LA GUERRA CONTRA EL *RANSOMWARE*: CÓMO EL CÓDIGO PENAL ENFRENTA UNA NUEVA AMENAZA DIGITAL

Zaira Gutiérrez Vázquez
Estudiante del. Master de Acceso y la Procura

RESUMEN

Actualmente, la sociedad se enfrenta a un aumento en los riesgos y amenazas a la seguridad originados por el paso del entorno físico al entorno digital. Este cambio ha propiciado que la ciberdelincuencia destaque como un área de interés para las distintas áreas del Derecho. Lógicamente, el Derecho Penal no ha permanecido al margen. Esta investigación explora la amenaza emergente que representa la ciberdelincuencia, con un enfoque particular en el fenómeno del *ransomware*. Esta clase de ciberataque, que se caracteriza por el secuestro de información y sistemas informáticos a cambio de rescates económicos, ha ganado notoriedad por su severidad. Sin embargo, en el contexto español, la respuesta legal a estos actos delictivos aún no está claramente articulada. Hasta ahora, solo existen dos sentencias relevantes de la Audiencia Nacional, ambas alcanzadas por conformidad, sin discusión de los fundamentos de la condena. Este estudio analiza la posible tipificación del *ransomware* como una versión contemporánea del delito de daños y del delito de extorsión.

I. INTRODUCCIÓN

El crimen de alta tecnología ha adquirido proporciones epidémicas que plantean una amenaza a la seguridad a escala global. Aunque es innegable la importancia de Internet como uno de los hallazgos más significativos de nuestro tiempo, la expansión de este fenómeno ha revelado no solo un progreso real a nivel social, sino también el surgimiento de nuevas formas de criminalidad y perpetración del delito: la ciberdelincuencia. Este fenómeno constituye uno de los desafíos más complejos que se han enfrentado hasta la fecha en el ámbito de la seguridad tanto a nivel nacional como internacional, lo que ha llevado a que la ciberseguridad se haya establecido como uno de los principales objetivos del siglo XXI.

La naturaleza y el impacto de la ciberdelincuencia van más allá de la esfera física, infligiendo a sus víctimas perjuicios que trascienden lo tangible. La transición hacia el ciberespacio de los modos operativos confiere a esta modalidad delictiva características distintivas: la complejidad en la atribución de responsabilidad debido a la ilusión de anonimato; su naturaleza transfronteriza, desafiando las nociones tradicionales de jurisdicción y *locus delicti*; y su capacidad para impactar simultáneamente a un amplio espectro de víctimas, comprometer sus sistemas y orquestar ataques con precisión quirúrgica. Así, el delito en el entorno digital –aunque comparta similitudes con los delitos tradicionales–, añade una mayor gravedad a las conductas, lo que se traduce en una potencial elevación de la antijuridicidad en determinadas situaciones.

El presente estudio se centra en el fenómeno del *ransomware*, es decir, la inserción de un *software* malicioso en un sistema operativo con el propósito de obtener acceso al sistema y a los datos, para posteriormente secuestrarlos. El incremento de estos ataques ha puesto de relieve la urgente necesidad de una respuesta jurídica adecuada que permita una efectiva prevención y persecución de estos delitos. En este sentido, solo existen dos sentencias relevantes emitidas por la Audiencia Nacional, Sala de lo Penal, Sección 4ª: la N.º 14/2016, de 3 de marzo, y la N.º 28/2016, de 4 de julio, alcanzadas por conformidad. Así, el objetivo es llevar a cabo un análisis exhaustivo de la potencial tipificación del *ransomware*, incluyendo su consideración como delito de daños o delito de extorsión.

II. RANSOMWARE

El *malware* es un software malicioso que incluye una amplia gama de programas, como virus[1], gusanos[2], bombas lógicas[3], caballos de Troya[4], registradores de teclas[5], programas

[1] Un virus es un *software* malicioso que se adjunta a programas o archivos legítimos para ejecutarse y propagarse cuando estos se abren. Requiere intervención humana para su activación.
[2] Un gusano es un *software* malicioso que se replica y propaga automáticamente a través de redes y sistemas sin intervención humana. Explota vulnerabilidades para infectar otros dispositivos, causando daños como sobrecarga de sistemas y robo de información. A diferencia de los virus, no necesita adjuntarse a programas existentes para ejecutarse.
[3] Una bomba lógica es un *software* malicioso que se activa cuando se cumplen ciertas condiciones predefinidas, como una fecha específica o una acción particular del usuario.
[4] Los caballos de Troya son programas maliciosos que se disfrazan de *software* legítimo para engañar a los usuarios y lograr que los instalen.
[5] Los registradores de teclas son programas maliciosos que capturan y registran cada pulsación de tecla realizada en un teclado. Su propósito es recopilar información confidencial, como contraseñas, datos bancarios y otros datos sensibles.

