

# 10

de  
Octubre



Miguel Aparicio

Abogado de ECIJA

## La criminalidad informática y los delitos del presente

Es bien sabido que los delincuentes siempre van por delante de la Ley. Ya lo decían los romanos y hoy lo sigue recogiendo nuestro Código Penal en sus dos primeros artículos: "*nullum crimen, nulla poena sine praevia lege*".



Y es que hay conductas delictivas que necesitan de una gran habilidad por parte de los operadores jurídicos encargados de su persecución y enjuiciamiento. Muchas veces, jueces, fiscales y policías tienen que ingeniárselas para encontrar el encaje procesal y penal de una presunta conducta criminal. **Esto se acentúa si hablamos de los cibercriminales y cibercrimitos**, pues su grado de sofisticación ocupa otra realidad respecto a lo que la sociedad imagina e incluso los medios para perseguirlos e investigarlos resultan escasos, desfasados y frágiles, debido a que los cibercriminales juegan con la ventaja de que el legislador penal va a ir siempre a rebufo de sus ciberconductas.

No descubrimos nada nuevo si decimos que las nuevas tecnologías nos han cambiado la vida, son una herramienta de la que no podemos prescindir y de la que nos beneficiamos día a día. El mundo online está presente en cada una de las facetas de nuestra vida y avanzan de una forma frenética (smartphones, tablets y portátiles, aplicaciones, medios de pago telemático, empresas online, criptomonedas...). **Pero, esas ventajas que nos da Internet, pueden convertirse en estupendas aliadas para los "cibercacos"**. Hoy, una persona puede entrar en tu ordenador, robar tus contraseñas, suplantar tu identidad, manejar tu webcam, operar con tu cuenta bancaria, etc. y todo ello sin que tú te percatas de que estás siendo víctima del delito.

Según el último informe del Instituto Nacional de Ciberseguridad, **los incidentes de ciberseguridad aumentaron un 200 % el año pasado**. Solo en nuestro país, 162.686 páginas web sufren ataques cada día.

Además, **contamos con un problema que los cibercriminales conocen a la perfección**, y es que nuestra Ley de Enjuiciamiento Criminal data nada más y nada menos que de 1882 y, aunque siendo una estupenda ley en constante renovación, no contempla el amplio escenario digital actual. A pesar de ello, sí es

cierto que, **con la últimas reformas entradas en vigor el pasado año**, hemos avanzado en cuestiones procesales y de prevención de los ciberdelitos (como la introducción de la figura del agente digital encubierto o "ciberagente secreto", por ejemplo), sin embargo nos queda mucho camino por recorrer para combatir las numerosas amenazas de la era digital.

Para la lucha contra este tipo de delincuencia, los garantes de la seguridad del Estado, como la Policía Nacional y la Guardia Civil, **cuentan con cuerpos especializados en ciberdelitos**. Así nos encontramos con la Brigada De Investigación Tecnológica, encuadrada dentro de la UDEF, y con el Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Guardia Civil. Por su parte, el Ministerio Fiscal también cuenta con una Fiscalía especializada en Criminalidad Informática.

Así con todo, sin ánimo de ser exhaustivos, vamos a citar a modo de información los delitos más comunes cometidos a través de la Red:

**Ataques contra el derecho a la intimidad: Allanamiento informático.**

Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. Se protege la vida privada y se castiga el mero allanamiento en el dispositivo. Si además robas información el delito también es de robo de información.

Infracciones a la Propiedad Intelectual **a través de la protección de los derechos de autor**: Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. Piratería y plagio.

Sabotajes informáticos: **Delito de daños mediante la destrucción o alteración de datos**, programas o documentos electrónicos contenidos en redes o sistemas informáticos. Delito de "cracking" dentro del que están los que tienen que ver con la interrupción de un servicio -los llamados ataques de denegación de servicio-. Robo de contraseñas.

Falsificaciones: **de documentos electrónicos, de tarjetas...** Fabricación o tenencia de programas de ordenador y software para la comisión de delitos.

Fraudes informáticos: **Delito de estafa a través de la manipulación de datos o programas** para la obtención de un lucro ilícito (sin duda el más común a día de hoy).

;Amenazas, coacciones; **calumnias e injurias graves**: Realizadas por cualquier medio online y redes sociales, sobre todo.

Pornografía infantil y delitos relacionados con los menores de edad: Utilización de menores o incapaces **con fines exhibicionistas o pornográficos**. Ver pornografía infantil online. Sexting, gossiping y sextorsion, childgrooming, cyberbullying...

Acoso o acecho online: El llamado "ciberstalking".

**Suplantar la identidad**: Generalmente a través de correos electrónicos o redes sociales mediante perfiles falsos o robos de perfiles reales.

Inutilizar o perturbar el funcionamiento de las **pulseras antiviolencia de género** o de mecanismos de control telemático.

Atentar contra el orden público a través de medios tecnológicos. Así como los llamados delitos de odio y la **ciberviolencia contra quien es diferente** (orientación sexual, raza, religión...).

Para terminar, destacar que la transformación que está motivando el Código Penal en el ámbito corporativo es imparable. Actualmente, una empresa puede cometer y/o sufrir del orden de 26 tipos de delitos tecnológicos, entre los que están desde la

estafa hasta los daños informáticos, así como la denegación de servicio, delitos contra la propiedad intelectual, espionaje, falsificación de tarjetas y cuentas, blanqueo informático de capitales y activos, **pornografía infantil, "hacking" y, por supuesto, el descubrimiento y revelación de secretos.**

