

electrónico a los usuarios un cargo de 78.000 pesetas en su tarjeta de crédito por un supuesto pedido realizado, que se cargaría antes de 48 horas. A uno de los detenidos se le intervino una base de datos de más de 30.000 personas y abundante información sobre tarjetas.

▪ **Agosto de 1999:** una red de aprendices de saboteadores se introduce en los ordenadores de la Presidencia del Gobierno y modifica la página *web* de Moncloa. La imagen de José María Aznar soporta cuernos y colmillos virtuales durante más de siete horas.

▪ **Diciembre de 1998:** la Guardia Civil contempla impotente cómo su página *web* es manipulada a través de ordenadores estadounidenses en dos ocasiones. El primer ataque, durante la Operación Salida, siembra el caos en el servidor de la Benemérita, impidiendo el correcto funcionamiento de sus servicios a los usuarios. La segunda broma redirecciona la página a una *web* de orientación homosexual. Los autores enmascararon su identidad a través del servicio de correo electrónico gratuito Hotmail, propiedad de Microsoft.

▪ **Abril de 1998:** asunto Hispahack. El Grupo de Delitos de Alta Tecnología (GEDAT), en coordinación con la Interpol, detiene al más famoso grupo de delincuentes cibernéticos españoles. El grupo Hispahack se le atribuía el ataque a los servidores del Congreso de los Diputados, la NASA y la Universidad de Oxford. Sus integrantes también se introdujeron en diversos sistemas informáticos para extraer las claves de acceso de miles de usuarios. Sus presuntos autores no fueron condenados por falta de pruebas documentales.

Qué dice la ley

Las prácticas delictivas en la red de redes apenas tienen un tratamiento específico en el ordenamiento jurídico español. Aquí están las principales y su tratamiento legal. Los delincuentes virtuales se enfrentan a penas de prisión de entre seis meses y cuatro años. Unas penas poco disuasorias, según los expertos

CIBERDELITO	TRATAMIENTO LEGAL
▪ Ataques de denegación de acceso: enviar multitud de peticiones un servidor de Internet, hasta que se sature y no sea capaz de responder a las de los usuarios legítimos.	Delito o Falta de Coacciones (art. 172 del Código Penal)
▪ Ataques sobre vulnerabilidad en el sistema: aprovechar un fallo en la seguridad del sistema para tomar el control de las máquinas (acceder a información, cambiar la página <i>web</i> ...)	Depende de la intención del ataque: si es cosa de <i>hackers</i> que acceden a un sistema sin borrar ficheros, no es delito. Si acceden a un sistema que borra <i>logs</i> , es delito o falta de daños (arts. 264 ó 625.1 C.P.). Si se usan datos personales reales de un usuario suplantado, es delito contra la intimidad (art 197.2).
▪ Alteraciones de una página web	Delito o falta de daños (art. 264.2 o 265.1 CP).
▪ Acceso a información económicamente valiosa y útil.	Delito de espionaje empresarial (art. 278 CP).
▪ Sniffers: programas que espían las conexiones que pasan por una red, tomando la información que pasa por ellas (nombres de cuenta, claves, números de tarjetas de crédito...).	Delito contra la intimidad informática (art. 197.1 CP).
▪ Spoofting: cambiar la dirección IP de origen en una conexión para ocultar la real y no ser descubierto.	Acto preparatorio impune. No es delito. Queda absorbido por el delito específico que cometa con esos mecanismos.
▪ Piratería de software: hacer una copia ilegal de un programa informático.	Delito contra la propiedad intelectual (art. 270 y siguientes del CP).
▪ Creación o difusión de virus	Delito o falta de daños informáticos (art. 264.2 o 625.1), en función de si los daños ocasionados superan o no las 50.000 pta.
▪ Apropiación indebida de dominios (ciberokupas): registrar una dirección de Internet con el nombre de una conocida empresa o marca comercial, para revenderla a la organización que debería darle nombre.	No es delito. Se requiere que la legislación mercantil considere el nombre de dominio como un nombre protegido por derechos de propiedad industrial (como el rótulo de un establecimiento o la marca de un producto). El Código Penal sanciona la imitación de marcas y la venta y difusión de productos amparados en marcas falsas; pero no es delito registrar un nombre de dominio que, hasta que no es objeto de registro por una empresa, no está protegido.
▪ Uso indebido del e-mail: envío de correo electrónico no solicitado con fines comerciales.	No es delito. Es infracción a la Ley Orgánica de Protección de Datos Personales (L.O. 15/1999, de 13 diciembre). La Agencia de Protección de Datos ya ha sancionado a alguna empresa por dicho comportamiento en 1999.