zombis[6] y puertas traseras[7]. Una subcategoría del *malware* es el "*scareware*", que explota el miedo de las personas a que se revele su información privada, se pierdan datos críticos o se dañen irreversiblemente sus dispositivos. El *ransomware* es, precisamente, un tipo específico de *scareware*. Es una categoría de *software* malicioso que, al ejecutarse, deshabilita de alguna manera la funcionalidad de un dispositivo electrónico, funcionando esencialmente como una versión digital del secuestro. El *ransomware* también se clasifica como un tipo de *software* viral, agrupado en "*familias*" y diferenciándose según si solo presenta amenazas superficiales o representa un problema real. Los tipos de *ransomware* que constituyen una amenaza real se dividen en dos grupos principales: variantes de "*uso único*" empleadas de manera *ad hoc* y *software* que sirve como una extensión de una infraestructura criminal más amplia en la que las víctimas pagan un rescate.

Comenzando con la mecánica funcional del *software*, los ataques de *ransomware* se clasifican según las técnicas y mecanismos que utilizan para infectar y afectar a los sistemas. Las variantes iniciales eran principalmente de bloqueo. En líneas generales, el *ransomware* de bloqueo restringe el acceso del usuario a los sistemas infectados bloqueando la interfaz o los recursos informáticos dentro del sistema, negando así el acceso al dispositivo electrónico o a los archivos. Así, se muestra un mensaje que exige un pago para restaurar la funcionalidad, lo que lo hace parecerse a otras variantes, pero opera de manera muy diferente[8].

En este sentido, si el sistema operativo de la víctima se imagina como una unidad de almacenamiento, donde el valor del sistema operativo radica en los elementos contenidos dentro de la unidad, el *ransomware* de bloqueo opera cambiando efectivamente la cerradura de la puerta, o, en algunos casos, el mecanismo por el cual la cerradura se activa. Los elementos dentro de la unidad de almacenamiento –es decir, los datos–, permanecen intactos, y se le pide a la víctima que pague para desbloquear la puerta (o para restaurar el mecanismo de bloqueo a su forma original en su caso). No obstante, lo más importante es que las víctimas de *ransomware* de bloqueo tienen otras opciones para recuperar el

[6] Los programas zombis, también conocidos como *bots*, son programas maliciosos que infectan dispositivos y los convierten en "*zombis*" o "*bots*" controlados de manera remota por un atacante. Estos dispositivos infectados forman parte de una red más grande conocida como botnet.
[7] Las puertas traseras son métodos secretos de acceso a un sistema informático, red o aplicación que eluden los procedimientos de autenticación normales. Los atacantes utilizan puertas traseras para obtener acceso no autorizado a sistemas comprometidos, permitiéndoles controlar el sistema.
[8] Ramsey, I. T., & Morse, E. A. (2016). *Ransoming data: Technological and legal implications of payments for data privacy*. Cyberspace Law Committee Winter Working Group, 7-10.

acceso, como intentar esquivar la puerta perforando la cerradura, quitando la puerta de sus bisagras o simplemente quitando las paredes que rodean el contenido de la unidad.

En la actualidad, las técnicas criptográficas aplicadas al *ransomware* operan de manera diferente, aunque el mensaje inicial—"*páganos o no podrás acceder a tus datos*"—parece igual a primera vista. En lugar de centrarse únicamente en bloquear el acceso, estas variantes emplean un enfoque conocido como *ransomware* criptográfico. En este caso, el *ransomware* cifra archivos en el sistema objetivo, de modo que el equipo informático sigue siendo utilizable, pero los usuarios no pueden acceder a sus datos[9].

Siguiendo con la metáfora de la unidad de almacenamiento, el *ransomware* criptográfico puede o no alterar la cerradura de la puerta principal. En su lugar, evalúa cada elemento dentro de la unidad, determinando el valor relativo de los archivos para el usuario, es decir, fotos personales, documentos de Word, archivos de Excel o PDFs. Una vez identificados, el programa cifra cada archivo, haciéndolo inutilizable hasta que se pague el rescate. Con este ataque, no hay opción de perforar la cerradura, quitar la puerta de sus bisagras o derribar la pared; cada archivo está bloqueado por separado e indefinidamente.

III. EL RETO DE TIPIFICAR LOS ATAQUES *RANSOMWARE*

Puesto que nos enfrentamos a un delito relativamente nuevo, surge la interrogante sobre cómo clasificar este tipo de conductas delictivas. En particular, nos preguntamos si estas acciones pueden encuadrarse dentro de los tipos delictivos ya existentes en nuestro Código Penal. Se consideran dos ámbitos de acción legal potencialmente aplicables: el delito de daños informático, que se centra en la alteración malintencionada de sistemas y datos; y la extorsión, caracterizada por la coacción para obtener beneficios económicos. La elección de estos tipos delictivos se basa en la similitud del ataque *ransomware* con estos delitos especificados en el Código Penal, así como en las únicas dos sentencias relevantes sobre *ransomware* en España sentencias de la Audiencia Nacional, Sala de lo Penal, Sección 4ª, N.º 14/2016, de 3 de marzo, y N.º 28/2016, de 4 de julio.

