Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1.ª), 183/2024, de 29 de febrero de 2024: sobre la aplicación del sabotaje informático agravado en el contexto del uso de una bomba lógica

1. ALGUNAS CONSIDERACIONES

En ocasiones los juristas recurrimos a la interpretación literal de los textos legales, sin embargo, no pocas veces, la comodidad de resolver las cuestiones complejas a golpe de diccionario o de sentido común no es suficiente para aquellas que desbordan los conocimientos jurídicos, tal como es el caso de las formas delictivas asociadas a las Tecnologías de la Información y las Comunicaciones (TIC). Este es el caso de la primera sentencia del Tribunal Supremo en la cual ha resuelto afirmativamente a la cuestión de si el empleo de una «bomba lógica» en el contexto de un ciberataque automatizado constituye o no una circunstancia agravante del delito de sabotaje contra sistemas informáticos. Antes bien, al comentario de esta jurisprudencia están dedicadas estas líneas.

2. RELATO DEL CASO Y DECISIONES DE LOS TRIBUNALES INFERIORES

El relato que motiva el caso judicial ocurrió el 2 de marzo de 2017. Ese día, Sixto (seudónimo), administrador de red que trabajaba en la Ciudad Financiera del Banco Santander, creó una bomba lógica para atacar los sistemas informáticos de la empresa. Este comando de instrucciones fue programado para activarse el 20 de marzo de 2017, fecha en la cual afectó a los equipos de la entidad financiera, al eliminar la configuración de arranque del sistema operativo Windows 7. Como resultado, 3.168 equipos en toda España se vieron afectados entre el 21 y el 27 de marzo de 2017. Esto causó problemas en 839 oficinas, cuyos perjuicios fueron valorados en 292.237,86 euros.

La Sección Veintinueve de la Audiencia Provincial de Madrid subsumió estos hechos en el delito de sabotaje contra sistemas informáticos del artículo 264 bis, 1, a y c) en relación con el del artículo 264 ter del Código Penal (CP), sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, por el cual se le condenó a 1 año, 9 meses y 1 día de prisión, y se determinó su responsabilidad civil con obligación de pagar una indemnización (Procedimiento Abreviado núm. 1125/2020, sentencia núm. 221/2021, de 22 de abril, y Auto de aclaración, de 27 de julio de 2021). En esta

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 204-210
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

misma sentencia se decidió absolver al acusado respecto a las agravantes del artículo 264.2 apartado 2.° y 5.° CP.

Frente a ello, cada uno de los actores procesales impugnaron la decisión. Así, la Sala de lo Civil y Penal del Tribunal Superior de Justicia de Madrid resolvió, por un lado, desestimar los recursos de apelación del condenado y de la parte civil Santander Global Technology S.L. y, por otro, estimar parcialmente el recurso del Ministerio Fiscal. En consecuencia, Sixto fue condenado por el tipo agravado del artículo 264 bis.2 del CP en relación el artículo 264.2.5, con el efecto de que las penas fuesen incrementadas a tres años de prisión, accesoria de inhabilitación especial para el ejercicio del derecho de sufragio durante el tiempo de condena y con una multa del triple del perjuicio causado ascendiente a 99.552 euros, con responsabilidad personal subsidiaria de un mes en caso de impago (Rollo de Apelación núm. 425/202, 24 de noviembre de 2021).

Esta última decisión fue recurrida por el condenado a través de un recurso de casación, alegando la infracción de preceptos constitucionales y legales, lo que resultó en la sentencia número 183/2024, emitida el 29 de febrero de 2024.

3. CONTROVERSIA SUSTANTIVA Y POSTURA DEL TRIBUNAL SUPREMO

El escrito del recurso de casación alegó tres motivos. Dos de ellos referidos a la infracción de garantías procesales relacionadas con la valoración de la prueba documental y la debida motivación de la decisión judicial, los cuales fueron desestimados por el Tribunal Supremo, al considerar que la decisión del Tribunal Superior era razonable y justificada. El tercero, concerniente al juicio de tipicidad respecto al empleo de una «bomba lógica».

El recurrente cuestionó que no debió aplicársele la agravante del artículo 264 bis. 2 del CP, el cual a su vez remite al artículo 264.2.5 y luego al artículo 264 ter a), ya que considera que la bomba lógica no constituye un «programa informático» según lo estipulado en el texto legal. No obstante, este motivo también fue desestimado.

