CONSIDERACIONES SOBRE EL DELITO DE DAÑOS INFORMÁTICOS, EN ESPECIAL SOBRE LA DIFUSIÓN DE VIRUS INFORMÁTICOS

Julio F. Mazuelos Coello

El delito de daños informáticos o también denominado sabotaje informático persigue la sanción de quien perturba un procesador de datos que es de esencial importancia para una empresa ajena o para una autoridad, a través del menoscabo, destrucción, deterioro, inutilización, eliminación o transformación de un equipo de procesamiento de datos o un soporte de datos. La configuración de un tipo penal especial de daños se fundamentaría en la toma de conciencia acerca de la necesidad de un desarrollo del procesamiento de datos libre de perturbaciones, para la economía y la administración pública y, a su vez, en la comprobación de los elevados daños que conlleva esta especial forma peligrosa de sabotaje económico[1].

En líneas generales, la doctrina concibe que los daños o sabotajes informáticos se presentan bajo dos modalidades, una eminentemente de contenido informático en la que se emplean procedimientos informáticos para su realización: difusión de un virus, otra de naturaleza mecánica en la que la destrucción o el daño es originado a través de un golpe, fractura, destrucción física del disquette, la computadora, el CD, consiguiéndose prácticamente el mismo efecto que con la intervención de naturaleza informática[2].

---

1 Cfr. KRUTISCH, *Strafbarkeit des unberechtigten Zugangs zu Computerdaten uns –systemen*, Frankfurt a. M., 2004, pp. 154 y s.

2 Cfr. MATA, *Delincuencia informática y Derecho penal*, Madrid, 2001, p. 59; una presentación de las

Esta afirmación parte de una equiparación fenomenológica de los daños sobre el proceso informático con aquellos que recaen sobre el bien material en sí; sin embargo, el centro de discusión en los delitos informáticos no es el bien *per se*, sino su funcionalidad. Aquí podemos adelantar que el contenido penal informático de la conducta en sentido estricto radica en la determinación de que el hecho sólo es posible en cuanto a realizarlo a través de la informática, lo cual posibilita descartar aquellas conductas que están en relación externa con el empleo de la tecnología informática; luego, se eliminan los daños de naturaleza mecánica y son remitidos al tipo penal genérico del delito de daños.

En definitiva, el delito de daños informáticos sólo es realizable mediante el empleo de procedimiento informático.

EL BIEN JURÍDICO

La cuestión acerca del bien jurídico protegido en el sabotaje informático no es pacífica en la doctrina. Así, por ejemplo, algunos autores vinculan este delito con la alteración de datos en general (§ 303a StGB) y sostienen que la propiedad constituye el bien jurídico protegido en el sabotaje informático[3]. Según otra interpretación, en el sabotaje informático se protege el funcionamiento libre de perturbaciones de los equipos de procesamiento de datos como bien jurídico supraindividual[4].

La doctrina mayoritaria en Alemania considera que el bien jurídico protegido en el sabotaje informático constituye el interés de las empresas, firmas y autoridades en el desarrollo de su procesamiento de datos libre de perturbaciones[5].

---

diversas modalidades puede verse en CORCOY, "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", *La Ley*, vol. 1, n.º 2400, 1990, pp. 1002 y ss.

3 Así, HAFT. "Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) – Teil 2: Computerdelikte", *NStZ*, 1987, pp. 6 y ss., 10. En la doctrina española, MATA, *Delincuencia informática*, . cit., pp. 78 y ss.

4 En este sentido, ACHENBACH, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, *NJW*, 1986, pp. 1835 y ss., 1838. Sin embargo, pareciera que los tipos penales que sancionan el sabotaje informático no persiguen una protección general de los sistemas de procesamiento de datos ante cualquier perturbación: cfr. las críticas con relación a esta interpretación del § 303 b StGB (sabotaje informático C.P. alemán) en SCHULZE-HEIMING, *Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls*, Münster/New York, 1995, p. 196. Nótese que tampoco este delito se orienta a la protección de la capacidad de funcionamiento de los sistemas de procesamiento de datos *per se*, sino a otorgar sólo protección frente a intervenciones de terceros; en este sentido, SCHLÜCHTER, *Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität*, Heidelberg, 1987, p. 71.