Las dos sentencias mencionadas están relacionadas con el *ransomware* conocido como "*virus de la policía*", fechadas el 3 de marzo[10] y el 4 de julio de 2016[11]. En este ataque *ransomware* se presentaban mensajes falsificados simulaban ser enviados por las

[9] Pollack, D. (2016). *Trading in fear: The anatomy of ransomware*. ID Experts.
[10] Sentencia de la Audiencia Nacional 14/2016 (Sala de lo Penal), de 03 de marzo de 2016.
[11] Sentencia de la Audiencia Nacional 28/2016 (Sala de lo Penal), de 04 de julio de 2016.

Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE), utilizando logotipos y elementos gráficos oficiales para aumentar su credibilidad. Las víctimas eran acusadas de participar en actividades ilegales en línea, tales como el intercambio ilícito de archivos, el acceso a material de abuso infantil o la visita a sitios web asociados con actividades terroristas. Estas acusaciones generaban un sentimiento de miedo e incertidumbre, impulsando a las víctimas a actuar rápidamente para evitar consecuencias legales. El mensaje incluía instrucciones precisas para pagar un supuesto "*multa*" o "*rescate*" a través de métodos de pago difíciles de rastrear, como tarjetas de prepago o criptomonedas.

El Ministerio Fiscal calificó los hechos atribuidos a un total de 11 acusados como constitutivos de los siguientes delitos:

1) Delito continuado de estafa: según los artículos 248, 250.6º y 74 del Código Penal, en concurso medial con el artículo 77, con un delito de daños informáticos del artículo 264, apartados 2 y 3.1 del Código Penal. Los daños informáticos se produjeron debido al uso de *malware* que bloqueaba el acceso a los datos, cuestión relacionada íntimamente con el *ransomware* per se.
2) Delito de blanqueo de capitales: conforme al artículo 301 del Código Penal.
3) Delito continuado de falsedad en documento mercantil: de los artículos 392.1, 390.1º, 2º y 74 del Código Penal.
4) Delito de pertenencia a organización criminal: según el artículo 570 bis, apartados 1 y 2.c) del Código Penal, al tratarse de una estructura organizada de carácter delictivo.
5) Delito contra la intimidad: conforme al artículo 197.2 del Código Penal, ya que, al tomar control de los ordenadores, tuvieron acceso a toda la información personal almacenada en ellos, incluyendo datos sensibles como correos electrónicos, documentos privados, y cualquier otra información confidencial que se encontrara en los dispositivos.
6) Usurpación de funciones públicas: según los artículos 402 y 402 bis del Código Penal.

De la jurisprudencia analizada, el único delito que se vincula de manera directa con el *ransomware* es el de daños informáticos. Esta relación se establece porque, a través de la introducción del *malware*, los ciberdelincuentes lograron hacer inaccesibles los datos

almacenados en el sistema. El ransomware bloquea el acceso a la información, impidiendo que los usuarios legítimos puedan utilizar sus datos hasta que se pague un rescate.

IV. ¿DELITO DE DAÑOS O EXTORSIÓN?

A. DELITO DE DAÑOS

La pregunta es, ¿pueden realmente contemplarse los ciberataques *ransomware* como una manifestación contemporánea del delito de daños? Gran parte de la academia apoya esta opción para la tipificación de este nuevo delito[12]. El artículo 264.1 CP sanciona con pena de prisión a quien, *"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, cuando el resultado producido fuera grave".*

La doctrina está dividida en cuanto al bien jurídico que debe protegerse. La mayoritaria opina que se debe proteger la propiedad[13], mientras que otros abogan por la protección de la utilidad de la información almacenada en los datos o documentos del sistema informático[14]. En mi opinión, el bien jurídico protegido no solamente abarca derechos materiales, como ocurre en el delito de daños convencional, sino también la información contenida en sistemas informáticos. En otras palabras, se puede tener derecho de propiedad sobre el *hardware* que contiene los datos atacados o derechos de propiedad intelectual sobre programas y bases de datos específicos y no poseer derechos de propiedad sobre los propios datos almacenados en el sistema y viceversa.

El tipo objetivo se refiere a los sujetos implicados y a la conducta delictiva. El sujeto activo incluye a cualquier persona que dañe los componentes de un sistema informático, ya que se trata de un delito común. En el contexto del *ransomware*, el sujeto activo es cualquier persona que utiliza *software* malicioso para comprometer un sistema informático (i.e., un ciberdelincuente que infecta el sistema de la víctima). El sujeto

[12] Barrio Andrés, M. (2018). *Ciberdelitos 2.0*. Wolters Kluwer.
[13] González Rus, J. J. (2007). Precisiones conceptuales y político-criminales sobre la intervención penal en Internet. In VVAA, *Delito e informática: algunos aspectos. Cuadernos penales José María Lidón* (No. 4, pp. 33). Universidad de Deusto.
[14] *Vid.* De la Mata Barranco, N. J., & Hernández Díaz, L. (2009). *El delito de daños informático, una tipificación defectuosa*. Estudios penales y criminológicos, (29), p. 326 y Corcoy Bidasol, M. (1990). *Protección penal del sabotaje informático*. Especial consideración de los delitos de daños. Diario La Ley, (1), pp. 1000-1016.

pasivo, por su parte, es el propietario del sistema informático afectado, que puede ser una persona, empresa o cualquier entidad con datos.