Sobre esta última controversia, el Tribunal Supremo se remitió al razonamiento judicial elaborado por la Audiencia Provincial, en cuya sentencia plasmó tanto el Convenio sobre Ciberdelincuencia de Budapest, del 23 de noviembre de 2001 (artículo 1), como la Directiva 2013/40/UE, del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (considerando 16), que ofrecen definiciones de lo que es un programa informático. Sobre el cual se afirma que «se incluye dentro del concepto de dato informático, pudiendo aquel definirse como un conjunto de líneas de código, o lo que es lo mismo, un conjunto de instrucciones escritas en algún lenguaje de programación [...]». A dicha conceptualización, el Supremo define «bomba lógica» como «un programa informático (un conjunto de líneas de

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 204-210
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

código) que se instala en una computadora y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción. Es un programa maligno que se activa al momento de realizar una acción, enviar un e-mail, ingresar a alguna aplicación, etc. [...]».

A partir de dicho análisis infiere que la bomba lógica que se insertó en el script «REBOOT.VBS» de la máquina central del banco y que desencadenó la inoperatividad de los ordenadores, según informe emitido por la firma Deloitte, es un programa informático y, por tanto, su utilización como medio para cometer el delito de sabotaje contra sistemas informáticos configura la modalidad agravada del apartado a) del artículo 264 ter CP.

Como resultado de esta interpretación, se confirmaron las penas impuestas al condenado. En sentido contrario habría correspondido establecer una pena conforme al tipo básico, esto es, de seis meses a tres años.

4. ANÁLISIS CRÍTICO A LA POSTURA DEL TRIBUNAL SUPREMO: ÉRASE UNA VEZ UNA BOMBA LÓGICO-JURÍDICA... QUE NO ESTALLÓ

4.1. En primer lugar, resulta fundamental tener una comprensión clara de las leyes penales aplicadas al caso. De acuerdo con la sentencia núm. 221/2021, de 22 de abril, la Audiencia Provincial subsumió los hechos en el artículo 264 bis, 1, a y c) CP en relación con el del art. 264 ter a), empero, absolvió por las agravantes del artículo 264.2 apartados 2.° y 5.°. Al respecto, la absolución respecto al apartado 5.° y la condena por la agravante del artículo 264 ter a) del CP resulta contradictoria, dado que la referencia a esta última solo sería procedente si se aplicara la primera. Por ello, es coherente que la Sala de lo Civil y Penal corrigiera esta inconsistencia, determinando de manera global que los hechos se encuadran en el artículo 264 bis, apartado 1, a y c), y apartado 2 que remite al artículo 264.2.5 y a su vez al artículo 264 ter a) del CP.

Ciertamente, la técnica legislativa de estas modalidades típicas, desarrollada por la Ley Orgánica 5/2010 y la Ley Orgánica 1/2015, suele resultar confusa. Por lo cual, es fundamental mantener la claridad en cuanto a la imputación penal para evitar posibles equívocos.

4.2. Entrando en la cuestión principal, cabe señalar que la interpretación del Tribunal Supremo sobre la aplicación de la agravante del artículo 264 ter a) del Código Penal plantea dudas en cuanto a su compatibilidad con el principio de *non bis in ídem*, así como el principio de proporcionalidad de las penas.

La razón principal radica en que el Supremo realiza exclusivamente una interpretación literal, dejando fuera de consideración que se trata efectivamente de un subtipo agravado. Esta técnica legislativa, en su lógica-sistemática, implica sancionar con

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 204-210
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

mayor rigor aquellos comportamientos típicos que reúnan ciertas circunstancias que influyan en su grado de lesividad. En este sentido, el alcance y el significado que se le deben atribuir a la agravante, por un lado, deben permitir distinguirse de los supuestos comprendidos por el tipo base y, por otro lado, deben fundar dicha distancia en un criterio cualificado de lesividad.

La primera de esas condiciones es una expresión del *non bis in ídem* material. El cual se define como el límite al doble castigo cuando hay coincidencia en el sujeto, los hechos y el fundamento jurídico. Al respecto, la jurisprudencia constitucional incorpora este principio en el artículo 25 de la Constitución española, que garantiza el derecho a la legalidad (STC 91/2008, de 21 de julio). En tanto, la segunda condición se refiere a los fundamentos de la determinación penal, ya que cada circunstancia de agravación se basa en razones y criterios lógicos que justifican su inclusión [BORJA JIMÉNEZ, E. 2015: *La aplicación de las circunstancias del delito: actualizado a la reforma 2015*. Valencia: Tirant lo Blanch, 25].

