

DELITOS INFORMÁTICOS: UN IMPORTANTE PRECEDENTE

Alberto Contreras Clunes (*)

I. PLANTEAMIENTO DEL TEMA

a) Cuestiones previas: En los últimos meses hemos observado a través de los distintos medios de comunicación, varios hechos punibles en los que la característica fundamental para su comisión ha sido el empleo de una computadora. En efecto, el caso sobre «espionaje informático» seguido contra la empresa Inverlink S.A.; el periodísticamente denominado caso «coimas», seguido en contra del Ministerio de Obras Públicas, son sólo algunos de los que aparecen a diario en los noticieros.

Los medios de comunicación en general han calificado estos hechos como «delitos modernos», «delitos tecnológicos», «delitos nuevos». En rigor la mayoría de ellos puede agruparse dentro de los Delitos Informáticos, previstos y sancionados en la Ley N°19.366, publicada en el *Diario Oficial* el 7 de junio de 1993. Esta ley en sus cuatro artículos tipifica conductas que utilizan las tecnologías de la información como medio de comisión de hechos punibles.

b) Análisis de la Ley N°19.366: El bien jurídico protegido, según la historia fidedigna de esta ley, es: La calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan.

(*) Profesor de Derecho Procesal. Universidad de Las Américas y Universidad Bolivariana.

Sin embargo, importante doctrina sostiene que los Delitos Informáticos son «pluriofensivos, por lo que atentan contra diversos bienes jurídicos, a saber, la propiedad, la intimidad, etc.»¹.

La doctrina suele clasificar los tipos penales de esta ley en: a) delitos de espionaje informático y b) delitos de sabotaje informático².

Esta ley consta de tan solo cuatro artículos, de los cuales los artículos 1, 3 y 4 exigen un dolo específico o directo en la comisión del delito, al exigir el tipo un actuar «malicioso».

Artículo 1° «El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuentita de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo».

Parte de la doctrina sostiene que no se trata de un Delito Informático propiamente tal, sino más bien de un «delito de daños convencional». Además, en esta disposición se mezcla erróneamente el daño producido al «software» con el «hardware».

Artículo 2° «El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio».

Se trata de un delito de espionaje informático, requiriendo el sujeto activo actuar con una determinada motivación, precisamente aquellas que el mismo tipo penal describe: «con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en él».

Artículo 3° «El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información, será castigado con presidio menor en

¹ Humberto Carrasco, Magíster Derecho Informático.

² Huerta M., Marcelo y Líbano M., Claudio, **Delitos Informáticos**, Ed. Cono Sur Ltda., 1996, p. 285.

su grado medio».

Nos encontramos frente a una especie de sabotaje informático, requiriendo el elemento subjetivo la concurrencia de un dolo específico o directo.

Artículo 4° «El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado».

Nuevamente se trata de una especie de espionaje informático, requiriendo el tipo un dolo específico. Además, se contempla una figura agravada, cuando quien incurre en este delito es el responsable del sistema.

II. LOS HECHOS

Entre los días 28 de diciembre de 2001 y 8 de enero de 2002, un ex empleado de la empresa ATI Chile, realizó diversas intromisiones ilegales al servidor de ésta, alterando, dañando y conociendo indebidamente información contenida en éste. Los sitios Web afectados fueron: www.guestbook.cl y www.metabuscador.cl

El imputado era un joven de 19 años, conocido en el Chat IRC con el seudónimo «POkey», el cual habría actuado por «venganza» en contra de la empresa, pues había sido despedido de ésta.

El «cracker»³ al ingresar ilegalmente a estos sitios, alteró el contenido de éstos, creando una nueva página Web (index.html) en reemplazo de la existente, que mostraba mensajes ofensivos⁴ hacia la empresa e indicaba que el sitio había sido hackeado.

El administrador del sistema informático procedió a efectuar una inmediata auditoría de todos los archivos «LOG» del servidor y pudo comprobar que dichos sitios habían sido víctima de una serie de ataques e intromisiones, además, la eliminación de algunos archivos de auditoría de transacciones de cuentas de FTP, para borrar rastros desde dónde se efectuaban los ataques. Incluso, mientras se realizaban las auditorías, se

³ Persona que «quiebra» un sistema de seguridad informática.