Por otra parte, el "*daño*" en el sabotaje informático se aleja de la tradicional noción de destrucción física permanente, adoptando un concepto funcional de la propiedad que trasciende la simple indemnidad del "*cosa*"[15]. La conducta delictiva incluye acciones como borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos, programas o documentos electrónicos ajenos. Así, se pretende abarcar una amplia gama de conductas, que aunque parecen sinónimas, se refieren a escenarios distintos. De esta manera, "*borrar*" implica que los datos desaparecen visualmente, pero siguen existiendo en el sistema y pueden recuperarse, mientras que "*suprimir*" se refiere a la eliminación total de la información del sistema[16]. En cambio, el término "*alterar*" significa cambiar la esencia o forma de algo, dañarlo o descomponerlo, y puede incluir la eliminación parcial o la adición de nuevos datos que cambien su contenido original.

Siguiendo este argumento, la acción de hacer inaccesibles los datos, programas o documentos informáticos incluye situaciones en las que, sin destruirlos o dañarlos, se impide el acceso a ellos para cualquier uso. Estas acciones afectan principalmente a los datos y programas, no a los dispositivos físicos (*hardware*) que los soportan[17]. El problema subyacente en el delito de daños informáticos es que no repercute directamente en los objetos materiales que almacenan la información, sino que afecta a la disponibilidad de la información, dañándola, alterándola, suprimiéndola o volviéndola inaccesible, afectando incluso la funcionalidad del programa[18]. En el caso del *ransomware*, los atacantes cifran los datos de las víctimas, impidiéndoles el acceso a su propia información.

La propia Fiscalía General del Estado en su Circular 3/2017 sobre delitos informáticos ha definido que, "*la conducta de hacer inaccesible abarca aquellos supuestos en los que la acción ilícita, ejercida sobre los datos y/o programas informáticos o documentos*

[15] Muñoz Conde, F. (2021). Derecho Penal. Parte especial (23rd ed.). Tirant lo Blanch.
[16] Tejada de la Fuente, E. (2019). La tipificación penal de los ataques a los sistemas de información. In A. Camacho Vizcaíno (Ed.), Tratado de Derecho Penal Económico (p. 917). Tirant Lo Blanch.
[17] Carrasco Andrino, M. (2009). *El acceso ilícito a un sistema informático*. In F. J. Álvarez García (Ed.), La adecuación del derecho penal español al ordenamiento de la Unión Europea. La política criminal europea. Tirant lo Blanch.
[18] Rodríguez Mesa, M. J. (2017). Los delitos de daños. In Capítulo XI del Título XIII del CP tras la reforma de la LO 1/2015. Tirant lo Blanch.

electrónicos, produce como consecuencia, sin afectar a la existencia o esencia de los mismos, la imposibilidad de acceder a ellos ya sea para conocer su contenido, para operar con ellos o, en general, para utilizarlos en cualquier modo. Un buen ejemplo de este efecto es el que produce el programa malicioso conocido como ransomware, que restringe el acceso a determinadas partes o archivos del sistema infectado, generalmente a través de su cifrado, situación que, en principio, solo podría solventarse, y así lo suele plantear el atacante informático, abonando el rescate que con esa finalidad reclama a sus víctimas"[19].

Dicho lo anterior, es de gran importancia matizar que el *ransomware* no busca necesariamente la destrucción o el deterioro irreversible de los datos o sistemas informáticos; sino que su objetivo principal es retener el acceso a estos hasta que se cumplan las demandas económicas de los atacantes. Así, el "*daño*" se utiliza más bien como una herramienta de coacción para exigir un rescate económico.

Asimismo, el tipo penal prevé el requisito de que el daño se produzca sin autorización, ya que quien destruye datos de su propia propiedad no comete delito[20]. Esto introduce una problemática particular en los ciberdelitos, donde a menudo la víctima tiene un papel en la comisión del delito[21]. Muchos ciberataques, incluyendo el *ransomware*, no tienen un objetivo específico hasta que un usuario interactúa con el ataque, convirtiéndose en víctima[22]. En la gran mayoría de ocasiones, la no adopción de medidas de seguridad o sistemas obsoletos, propician estos ataques. En otros tantos, los atacantes utilizan tácticas de ingeniería social para engañar a la víctima y hacer que descargue el *malware*. Esta participación involuntaria proporciona al ciberdelincuente el acceso necesario al sistema informático.

