Víctor Jiménez
Abogado de Hispajuris

RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS: DELITO DE DAÑOS INFORMÁTICOS

Una persona jurídica puede verse imputada por daños informáticos, regulados en los artículos 264 y siguientes del Código Penal. A continuación se exponen las conductas que pueden generar este tipo de situaciones.

Víctor Jiménez

Todas las organizaciones, sean o no de carácter empresarial, pueden ser sancionadas penalmente siempre que se den todos los requisitos que se establecen en el artículo 31 bis y concordantes del Código Penal.

Estos requisitos son los siguientes:

1. Que se constate la comisión de un hecho delictivo por el que la responsabilidad penal de una persona jurídica esté tipificada.

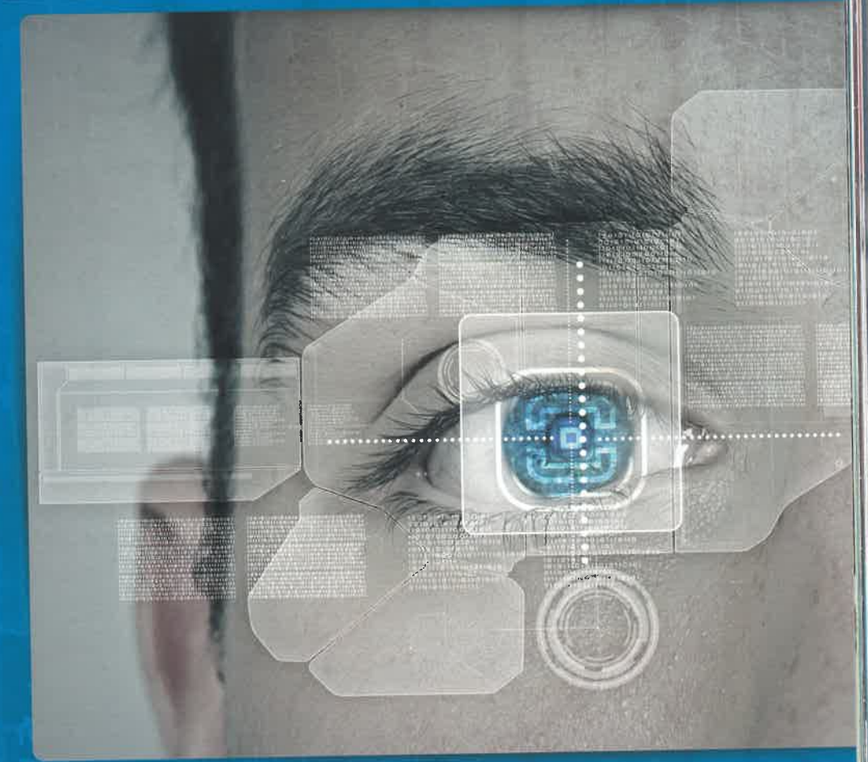
2. Que la persona física autora sea miembro de la organización o la represente de cualquier modo válido.