⁴ «Sí, soy un criminal ..., mi crimen es ser mejor que todos ustedes, algo que jamás me perdonarán ...».

pudo comprobar que el «cracker» intentaba ingresar al correo electrónico del gerente general de la empresa, hecho que pudo ser controlado a tiempo.

Se pudo comprobar que el 90% de los ataques provenía desde una IP fija, que correspondía a un Ciber Café en el cual el imputado trabajaba como administrador. El resto de los ataques provenía desde cuentas conmutadas de acceso a Internet, fundamentalmente desde el domicilio del imputado.

Una vez iniciada la investigación y presentada la querella criminal por delitos informáticos, el caso tomó especial importancia en la prensa de la ciudad de Talca y entre los usuarios del Chat IRC. Aprovechando este momento, el imputado concurrió en forma voluntaria al diario *El Centro* de Talca y entregó una entrevista, siendo portada, bajo el título: «*Yo soy el ciber pirata*». De esta manera lograba la fama y reconocimiento por sus pares, hecho buscado comúnmente entre los «crackers». Incluso ofrecía sus servicios para reparar las fallas de seguridad del sistema.

III. EL JUICIO ABREVIADO

El día fijado para la audiencia de preparación del juicio oral, los intervinientes: Ministerio Público, Defensor Penal Público y Querellante, acordaron proceder conforme al Procedimiento Abreviado⁵. Para ello el querellante tuvo que desistirse de otros dos delitos a fin de cumplir con los requisitos establecidos en el Código Procesal Penal. Una vez realizadas las preguntas de rigor al acusado, la Juez de Garantía señora Marta Asiaín Madariaga, autoriza la realización del juicio abreviado y da la palabra al fiscal para que exponga el caso.

El fiscal jefe de la ciudad de Talca don Carlos Olivos Muñoz, realizó una clara exposición respecto de los hechos, la investigación realizada, todos los medios de prueba reunidos durante ocho meses de investigación y solicitó la aplicación de una pena de 3 años y un día de presidio, por tres delitos informáticos: artículos 1, 2 y 3 de la Ley 19.223.

El querellante, abogado Alberto Contreras Clunes, ratifica todo lo señalado por el fiscal y recalca la gravedad de los delitos imputados, los perjuicios ocasionados a la

⁵ Artículo 406 del Código Procesal Penal.

empresa y el actuar malicioso del acusado. También resalta el hecho que el acusado confiesa su participación en su declaración policial y el jactarse de ello en la entrevista del diario *El Centro*.

Importante resulta la inclusión de un peritaje informático realizado por la Brigada del Ciber Crimen de la Policía de Investigaciones de Chile. En efecto, se realizó un peritaje a la computadora que ocupaba el acusado en el Ciber Café, como a su computadora personal. Por medio de un sofisticado programa, inaugurado en esta ocasión, se logra recuperar diversos archivos borrados del disco duro de la CPU del Ciber Café. Merece especial atención uno, consistente en un correo electrónico enviado por el acusado a su pareja en el cual le cuenta: *«estoy borrando unas («weas») que me pueden comprometer en los asuntos judiciales ...»*, enviado precisamente en la tarde del día anterior al que prestó declaración policial.

En sus conclusiones el peritaje señala que: *«El computador en cuestión cuenta con las capacidades técnicas necesarias y los programas adecuados tanto para navegar por Internet como para efectuar daños a sistemas informáticos»*. En efecto, se pudo determinar que el disco duro contenía 24 programas: *«... de uso frecuente por los Hackers, Crackers o Criminales Informáticos»*.

Finaliza el querellante señalando la importancia que tiene la informática en la actualidad, las potenciales víctimas de este tipo de delitos y los graves perjuicios que se causan a las empresas, pudiendo éstas llegar a quebrar económicamente por el desprestigio que estos delitos le provocan, solicitando la imposición de una pena de cinco años de presidio, en atención a tratarse de reiteración de delitos, contemplados en los artículos 1, 2 y 3 de la Ley 19.223.