Además, para que se configure el delito, la conducta de sabotaje debe ser considerada "*grave*" y el resultado también debe ser "*grave*"[23]. Este uso de conceptos jurídicos

[19] Fiscalía General del Estado. (2017). Circular 3/2017, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos. https://www.fiscal.es/FIS-C-2017-00003

[20]Juzgado de Instrucción N.º 32 de Madrid. Auto de 30 de octubre de 2013.

[21] Miró Llinares, F. (2011). *La oportunidad criminal en el ciberespacio*. Revista electrónica de ciencia penal y criminología, 13, p., 47.

[22] Miró Llinares, F. (2013). *La victimización por cibercriminalidad social: Un estudio a partir de las teorías de las actividades cotidianas en el ciberespacio.* Revista española de investigación criminológica, p., 11.

[23] Corcoy Bidasolo, M. (1999). *Protección penal del sabotaje informático. Especial consideración de los delitos de daños.* La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía.

indeterminados genera numerosas dificultades en su aplicación práctica. Por ejemplo, la gravedad del daño puede depender de factores como el tipo de datos afectados o si la pérdida de datos es permanente o temporal. Esencialmente, el daño debe tener un impacto patrimonial significativo, requiriendo una valoración económica basada en los perjuicios derivados del delito, más que en el valor del elemento informático comprometido[24]. No obstante, este enfoque hacia la "*gravedad*" de los daños plantea problemas con la seguridad jurídica y frecuentemente resulta en que la conducta quede atípica.

A mi juicio, el *ransomware* si causa "*daños graves*" al hacer inaccesibles los datos. Puede provocar la interrupción total o parcial de dispositivos electrónicos y operaciones comerciales, la pérdida de datos críticos, y la violación de la privacidad y confidencialidad de la información. Sin embargo, es crucial no confundir el daño directo (elemento del tipo penal) con el perjuicio causado, como los costos de limpieza de sistemas, la adquisición de nuevo *software* de protección, y el lucro cesante. Estos conceptos forman parte del perjuicio y pueden reclamarse en la responsabilidad civil, pero no constituyen el daño en sí mismo[25].

El análisis jurídico de los daños informáticos en presencia de copias de seguridad sugiere que, si los datos afectados por ataques como el *ransomware* pueden restaurarse, el delito podría considerarse tentativa, dado que el daño no es permanente[26]. No obstante. si la restauración es compleja y el ataque causa problemas adicionales al sistema, se considera que el daño se ha consumado[27]. A diferencia de los daños materiales, que son permanentes y tangibles, los daños informáticos pueden ser reversibles, aunque esto no disminuye su gravedad, especialmente cuando la recuperación implica costos significativos.

El tipo subjetivo de la conducta delictiva en cuestión se caracteriza por su exclusiva realización mediante la intención dolosa directa o eventual, tanto por parte de personas físicas como jurídicas[28]. En lo que respecta al dolo eventual, la Sala de lo Penal del

---

[24] Barrio Andrés, M. (2011). *Los delitos cometidos en Internet: marco comparado, internacional y derecho español tras la reforma penal de 2010*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario.
[25] Fernández, J. (2022). *El delito de daños en el derecho penal español: Una perspectiva contemporánea*. Revista de Derecho Penal y Criminología, 15(2), pp. 45-67.
[26] López, P. (2020). *El impacto de las nuevas tecnologías en el delito de daños: Una revisión crítica del artículo 264.1 del Código Penal.* Derecho y Sociedad, 35(1), pp. 89-110.
[27] Sentencia de la Audiencia Provincial de Sevilla, 7ª de 30/12/2011.
[28] Barrio Andrés, M. (2018). *Ciberdelitos 2.0.* p. 127.

Tribunal Supremo respecto del delito genérico de daños en su sentencia 97/2004, de 27 de enero *"que éste no exige un dolo especifico; basta con un dolo de segundo grado e incluso un dolo eventual (STS NÚM. 722/95 de 3 de junio [RJ 1995, 4535] y núm. 30/01 de 17 de enero [RJ 2001,397]). Existe el delito de daños, aunque el culpable no buscase directamente la causación de los daños, bastando que los asumiese como resultado o consecuencia muy probable de su acción".* De este modo, la ilicitud de las acciones realizadas sin autorización y de forma grave debe interpretarse como la actuación del autor con pleno conocimiento de su falta de autorización y de que su conducta puede causar un daño significativo a datos, programas informáticos y documentos electrónicos[29]. En este contexto, la intención dolosa de un ataque *ransomware* es clara: los perpetradores actúan con pleno conocimiento de que están realizando una acción ilegal y dañina.

El artículo 264 bis del Código Penal regula la conducta conocida como "*Denegación de Servicio*" (DoS), una variante del delito de daños informáticos. Este artículo se centra en quienes, sin autorización y de manera grave, obstaculicen o interrumpan el funcionamiento de un sistema informático ajeno a través de la introducción o transmisión de datos, o la destrucción de sistemas informáticos, tal como se describe en el artículo 264. La pena básica para estas conductas es de prisión de seis meses a tres años[30]. Existe una diferencia clave entre el artículo 264 y el artículo 264 bis: el artículo 264 se enfoca en la destrucción o inaccesibilidad de datos y sistemas, mientras que el artículo 264 bis se centra en la interrupción del funcionamiento de sistemas informáticos[31], que se alejaría completamente de la conducta del ciberataque analizado.