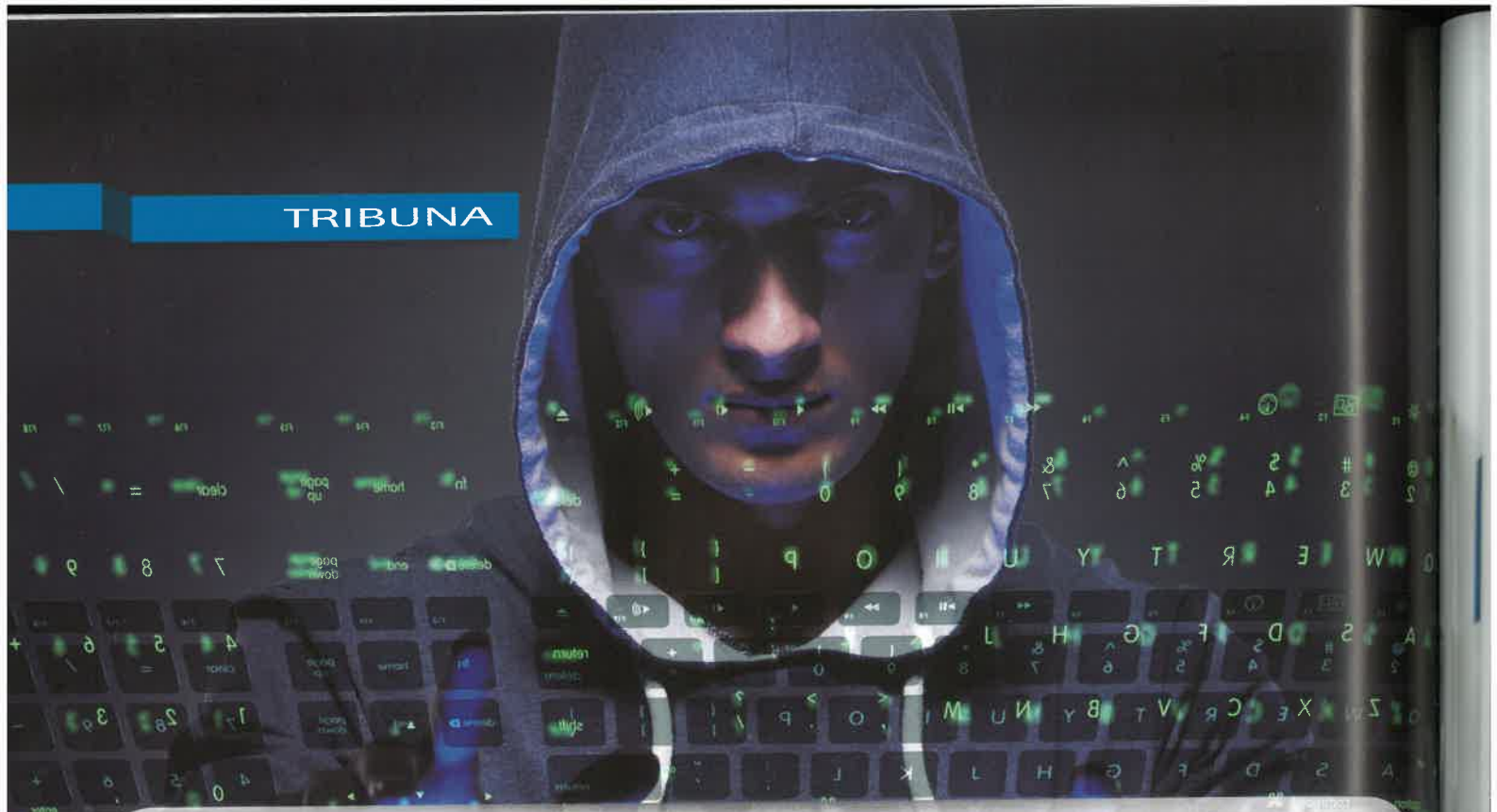
3. Que la entidad reciba algún beneficio directo o indirecto por el hecho en sí y que no cuente con las medidas adecuadas para prevenir la comisión de ese delito en concreto (es decir, un Sistema de *Compliance* penal correcto y completo).

En este contexto, uno de los posibles delitos por los que se puede imputar a una persona jurídica es el de daños informáticos, regulado en los artículos 264 y siguientes del Código Penal. A efectos de los Sistemas de *Compliance*, una organización sólo puede responder por ciertas conductas, aunque no todas. En concreto, las conductas que pudieran generar responsabilidad a una persona jurídica son las siguientes:

- Borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave (siempre que se hubiera hecho sin autorización y de manera igualmente grave). Este es el llamado "tipo básico", y está recogido en el artículo 264 del Código Penal, según la redacción dada por la Ley Orgánica 1/2015.
- Obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno mediante alguna de esas conductas, introduciendo o transmitiendo datos o destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Este tipo, recogido en el artículo 264 bis del Código Penal, es una novedad introducida por la Ley Orgánica 1/2015, a los efectos de trasponer el contenido de la Directiva 2013/40/UE, de 12 de agosto, del Parlamento y del Consejo relativa a los ataques contra los sistemas de información, y de la Convención sobre Ciberdelincuencia de Budapest. Tal como indica la Fiscalía Delegada de Delitos Informáticos de la Fiscalía Superior del Principado de Asturias, se definen las conductas de forma abierta con la finalidad de tratar de incluir toda clase de comportamientos.
- Producir, adquirir para su uso, importar o, de cualquier modo, facilitar a terceros (con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos puntos anteriores) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o bien una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información. La Fiscalía General del Estado indica que la inclusión de este artículo, que también es una novedad de la Ley Orgánica 1/2015, traspone otra sección de la mencionada Directiva 2013/40/UE, de 12 de agosto, del Parlamento y del Consejo (en concreto, su artículo 7). En este caso, la Fiscalía indica que "En los últimos años es cada vez más frecuente detectar programas o herramientas informáticas preparadas específicamente para alterar, dañar o destruir datos o programas informáticos u obstaculizar o interrumpir el normal funcionamiento de un sistema, de tal modo que su única utilidad es precisamente llevar a efecto esas acciones ilícitas (...). Pues bien, la realización de las conductas típicas a efectos de obtener o facilitar a otros la disponibilidad de estos programas, así como también de contraseñas de ordenador, códigos de acceso o datos que permitan el acceso a la totalidad o a una parte de un sistema informático, integrará esta conducta cuando quien así actúe no se encuentre debidamente autorizado para ello y, además se acredite la intención de destinarlos a la comisión de cualquiera de las conductas de daños informáticos anteriormente examinadas".