5 Así, KRUTISCH, *Strafbarkeit*, Ob. cit., p. 155; LENCKNER/WINKELBAUER, Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG (I), *CR*, 1986, pp. 128 y ss., 483 y ss., 654 y ss., pp. 824 y ss., p. 830; MÖHRENSCHLAGER, Das neue Computerstrafrecht, *wistra*, 1986, pp. 128 y ss., p. 142; MÜHLE, *Hacker und Computer-Viren im Internet – eine strafrechtliche Beurteilung*, Passau, 1998, p. 122; SONDERMANN,

En el ámbito penal informático es necesario mantener una concepción del objeto jurídico de protección alejada de una idea naturalística de los daños, en la que la afectación no deba de verificarse a través de la lesión corporal de un bien, resultando importante emplear una noción normativa de daños en la que el centro gravitante radique en la funcionalidad del bien y no en su integridad corporal.

No obstante, desde una visión sistemática de la parte especial del Derecho penal, ha de verificarse que el delito genérico de daños comprendería, como lo hemos sostenido líneas arriba, los daños físicos causados sobre la corporalidad del bien (computadora), a pesar de que se produzca el mismo resultado que en el envío de un virus: destrucción de la información, sobre todo de cara a la pena a ser aplicada. De ahí que un autorizado sector de la doctrina[6] propone que en tales casos sea de aplicación el tipo penal especial.

En igual sentido ha de ser concebida la información en internet como un referente funcional, luego la perturbación ha de recaer sobre información almacenada en la red, información transportada en la red o sobre el contenido de la información en la red.

En definitiva, se trata de una noción normativa de daños referida a la funcionalidad del bien y no a su integridad corporal.

ASPECTOS OBJETIVOS

El delito de daños informáticos acude a la técnica legislativa de enumerar expresamente los objetos materiales sobre los que ha de recaer la acción. Así, en relación con el objeto material de este delito se tiene que está comprendido por una base de datos, un sistema, una red de computadoras, lo cual a su vez encierra los programas o documentos electrónicos. Todos estos elementos pueden ser reconducidos, desde una perspectiva informática, al conjunto de elementos lógicos que requiere un sistema informático: *software*, y al conjunto de elementos materiales que éste también requiere: *hardware*.

Tratándose del delito de daños, se sostiene que el objeto material ha de ser ajeno al autor, salvo el caso de algunas regulaciones que sancionan la sustracción de bien propio a su utilidad social. De todos modos, la tendencia actual es resaltar la dimensión social de la información.

Computerkriminalität – Die neuen Tatbestände der Datenveränderung gem. § 303 a StGB und der Computersabotage gem. § 303 b StGB, Münster, 1989, p. 86.

6 Respecto de un privilegio con relación a las consecuencias jurídicas, González Rus, Protección penal de sistemas, elementos, datos y programas informáticos, *RECPC*, 1, 1990, en [http://www.criminet.ugr.es/recpc], p. 7; con relación al resultado producido, cfr. Mata, *Delincuencia informática*, cit., p. 65.

Por lo general, se deja abierto a la concurrencia de diversos medios de comisión del hecho, por lo que es posible verificar la posibilidad de la realización omisiva de este delito; para ello ha de contarse con una posición de garante en el agente, en la que el obligado tiene el deber de evitar las infecciones de virus informáticos en un sistema determinado, y pese a ser consciente de ello no lo hace.

Un tema de discusión es el relacionado con la destrucción o menoscabo de datos o información que es conservada, además, en copia en otros archivos, esto es, no se llega a perder del todo la información, pues la destrucción real se lleva a cabo recién con la destrucción de la última de las copias existentes. De ahí que para un sector de la doctrina estos supuestos constituyan una tentativa imposible[7], no punible.

Desde una visión funcional del objeto material sobre el que recae la conducta en el delito de daños informáticos, se llega a una solución diferente. La existencia de una copia de la información es una cuestión meramente circunstancial, fenomenológica, no determinante en sentido normativo. Admitir su incidencia normativa significaría tener que preguntarse en todas las destrucciones de archivos si no existe una copia para afirmar la tipicidad de la conducta. Además, se ha de tomar en cuenta que el archivo en concreto, por más copias que puedan existir, posee su propia funcionalidad que se ve afectada por su destrucción; más allá de su integridad corporal (ésta se conserva con la copia), es la funcionalidad del archivo la que recibe el ataque. Por ejemplo, se destruye información colgada en la red, existe una copia, pero determinados usuarios no han podido acceder a la información; luego, se menoscaba la funcionalidad de la información y no su integridad corpórea. Una vez más se evidencia la necesidad de configurar los delitos informáticos, en particular el de daños informáticos, a partir de la dimensión social de la información.

a) Los daños informáticos en la legislación peruana

Este delito se encuentra previsto en el artículo 207-B del Código Penal, y se sanciona a partir de la conducta de intrusismo informático, esto es, el acceso no autorizado a una base de datos o a un sistema informático con el fin de alterarlos, dañarlos o destruirlos.