Por último, el artículo 264 ter, que también es un subtipo del artículo 264, tipifica el acto de facilitar la comisión de las conductas reguladas en los dos artículos anteriores. En este sentido, se considera delito cuando un individuo, sin la debida autorización, proporciona a terceros: a) un programa informático diseñado para cometer alguno de los delitos mencionados en los artículos 264 y 264 bis; o b) una contraseña de ordenador, código de acceso u otra información similar que permita acceder total o parcialmente a un sistema de información. Además, si alguna de las conductas ilícitas descritas en los

[29] Florea, A. A. (2022). *Aspectos fundamentales del delito de daños informáticos y responsabilidad penal corporativa*. Universidad de Deusto.
[30] Rodríguez Mesa, M. J. (2017). *Los delitos de daños*. Capítulo XI del Título XIII del CP tras la reforma de la LO 1/2015. Tirant lo Blanch.
[31] *Vid.* Florea, A. A. (2022), 60.

tres artículos anteriores es cometida por una persona jurídica, se aplicará el artículo 264 quater, que establece las penas correspondientes para este tipo de entidades[32].

En conclusión, podría ser acertada la tipificación un ataque de *ransomware* como un delito de daños contemporáneo, al abarcar el artículo 264 del Código Penal tanto la destrucción física como la inaccesibilidad a los datos debido a la manipulación no autorizada. No obstante, aunque estas conductas se subsuman mayoritariamente en el delito de daños informáticos, no colma todo el injusto del propio ataque. Desde mi perspectiva, el *ransomware*, además de ser un delito en sí mismo, constituye un medio o instrumento para la posible comisión de otros que deben ser también tenidos en cuenta, como es el caso del delito de extorsión[33].

B. EXTORSIÓN

El artículo 243 del Código Penal regula el delito de extorsión, castigando al que "*con ánimo de lucro, obligare a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero, será castigado con la pena de prisión de uno a cinco años, sin perjuicio de las que pudieran imponerse por los actos de violencia física realizados*"[34].

Así, se ensambla como un delito pluriofensivo, afectando a múltiples bienes jurídicos como la libertad, el patrimonio y la integridad física de la víctima. Además, se comete mediante el uso de violencia o intimidación para doblegar la voluntad del sujeto pasivo con el objetivo de causarle un perjuicio patrimonial. A pesar de esto, su naturaleza es principalmente patrimonial[35] debido a la necesaria concurrencia del ánimo de lucro[36]. Se considera un delito de encuentro forzado[37]. En esta modalidad, el sujeto pasivo es obligado a facilitar la creación y entrega de un documento que incorpora un valor

[32] Corcoy Bidasolo, M. (1999). *Protección penal del sabotaje informático. Especial consideración de los delitos de daños.* La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía.
[33] Velasco, E. [Canal vLex]. (2023). I Congreso de Ciberseguridad: El valor de proteger la información, las personas y las empresas. [Archivo de vídeo]. YouTube. https://www.youtube.com/watch?v=eGDXNY3ItXc&t=2643s; Robles-Carrillo, M. y García-Teodoro, P. (2022). Ransomware: An Interdisciplinary Technical and Legal Approach. Security and Communication Networks, 2022. https://doi.org/10.1155/2022/2806605.
[34] Díaz-Maroto y Villarejo, J. (1997). *Los delitos de daños*. Diario La Ley, Sección Doctrina, (Ref. D-91, tomo 2). Editorial La Ley.
[35] El patrimonio, en este contexto, debe entenderse de manera similar a su interpretación en otros delitos como el hurto o el robo, es decir, se refiere a la lesión de valores patrimoniales específicos, como la propiedad, la posesión o el derecho de uso. No se trata del patrimonio entendido como un *universitas iuris*.
[36] *Vid.* STS 1009/2022, 11 de Enero de 2023 y STS 426/2017, 14 de Junio de 2017.
[37] Sentencia del Tribunal Supremo 426/2017, de 14 de junio

económico, resultando en un perjuicio ya sea para la propia víctima o para un tercero. Por último, la extorsión es un tipo penal de resultado cortado, porque una vez que se ha logrado que el sujeto pasivo realice u omita el acto o negocio jurídico, todo lo que ocurre posteriormente pertenece no al acto de comisión del delito, sino a su fase de agotamiento.

