

La Cámara del Crimen procesó a un ex empleado que ingresó en el sistema de la empresa e infectó con virus los servidores, provocando la destrucción de información vital para la firma. El tribunal aludió al artículo 183 del Código Penal.

La Cámara Nacional de Apelaciones en lo Criminal y Correccional confirmó el procesamiento de un ex empleado que tras ser echado de la empresa para la que trabajaba, "crackeó" sus sistemas y los infectó con virus, provocando la destrucción de información vital para la firma.

La Sala I de la Cámara, con las firmas de los jueces Jorge Rimondi y Gustavo Bruzzone, reconoció que los hechos eran anteriores a la ley que introdujo los delitos informáticos, pero afirmaron que el Código Penal ya preveía esa conducta. Además, consideraron que el hacker procedió a "destruir o inutilizar a través de un virus o al hacer desaparecer mediante el borrado un archivo de computadora como campo magnético conformado tecnológicamente", con lo cual "se estaría dañando una cosa".

En el fallo se detalla que se pudo comprobar que el imputado había "borrado múltiples directorios conteniendo datos, programas, registros y archivos" lo que provocó la desaparición de "la facturación de la noche anterior al 19 de febrero de 2008".

A su vez, a través del análisis de los registros de logs (archivos con registros de todos los movimientos de entrada o salida de cualquier tipo de información) se establecieron "intentos de ingreso de contraseñas fallidos y luego exitosos correspondientes al imputado quien, pese a haber sido desvinculado de la empresa el 28/1/2008, el 15/2/2008 solicitó le sea reactivada a efectos de retirar material personal de su computadora".

Además, cuenta el informe de la sentencia, "se da cuenta que el IP desde donde se realizaron las operaciones se encuentra registrado a nombre de M. G., pareja del imputado, lugar en el que éste también residía".

En este aspecto, los jueces aludieron al artículo 183 del Código Penal que establece que "será reprimido con prisión de 15 días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado".

Entre los fundamentos también se especifica que “un sistema operativo se compone del hardware y del software”. Este último es el componente “lógico o intangible” del sistema informático, y el procedimiento del imputado “consistió en alterar ese conjunto de instrucciones logrando que el hardware ejecutase órdenes que se tradujeron en acciones nocivas, no aprobadas por sus legítimos usuarios, siendo el ejemplo más claro el borrado de archivos de datos insertos en el disco rígido”. En este sentido, los camaristas entendieron hardware y software representan “una unidad compleja tangible-lógica”, y que “la afectación de uno implica al del otro, por lo que concluye que éste sí reúne los requisitos de cosa en el sentido del artículo 2311 del CC”.

“Sin duda es una obra humana que se puede detectar, aprehender, destruir o eliminar. Lo expuesto es perfectamente aplicable a la comisión del delito a través de Internet, modalidad conocida como sabotaje informático (cracking) constitutiva de una conducta dirigida a menoscabar la integridad y disponibilidad de la información desde una computadora que accede a través de una conexión remota; tal como sucedió en el caso a estudio”, concluyó la Cámara.

Los hechos ocurrieron en febrero de 2008 cuando la empresa despidió a quien durante 17 años fuera su Supervisor de Operaciones del sector de informática.

[Fallo completo](#)