El consentimiento del titular del bien elimina la conducta típica del acceso indebido, lo cual repercute definitivamente en la atipicidad del delito de daños informáticos. Sin embargo, no se recoge el supuesto en el que el titular consiente en el acceso al sistema pero no respecto de la causación del daño; al haber sido legítimo el acceso, no existiría la conducta base sobre la que se construye el comportamiento de daños, luego éste quedaría impune.

---

7 En este sentido, Mata, *Delincuencia informática*, cit., p. 74.

La construcción peruana de los daños informáticos emplea el recurso a los denominados elementos subjetivos de intención trascendente, en concreto, a aquellos definidos como de resultado cortado, en que el legislador exige sólo la realización de la conducta y prescinde de la producción del resultado.

– La *alteración* del bien ha de ser comprendida como la modificación del estado en que el éste se encontraba, esto es, la manipulación de los soportes lógicos, los datos o programas contenidos en la computadora.

– Por *dañar* se ha de entender que se refiere a la afectación de la cosa sin que represente su inutilización. Constituye el menoscabo del soporte lógico que dificulta su procesamiento, pero que no genera su pérdida definitiva.

– La *destrucción* ha de ser concebida como la inutilización absoluta del bien, es la pérdida del bien.

b) En especial: difusión y transmisión de virus informáticos

Una de las más preocupantes formas de abuso del internet la constituyen los ataques a un sistema de datos ajeno mediante virus informáticos. Su peligrosidad resulta especialmente de la creciente interconexión global de direcciones de datos a distancia vía internet y, unido a ello, de la elevada velocidad del procesamiento de información.

Un virus informático es un código de programa capaz de reproducirse por sí mismo y que puede ejecutar de manera ilegal una función definida, la cual no es deseada por un usuario autorizado[8]. Los programas de virus informáticos presentan por lo general por lo menos dos propiedades funcionalmente separadas entre sí: infección y función[9]. El componente de infección contiene todas las funciones necesarias para la reproducción del virus, como por ejemplo la búsqueda de programas no infectados. El componente de función ejecuta una función (de daños) ya definida con anterioridad.

Al activarse el programa principal del virus informático cómo, uno tras otro, primero el componente de infección, luego el componente de función, después de ello rebota en el programa en el que el virus se ha anidado. El componente funcional se ejecuta principalmente tan pronto el usuario accede al virus; la activación de este componente puede, además, atarse a la entrada o no de una determinada condición desencadenante: la hora, la fecha, la entrada de un *password*, etc. Como consecuencia de la separación de los componentes infección y función, puede incrementarse en el tiempo el programa del virus sin ser descubierto.

---

8 En este sentido, VON GRAVENREUTH, *Computerviren. Technische Grundlagen. Rechtliche Gesamtdarstellung*, 2.ª ed., Köln, Berlin, Bonn, München, 1998, p. 2.

9 Cfr. VETTER, *Gesetzeslücken bei der Internetkriminalität*, Hamburg, 2003, pp. 74 y ss.

El proceso de infección de un virus informático comienza con la búsqueda en la computadora de programas para infectar y sigue con la elección de uno de ellos; allí se implanta y copia por sí mismo su código; a partir de aquí se encuentran varias posibilidades a disposición: en su forma más sencilla el virus informático copia su código al inicio o al final del programa: en el primer caso corre primero el programa del virus y luego el programa seleccionado del computador, y se produce aquí la infección; en el segundo caso es posible que no se active el virus con una previa destrucción del programa infectado. Consecuencia de la infección es que el programa infectado nunca más corra libre de errores.

La peligrosidad de los virus informáticos proviene de su capacidad para poder ejecutar determinadas funciones, pues la rutina de la función puede definirse libremente por el programador, en lo cual no existe prácticamente ninguna barrera. La oferta llega desde funciones con efectos solamente molestosos (la aparición de una determinada palabra en algunas funciones del teclado) hasta funciones con dirección a objetivos que perturban la realización del trabajo (la variación de la composición del teclado). Otros tipos de virus dañan o destruyen datos o archivos en disquettes o discos duros a través del borrado o la sobre-escritura.

