es que las penas deben ser proporcionales a la gravedad del delito cometido, y que las penas de privación de libertad únicamente deben aplicarse para los delitos más graves y aberrantes.

Las nuevas tecnologías a veces generan situaciones no previstas en las leyes. Sin embargo, no siempre es así. Por ejemplo, el phishing, la estafa nigeriana y otros tipos de estafas llevadas a cabo por Internet están contemplados en las legislaciones de todos nuestros países. Esto es así porque se tratan lisa y llanamente de estafas, un delito que tiene una larga historia en nuestros códigos penales. El hecho de que la estafa se realice por medios informáticos no cambia la naturaleza del delito (que consiste en engañar a otra persona para quedarse con su dinero).

Algo similar ocurre con los delitos contra la integridad sexual. El hecho de que se cometan usando medios informáticos no cambia la naturaleza del delito.

En ocasiones, es razonable que el uso de medios informáticos se considere agravante de un delito, porque en algunos casos su uso tiene el potencial de causar un daño mayor a la víctima. Pero, tal como comenta Beatriz Busaniche en [el material principal de este módulo](#), lo que es sumamente peligroso es duplicar delitos o crear delitos nuevos para Internet, como si Internet estuviera en una dimensión distinta que la dimensión offline.

Es importante saber que cuando en los medios de comunicación se habla de los graves peligros de Internet, o de la impunidad que reina en Internet, se pasa por alto que la mayoría de nuestros códigos penales ya tienen herramientas para castigar las estafas, la violación de la correspondencia electrónica, el daño a sistemas informáticos y el acoso sexual por Internet, por ejemplo. Lo que en realidad oculta muchas veces este discurso mediático es la pretensión de brindar más poderes a la policía y a otros organismos del Estado para violar la privacidad de los ciudadanos o aplicar la censura en Internet. También es muy común que políticos oportunistas usen casos mediáticos para quejarse de que Internet es tierra de nadie, pidiendo la creación de nuevos delitos y el

establecimiento de penas desproporcionadas.

Por eso, siempre que escuchemos este discurso, lo importante es estar alertas y cuando se pidan nuevos delitos para Internet, siempre pensemos: ¿este delito no existe ya?, ¿la pena que se pide es proporcional a la gravedad del delito?, ¿la redacción del delito puede hacer que se metan en la misma bolsa acciones dignas de castigo y otras que no lo son?

Dos casos concretos pueden ayudar a entender mejor lo que planteamos en el módulo. Uno es el caso del grooming y otro es el de la suplantación de identidad.

El "grooming" ha sido descrito en Argentina como el contacto, a través de medios electrónicos, de un adulto con una persona menor de edad con el propósito de cometer un delito contra la integridad sexual de ella. Incorporar este nuevo delito, que a primera vista parecería estar hecho para proteger a los niños en Internet, en realidad es peligroso e innecesario. Innecesario, porque los delitos contra la integridad sexual ya existen independientemente del medio por el cual se cometan. Peligroso, porque pretende juzgar de manera diferente las acciones que las personas hacen en Internet y las que se hacen offline. Peligroso, también, porque no pretende castigar hechos ni acciones preparatorias sino meras intenciones o propósitos, cosa que el derecho penal siempre se abstuvo de hacer. Pueden leer más en detalle sobre la legislación de grooming en Argentina, en [este texto de Gustavo Garibaldi](#).

La “suplantación de identidad” por medios electrónicos es otra de las figuras penales que despierta simpatías en muchos ámbitos políticos y en los medios de comunicación, pidiendo penas que llegan con frecuencia a cifras disparatadas como seis u ocho años de prisión. Pero, ¿de qué nos protege tipificar como delito la suplantación de identidad? Si se nos pretende proteger de estafadores, sólo es necesario revisar que el delito de estafa abarque aquellos casos donde la misma se comete a través de la manipulación de datos personales. Si se nos pretende proteger de que alguien publique información falsa y maliciosa sobre nosotros, sólo es necesario aplicar, por ejemplo, tipo penales como las calumnias e injurias. Pero lo peor no es eso, sino que en muchos casos el delito de suplantación de identidad está redactado de forma imprecisa, afectando potencialmente a quienes utilizan identidades ficticias para hacer una parodia y a quienes recurren al anonimato para expresarse sin miedo a sufrir represalias. En suma, este nuevo delito pretende castigar algo que ya estaba castigado, y agrega amenazas penales para acciones totalmente legítimas.

En definitiva, lo que a los docentes de este curso nos gustaría que ustedes se lleven de este módulo es la idea de que no siempre la creación de nuevos delitos para Internet ni el aumento de las penas hace que estemos más seguros cuando estamos en línea. Por el contrario, a veces estas nuevas leyes penales, asociadas al discurso de la ciberseguridad, pueden poner en riesgo nuestros derechos. Por eso, para legislar sobre estos temas siempre hace falta un debate amplio e informado.