> *"En los últimos años es cada vez más frecuente detectar programas o herramientas informáticas preparadas específicamente para alterar, dañar o destruir datos o programas informáticos..."*





Es habitual valorar este riesgo penal en las empresas intensivas en tecnologías de la información y las comunicaciones, si bien hay que tener en cuenta, a estos efectos, que únicamente estas tres conductas son susceptibles de hacer que una persona jurídica incurra en responsabilidad penal.

Se excluye, pues, el hecho de destruir, dañar de modo grave, o inutilizar para el servicio, obras, establecimientos o instalaciones de las Fuerzas Armadas o de las Fuerzas y Cuerpos de Seguridad, así como el de borrar o inutilizar los datos informáticos mediante incendio o explosión.

En otras palabras, una persona jurídica no puede responder penalmente por los delitos tipificados en los artículos 265 y 266 del Código Penal, por no estar previsto expresamente.

Debe tenerse en cuenta, además, que los comportamientos penalmente reprochables tanto pueden ser dolosos como meramente imprudentes: en este sentido, el artículo 267 del Código Penal sanciona los comportamientos de todos los artículos anteriores (incluyendo, pues, los mencionados 264 y siguientes de esta norma) si los daños se hubieren producido por imprudencia grave en cuantía superior a 80.000 euros, siempre que haya una denuncia previa de la persona agraviada o su representante legal.

Debe entenderse por ello, pues, que un daño informático cometido por mera imprudencia y que tuviera un valor inferior a 80.000 no sería punible, si bien hay que tener en cuenta que la imprudencia, al tratarse de un elemento subjetivo, debe acreditarse por la parte interesada con el mismo rigor con el que se deben demostrar los hechos objetivos en sede procesal. Es decir, que no basta con alegar imprudencia, sino que ésta debe demostrarse fehacientemente.

Un ejemplo práctico de este delito lo encontramos en el reciente Auto de la Audiencia Nacional 909/2017, de 03 de noviembre. En este caso, una determinada entidad fue acusada, entre otros, por este delito por haber destruido los discos duros de su sede ante la perspectiva de una investigación judicial. La Audiencia Nacional estimó la acusación, apoyando su fallo, fundamentalmente, en estos puntos:

- Se consideró constatada la comisión de un delito informático, puesto que se había destruido información y documentación electrónica que pudiera ser relevante para el proceso por el que se venía juzgando a la organización. Además, la información había sido borrada por parte de un miembro de la misma. Estamos, pues, ante un supuesto del tipo básico de este delito.
- La persona jurídica recibió un beneficio indirecto por ello, dada la importancia que tenían los datos borrados en relación con la instrucción de un procedimiento judicial penal que sí afectaba a la entidad. Recuérdese que, tal como indica la STS 154/2016, de 29 de febrero, la mera expectativa de beneficio ya tiene esta consideración, sin necesidad de que éste sea económico.
- La organización carecía de un Sistema de *Compliance* suficiente; de hecho, se aportó un protocolo de actuación para el borrado de archivos informáticos, pero la Audiencia no lo consideró suficiente a los efectos del artículo 31 bis.5 CP.

Una persona jurídica puede responder por un delito de daños informáticos, aunque sólo en algunas modalidades, y con la particularidad de que responderá aunque los sistemas informáticos fuesen ajenos a la persona física que resultase autor material de los hechos

En conclusión, una persona jurídica puede responder por un delito de daños informáticos, aunque sólo en algunas modalidades, y con la particularidad de que responderá aunque los sistemas informáticos fuesen ajenos a la persona física que resultase autor material de los hechos (por ser titularidad de la organización) pero actuase en beneficio de ésta.