Los virus informáticos se propagan, por lo general, sobre un intercambio de programas por medio de soportes de datos, sobre el buzón de correo y especialmente sobre internet[10]. Anteriormente representaban, sobre todo, las copias robadas y los software de dominio público las principales fuentes de propagación de virus; actualmente esta se desarrolla principalmente a través de internet[11], y la masificación de la difusión de virus se presenta a través del correo electrónico y su *attachtment* que es en sí el portador del virus, al ser activado con un doble clic.

Ahora bien, el objeto sobre el que recae la acción en el sabotaje informático es el procesamiento de datos, por ello la perturbación sobre un equipo de procesamiento de datos como tal, sólo es comprendida dentro del sabotaje informático si con ello se ha dañado el correspondiente procesador de datos[12].

c) Aspectos subjetivos

En cuanto al tipo subjetivo, se trata de un delito eminentemente doloso[13]. La posibilidad de la sanción de una difusión negligente de un virus informático no es del *lege lata* posible, debido a que el castigo de las realizaciones culposas sólo procede cuando se

---

10 Cfr. von Gravenreuth, *Computerviren*, cit., p. 20.

11 Cfr. Hofer, Computer- Viren-Herkunft, Begriff, Eigenschaften, Deliktsformen, *Jur-PC*, 1991, pp. 1367 y ss., p. 1369.

12 Cfr. Krutisch, *Strafbarkeit*, cit., p. 156, con mayores referencias.

13 Así, Krutisch, *Strafbarkeit*, cit., p. 162; Vetter, *Gesetzeslücken*, cit., p. 80.

encuentra expresamente recogido en la ley (*numerus clausus*), lo cual no ocurre en la mayoría de legislaciones sobre la materia. Esto es, el delito de sabotaje informático se castiga únicamente en su forma dolosa.

Algunas legislaciones recogen de manera expresa la sanción de la realización imprudente del delito de daños; así el artículo 267 del Código Penal español, bajo ciertas exigencias, como que se trate de una imprudencia grave[14].

Uno de los temas que se plantea, sin embargo, es en qué medida es posible delimitar el dolo eventual respecto de la culpa consciente en determinados supuestos de sabotaje informático: la doctrina tradicional concibe que el autor actuará con dolo eventual si aprueba o se conforma con el resultado, mientras que actuará con culpa consciente si confía en que el resultado típico no sobrevendrá.

EL PERJUICIO

Los perjuicios que van acompañados de los menoscabos de los sistemas de información y los sistemas de comunicación no significan, sin embargo, solamente pérdidas financieras para las empresas implicadas, sino que existe el peligro de que sean detenidos los posteriores desarrollos en el sector tecnológico del que se trate. Pues, la disposición para inversiones en el desarrollo posterior de las tecnologías de la información y la comunicación depende en una considerable medida de la aceptación del usuario y de su confianza en la seguridad y fiabilidad de los sistemas[15].

Uno de los elementos característicos de la criminalidad informática es la considerable elevación de los daños que pueden ser ocasionados por este tipo de comportamientos. Es posible distinguir entre daños directos e indirectos[16]. El elevado número de daños económicos directos que se causan de manera inmediata al patrimonio de los afectados se puede atribuir, entre otros factores, a la permanencia de la conducta en los delitos informáticos, situación que es abiertamente posibilitada mediante el procesamiento electrónico de datos, a través de la repetición programada del daño que tiene como consecuencia que la manipulación de un programa realizada sólo una vez repercuta automáticamente sobre todos los siguientes, sin posteriores intervenciones del autor. Los daños indirectos son, igualmente, considerables y están ligados, por ejemplo, al hecho de que el hacer público el ataque al sistema informático de una empresa trae

---

14 Sobre ello véase, Mata, *Delincuencia informática*, cit., pp. 76 y s., aunque con reparos político- criminales; Moron, *Internet y Derecho penal: hacking y otras conductas ilícitas en la red*, Pamplona, 1999, pp. 60 y s., admite que la forma imprudente no es la realidad que el legislador ha querido encauzar normativamente.

15 En este sentido, Krutisch, *Strafbarkeit*, cit., p. 23.

16 Así, Krutisch, *Strafbarkeit*, cit., pp. 37 y s.

consigo un considerable menoscabo de la confianza e imagen y, como consecuencia, una grave pérdida financiera.

Uno de los temas de discusión en relación con el contenido de la afectación es si ya es posible considerar el menoscabo del mero valor de uso para afirmar la existencia del resultado en el delito de daños informáticos. Si se pone el acento en la funcionalidad del bien, ya se habría producido el resultado, mientras que si se mantiene una noción naturalística sería necesario que el resultado esté acompañado de una afectación material de la cosa.