Por su parte el defensor penal público don Joaquín Lagos León, alegó indicando que no se encontraba acreditada la participación de su defendido en los hechos, negándole valor a la declaración policial.

Introdujo una novedosa jurisprudencia del derecho norte americano, en la cual se penaliza a las empresas que ofrecen servicios de seguridad informática y son víctimas de «hackers», puesto que no dan cumplimiento a los servicios ofrecidos⁶.

⁶ La empresa víctima se dedica sólo a «Web hosting», es decir, alberga páginas Web, las diseña y mantiene.

Trata en detalle las circunstancias personales del acusado, indicando que se trata de un joven autodidacta en computación, de esfuerzo, padre de familia, casado. Solicita la absolución de su representado y en caso de condena, se aplique el mínimo de la escala, esto es, la pena de 541 días de presidio, con el beneficio de libertad vigilada, al no registrar antecedentes penales.

IV. EL FALLO

Al finalizar la audiencia, la Juez de Garantía dicta su veredicto: Culpable por los delitos N°1, 2 y 3 de la Ley 19.223, fijando la fecha de la lectura del fallo para el día 11 de abril de 2003.

El fallo consta de 13 fojas en las que pormenorizadamente se analizan todos los medios de prueba, describiendo en forma precisa el actuar delictivo y la forma en que éste se encontraba acreditado.

Al fijar la pena, la Juez advierte que tratándose de reiteración de delitos resulta más beneficioso aplicar una pena única conforme al artículo 351 del Código Procesal Penal. Señala también que lo dispuesto en el inciso cuarto de dicho artículo, es: *«una facultad para el Tribunal»* en consideración a que el querellante solicitó una pena superior a la del fiscal.

Por otra parte, afirma que: *«la entidad de las atenuantes⁷ no nos convence, teniendo presente que según quedó establecido se trata de delitos reiterados, por lo que la pena que se impondrá en el grado señalado se considera más condigna con el actuar ilícito del acusado»*.

En atención a ello aplica la pena de tres años y un día de presidio, que es el mínimo de la escala penal de presidio menor en su grado máximo.

V. COMENTARIOS

Tratar los Delitos Informáticos es en sí un tema complejo. Sin embargo, la claridad del fallo nos deja plenamente satisfechos que se ha comprendido en toda su dimensión

⁷ Artículo 11 N°6 y N°9 del Código Penal.

el tipo penal y las consecuencias que de él derivan.

Siendo muchas veces la prueba pericial esencial en el esclarecimiento de los hechos y la participación del autor de estos ilícitos, ella fue cabalmente comprendida y acreditó, más allá de toda duda razonable, la participación culpable del acusado.

La oportuna incautación de la CPU del acusado y del servidor del Ciber Café, además, del análisis exhaustivo dichos equipos; logró precisar con fecha, hora, minuto y segundo cuando se cometieron los ataques, como también el lugar de origen de éstos y el usuario que los realizó.

La oportuna detección de los ataques y las rigurosas medidas de seguridad aplicadas por la empresa, evitaron que los daños y perjuicios fuesen mayores.

La adecuada colaboración entre el fiscal jefe del Ministerio Público de la ciudad de Talca señor Carlos Olivos con el abogado querellante y la víctima, lograron diseñar una investigación que a lo largo de ocho meses obtuvo abundantes medios probatorios que incriminaron al imputado.

Siendo éste el primer caso sobre Delito Informático dentro de la reforma procesal penal y la meridiana claridad de los fundamentos en la sentencia condenatoria, se convertirá necesariamente en un obligado precedente.

Es necesario destacar que, más allá del éxito en la resolución del caso, existió una empresa que se atrevió a denunciar el delito, con todas las consecuencias que trajo para con sus clientes y prestigio, algo que por lo general no hacen las víctimas de estos delitos.

Como conclusión final simplemente cabe señalar que en la actualidad existe suficiente tecnología para investigar este tipo de delitos y, mejor aún, es posible sancionar a los autores de éstos, erróneamente denominados «hackers», siendo en rigor, simples delincuentes informáticos⁸.

⁸ Más información sobre este caso en: www.abogadoalbertocontreras.com y www.atichile.cl