En el contexto del *ransomware*, esta estructura de resultado cortado y encuentro forzado es claramente visible. Los atacantes no necesitan obtener un beneficio económico inmediato para que el delito se considere consumado; basta con que la víctima acceda a sus demandas, como el pago del rescate, para que el delito esté completo. Al igual que en la extorsión tradicional, el resultado cortado se observa cuando la víctima realiza el pago, independientemente de si los datos son recuperados posteriormente o no. Además, el encuentro forzado se manifiesta en la obligación de la víctima de efectuar el pago bajo la amenaza de perder permanentemente sus datos.

En cuanto a su tipo objetivo, el sujeto activo en el delito de extorsión puede ser cualquiera, mientras que el sujeto pasivo es la persona sobre la que se ejerce la violencia o intimidación con el fin de doblegar su voluntad; esto puede incluir tanto al titular del patrimonio afectado como a un tercero con capacidad de disposición sobre dicho patrimonio[38].

La conducta típica del delito de extorsión consiste en obligar a otro a realizar una acción u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero utilizando la violencia o la intimidación. Por tanto, se exige que el sujeto activo obligue al sujeto pasivo a realizar u omitir algo, que se entiende contrario a su voluntad[39]. Esta obligación debe cumplirse mediante "*violencia o intimidación*", lo que incluye los casos de fuerza física directa (*vis* física) y los de coacción (*vis* compulsiva) sobre otra persona.

Es crucial recalcar que estos dos términos han de verse a la luz del delito de robo según el artículo 242 del Código Penal[40]. En este sentido, la violencia se refiere a la aplicación directa de fuerza física contra alguien, mientras que la intimidación no requiere un ataque físico. Basta con que el autor amenace o advierta a la víctima con un daño "*inmediato, grave, personal y posible*", generando un sentimiento de miedo, angustia o

[38] Nuñez Castaño, E. (2017). *Manual de Derecho penal económico y de la empresa.* Tirant lo Blanch.
[39] *Ibid*. Díaz-Maroto y Villarejo, J. (1997). *Los delitos de daños*.
[40] Bajo Fernández, M., Pérez Manzano, M., & Suárez González, C. (1993). *Manual de derecho penal. Parte especial*. Delitos patrimoniales y económicos (2nd ed.). Centro de Estudios Ramón Areces.

intranquilidad ante la posibilidad de un daño real o imaginario[41]. Esta interpretación ha sido respaldada por la jurisprudencia basada en el artículo 1267 del Código Civil[42]. Además, la violencia y la intimidación deben estar orientadas a lograr el objetivo propuesto, es decir, a hacer que el sujeto pasivo lleve a cabo el acto o negocio jurídico, sin que sea imprescindible que la violencia o la intimidación afecten directamente al titular del patrimonio que se busca perjudicar – siempre y cuando dicho sujeto tenga la autoridad suficiente para realizar el acto adecuado.

Siguiendo esta descripción, los ataques *ransomware* podrían verse como una forma moderna de extorsión. Ya que, además de infectar los sistemas informáticos de las víctimas, se exige un pago para descifrarlos, lo que claramente implica un ánimo de lucro. Este *modus operandi* refleja la naturaleza híbrida de la extorsión. Al igual que en el delito clásico, los atacantes coaccionan a las víctimas mediante amenazas implícitas o explícitas de pérdida permanente de datos (coacción que recuerda a las amenazas condicionales) y buscan obtener un beneficio económico (elemento patrimonial). La víctima, bajo esta presión, puede verse obligada a realizar el pago, que constituye el acto o negocio jurídico al que fue coaccionada.

En cuanto al perjuicio, éste debe ser entendido como una disminución patrimonial del sujeto pasivo[43]. Para la consumación del delito, no es necesario que el perjuicio indicado se materialice realmente. El delito se completa cuando el agresor consigue que la víctima, mediante coacción, realice u omita el acto o negocio jurídico deseado, incluso si al final no hay una disminución efectiva en el patrimonio de la víctima. La jurisprudencia indica que "*cualquier evento posterior no pertenece al acto de cometer la infracción, sino a su fase de agotamiento*"[44] y que "*los actos posteriores destinados a asegurar o obtener el beneficio, o a neutralizar a la víctima para que no impida las intenciones del agresor, forman parte de la fase de agotamiento*"[45].

El último requisito necesario en el plano subjetivo es que el comportamiento del autor esté motivado por un ánimo de lucro. Este elemento subjetivo, común a todos los delitos

[41] Vives Antón, T. S., Orts Berenguer, E., Carbonell Mateu, J. C., González Cussac, J. L., & Martínez-Buján Pérez, C. (2010). *Derecho penal parte especial*.
[42] *Vid*., STC Supremo de 11 de noviembre de 1985, 28 de octubre de 1988 y 12 de febrero de 1991.
[43] Se entiende perjuicio como *"toda disminución, económicamente evaluable, del acervo patrimonial que jurídicamente corresponde a una persona, obtenida a través de una acción antijurídica que persigue la obtención de un lucro injusto"* visto en Huerta Tocildo, S. (1981.) *Los delitos patrimoniales*.
[44] Sentencia del Tribunal Supremo de 16 de febrero de 1988.
[45] Sentencias del Tribunal Supremo de 3 de junio de 1988y 15 de noviembre de 1994.

contra bienes patrimoniales, implica que el autor debe actuar con la intención de obtener alguna ventaja económica. La jurisprudencia generalmente interpreta el ánimo de lucro como "*cualquier utilidad o beneficio que el autor pretenda obtener con su conducta*"[46], ya sea para sí mismo o para un tercero.