4.3. Destaca el sentido literal que el Tribunal Supremo le atribuye a su interpretación cuando argumenta con base a las definiciones de los instrumentos internacionales y multinivel, las cuales permiten concluir que, efectivamente, la categoría de «bomba lógica» queda comprendida bajo el concepto técnico de programa informático. No obstante, procede a aplicar una circunstancia agravante sin explicar de qué manera se justifica un reproche más severo respecto a la modalidad básica, la cual ya contempla el supuesto de manipulación de programas informáticos[1]. En este punto se aprecia la insuficiencia en la argumentación judicial, ya que no aporta un contenido diferenciado al subtipo agravado.

4.4. Para una mayor claridad, la doctrina especializada y, en particular, la Fiscalía General, a través de su Circular 3/2017, se han pronunciado sobre la interpretación del artículo 264 ter a) del CP. Al respecto, se afirma que dicho artículo puede ser considerado tanto en su forma básica (delito de abuso de dispositivos) como en su variante agravada (cuando se aplica vía remisión del artículo 264.2.5).

Su incorporación como tipo base responde al artículo 6 del Convenio de Budapest y al artículo 7 de la Directiva 2013/40/UE, en los cuales se propone sancionar penalmente la posesión de determinados instrumentos que puedan utilizarse para la comisión de delitos contra datos y/o sistemas informáticos [ANDRÉS DOMÍNGUEZ, A. 2015: «Comentario previo a los artículos 264, 264 bis, 264 ter, 264 quater, 265, 266, 267».

1. El tipo base prevé una sanción penal para «el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior [art. 264.1] […]». Las cuales son que «por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos».

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 204-210
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

En M. Gómez Tomillo (ed.): *Comentarios prácticos al código penal. Delitos contra el patrimonio y socioeconómicos (artículos 234-318 bis)*. Pamplona: Aranzadi, 361]. Para algún sector de la doctrina, esto constituye la criminalización de un acto preparatorio bajo la forma de un delito de mera actividad [CORCOY BIDASOLO, M. 2015: «Capítulo IX. De los daños». En M. Corcoy Bidasolo y S. Mir Puig (eds.): *Comentarios al código penal. Reforma LO 1/2015 y LO 2/2015 (versión online)*. Valencia: Tirant lo Blanch, 925; RODRÍGUEZ MESA, M. 2017: *Los delitos de daños. Capítulo IX del título XIII del CP tras la reforma de la LO 1/2015*. Valencia: Tirant lo Blanch, 96]. En tanto, su incorporación como agravante en los artículos 197 y 264 sería una innovación legislativa, ya que lo establecido en la LO 1/2015 excede lo dispuesto en la normativa europea.

4.5. Antes bien, la descripción «programas informáticos concebidos o adaptados para cometer delitos» resulta de amplio alcance. Empero, tal como se establece en la parte considerativa de la directiva antes citada, resulta evidente que esta expresión de política criminal comunitaria y nacional tiene como escenario de referencia los ciberataques mediante la propagación de *malware* (programas dañinos). Bajo esa lógica, y con base en el contexto y la singularidad de esta forma de criminalidad, se entiende que tales programas habrían de consistir en aquellos objetivamente elaborados para tales fines [Rodríguez Mesa, M. 2017: *Los delitos de daños. Capítulo IX del título XIII del CP tras la reforma de la LO 1/2015.* Valencia: Tirant lo Blanch, 95]. De la misma opinión es la Circular 3/2017, en dónde se recurre a una definición de *malware* elaborada por el Instituto Nacional de Ciberseguridad.

Entre la tipología de malwares más conocidos se cuenta a los virus, gusanos, troyanos, *bots*, *botnets*, *ransomware*, *spyware* y *cryptojacking*. Aunque realmente la definición de *malware* más común alude a la intencionalidad de su empleo, por ello, su alcance puede resultar tan vasto que puede terminar comprendiendo cualquier *software* o fragmento de código. En este sentido, el concepto técnico en sí mismo no sería suficiente para delimitar el ámbito de aplicación de la ley, sino que haría falta atender a criterios de lesividad para dotarle de razonabilidad al artículo 264 ter a).