De acuerdo con los tipos penales mencionados anteriormente, cuando ocurra una conducta de *ransomware*, es decir, el secuestro de datos acompañado de una demanda económica, sin ser necesario que se produzca efectivamente un perjuicio patrimonial, estaríamos hablando de un delito de daños informáticos (Art. 264 CP), y de extorsión (Art. 263 CP). En el contexto de los daños informáticos, el *ransomware* se erige como el ejemplo más claro de, en primer lugar, la conducta de "*hacer inaccesibles datos o programas informáticos*", que incluye cualquier acción que impida de forma permanente o temporal la disponibilidad y el uso adecuado de los datos informáticos por parte del "*titular*" del derecho; y en segundo lugar, del impacto de los programas maliciosos, es decir, la acción de bloquear el acceso a documentos electrónicos, programas y/o datos informáticos sin alterar su existencia o esencia, con el objetivo de acceder a su contenido. Por otra parte, en el contexto de la extorsión, se consigue sancionar todas aquellas conductas destinadas a limitar la voluntad del sujeto pasivo causándole un perjuicio patrimonial, como es el perseguido por el *ransomware*[47].

V. CONCLUSIONES

El derecho penal tiene la función de tutelar bienes jurídicos de importancia social y de proteger a las víctimas. Por tanto, se hace más necesario que nunca considerar cómo debe abordar los nuevos riesgos que surgen en el tráfico jurídico y la actividad económica contemporánea. El propósito de este trabajo es examinar las soluciones propuestas por los tribunales españoles para la persecución y el juicio del *ransomware*, buscando una solución que aborde la complejidad del delito, proteja a las víctimas y garantice la seguridad jurídica. Este estudio ha demostrado que la comisión de ransomware va más allá del delito de daños informáticos, que hasta ahora ha sido el único aplicado.

Para la correcta aplicación de un tipo penal, es imprescindible que la conducta delictiva encaje de manera precisa en la descripción del delito tipificada por la ley.

[46] Sentencias del Tribunal Supremo de 12 de febrero de 1985 y 25 de marzo de 1993.
[47] Yhisselot, D. (2023). *El ransomware. La nueva amenaza digital. Análisis de la regulación del ransomware en el ordenamiento jurídico español y el impacto victimológico*. Universidad Autónoma de Barcelona.

Cuando una conducta no encaja claramente en la tipificación penal, cualquier intento de forzar su inclusión bajo un tipo penal determinado implica una interpretación extensiva o analógica de la ley. Este enfoque va en contra del principio de legalidad y específicamente de la prohibición de la analogía en perjuicio del acusado. La analogía desfavorable está prohibida en el derecho penal porque vulnera la seguridad jurídica y la previsibilidad del sistema legal, elementos esenciales para garantizar que los ciudadanos sepan cuáles conductas son delictivas y cuáles no. Forzar la interpretación de un tipo penal para que abarque conductas que no encajan claramente en su descripción puede resultar en una aplicación injusta de la ley.

Observando las particularidades de los ciberataques *ransomware* existen tres vías de acción: a) mantener la regulación tal y como está y encajarlo en la figura del delito de daños informáticos; b) considerar al *ransomware* como un delito en el que concurren varios ilícitos, que se pueden vincular o desvincular en atención a las características concretas en las que se haya producido el ilícito; y c) considerarlo un delito independiente autónomo.

Dicho lo anterior, el legislador ha optado por no llevar a cabo esta reforma legislativo sino incluir estos nuevos delitos – incluyendo el *ransomware* – en los ya preexistentes. En este contexto, la solución más sensata en mi opinión sería optar por la segunda propuesta, es decir, el abordaje de esta realidad delictiva desde una visión dual: el delito de sabotaje informático (artículo 264 del Código Penal), por cuanto se imposibilita el acceso a los datos yacentes a los sistemas, y el delito de extorsión (artículo 243 de Código Penal) debido a que el objetivo de tales acciones es la consecución de un beneficio económico para el ciberdelincuente.

Finalmente, las propuestas de enjuiciamiento presentadas aquí no son inflexibles por razones obvias: los ciberataques, y en particular el *ransomware*, son un fenómeno en constante cambio. En otras palabras, las directrices expuestas en este trabajo se sitúan en el contexto actual del *ransomware*, sin perjuicio de que estudios futuros en esta materia puedan sugerir enfoques distintos, basándose en las nuevas características de este tipo de conductas. Por lo tanto, es esencial mantener una actitud abierta y adaptable en la aplicación de la ley, asegurando que las medidas adoptadas evolucionen junto con las amenazas emergentes.

* * *