4.6. Dicha perspectiva de interpretación resulta compatible con la agravante de los sabotajes informáticos objeto de estudio, pues significaría que el acto reviste una mayor lesividad por la utilización de un instrumento u objeto (in)material especialmente desarrollado para tales fines. En particular, conviene subrayar que los *malwares* pueden revestir distintas funcionalidades y propagarse de modo masivo o dirigido, según las instrucciones bajo las que fuesen programados. Inclusive es posible que el agente aproveche la programabilidad de las herramientas informáticas para que el *malware* se autoejecute, y valerse de su capacidad de replicarse e infectar otros[2].

2. Un caso que ejemplifica lo anterior fue el ataque masivo a escala mundial del *malware* WannaCry, desarrollado y programado de modo tal que, cada vez que infectaba un ordenador, debía ejecutar de modo inmediato un conjunto de programas orientados a tareas específicas.

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 204-210
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

Es decir, ciertos *malwares* constituyen una forma más sofisticada y alevosa para cometer el acto delictivo, ya que, bajo esta modalidad, el sujeto activo lleva a cabo las operaciones necesarias para que el código malicioso y sus herramientas informáticas activen distintas técnicas de ofuscación y con ello burlen los controles de antivirus o demás medidas de protección en el sistema informático de la víctima, y tengan éxito en su misión de afectar el sistema informático de la víctima.

4.7. Siendo así, nuevamente, la controversia se orienta a establecer si una «bomba lógica» tiene las características para considerarse no solo un programa informático o un *malware*, sino un instrumento con entidad suficiente para justificar un incremento de la sanción punitiva respecto de la modalidad básica. Esta cuestión sería merecedora de una exploración por las categorías del bien jurídico penalmente protegido, resultado típico, lesividad y dañosidad, etcétera, y, particularmente, para los delitos de sabotajes contra datos y sistemas informáticos, examinar los contornos del llamado requisito de la doble gravedad (gravedad de la acción y del resultado).

Es en este punto donde el análisis del Tribunal Supremo tuvo la oportunidad de explorar importantes aspectos sustantivos de esta figura delictiva. Sin embargo, esto no se logró, ya que su interpretación se limitó al sentido semántico del enunciado legal. Como resultado, la justificación de la aplicación de la agravante queda pendiente, lo que genera cuestionamientos en relación con el principio de proporcionalidad de las penas. En este caso, se advierte que hubiera sido adecuado mantener la subsunción en la modalidad básica y absolver en el extremo de la agravante.

5. CONCLUSIONES

El Tribunal Supremo tuvo la ocasión de profundizar en aspectos sustantivos de la figura delictiva del sabotaje informático agravado. Sin embargo, la interpretación de la sala se circunscribió predominantemente al sentido literal y fragmentado del enunciado legal, dejando de lado un análisis más profundo que podría haber esclarecido importantes cuestiones doctrinales y jurisprudenciales.

La carencia de un análisis robusto trae consigo una consecuencia significativa: la aplicación de la agravante queda pendiente de una justificación clara. Esto plantea serios cuestionamientos respecto al principio de proporcionalidad de las sanciones penales.

El Tribunal hubiera podido, y tal vez debido, abordar la cuestión desde una perspectiva más holística, considerando no solo la subsunción a la definición de programas

Así, estaba compuesto por un *software* de infiltración, otro de escaneo de discos para localizar archivos con determinado formato, otro de encriptación y, asimismo, una plataforma web donde comunicar el pago del rescate y solicitar la descodificación de los ficheros.

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 204-210
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

informáticos, sino la necesaria interpretación sistemática de los subtipos agravados. Tal enfoque habría permitido una aplicación más matizada y justificada.

Existe una necesidad de clarificar y definir con precisión conceptos clave como programa informático y *malware* en el escenario de los delitos de sabotajes informáticos, para evitar interpretaciones ambiguas y garantizar una aplicación coherente de la ley en futuros casos similares.

En vista de la falta de justificación adecuada de la agravante, habría sido más coherente con los principios del derecho penal absolver al acusado de la agravante y mantener la subsunción del hecho en la modalidad básica del delito de sabotaje informático. Este enfoque no solo habría respetado el principio de proporcionalidad, sino que también habría proporcionado una guía más clara y precisa para futuras interpretaciones jurídicas en casos similares.

Wendy REQUEJO-PASSONI
Graduada en Derecho
Máster en Derecho Penal
Doctoranda
Universidad de Salamanca
wrequejopassoni@usal.es

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 204-210
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA