IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

El dilema de las copias de seguridad en el delito de sabotaje contra datos informáticos en el derecho penal español

Wendy Requejo-Passoni
Universidad de Salamanca

Fecha de presentación: octubre 2023
Fecha de aceptación: abril 2024
Fecha de publicación: octubre 2024

Resumen

Esta investigación se centra en proporcionar una nueva perspectiva desde la cual examinar la respuesta dogmático-penal en casos de ciberincidentes, en los que la información afectada sea recuperable mediante copias de seguridad. Con este propósito se analizará el delito de sabotaje contra datos informáticos, conforme al artículo 264.1 del Código Penal español reformado por la Ley Orgánica 1/2015, en atención a las reformas legislativas comunitarias en materia penal y de ciberseguridad. Además, se explorarán diversas perspectivas doctrinarias y jurisprudenciales. Como se demostrará en este trabajo, la recuperabilidad del objeto material del delito convierte el supuesto fáctico descrito en un caso de atipicidad. Asimismo, en situaciones de pérdida total o parcial de la información, la reacción penal solo estará justificada si se cumple con el elemento típico de la doble gravedad, como consecuencia del sentido interpretativo restrictivo plasmado en el texto legal y a la política criminal de la Unión Europea en materia de ciberdelincuencia.

Palabras clave

copias de seguridad; sabotaje informático; lesividad; ciberseguridad

The dilemma of backups in the crime of sabotage against computer data in Spanish criminal law

Abstract

This research focuses on providing a new perspective from which to examine the dogmatic-criminal response in cyber incidents where the affected information is recoverable by backup. For this purpose, the crime of sabotage against computer data will be analysed, in accordance with Article 264.1 of the Spanish Criminal Code reformed by Organic Law 1/2015, in attention to community legislative reforms in criminal and cybersecurity matters. In addition, various doctrine and case law perspectives will be explored. As it will be demonstrated in this work, the recoverability of the material object of the crime turns the factual assumption described into an atypical case. Likewise, in situations of total or partial loss of information, the criminal reaction will only be justified if the typical element of double severity is met, as a result of the restrictive interpretative sense embodied in the legal text and the criminal policy of the European Union on cybercrime.

Keywords

backups; computer sabotage; lesivity, cybersecurity

Introducción

En el cine hollywoodense existen muchas joyas realmente fascinantes tanto por su estética como por la profundidad de lo que nos evoca a reflexionar. Una de ellas es la película *Atrapado en el tiempo* (Groundhog Day, 1993). Su premisa es sencilla: se trata de un hombre (Phil) atrapado en un bucle temporal, que pese a sus persistentes suicidios vuelve a despertar, sin rasguño alguno, en el mismo día y lugar. Tal como si contase con múltiples ejemplares de su propia existencia física, a los cuales siempre puede recurrir. En un escenario como el antes descrito, probablemente atentar contra la vida del personaje significaría una ofensa pública menor, pues, al día siguiente podría vérsele nuevamente cruzando la calle. O por el contrario, podría insistirse en que es legítimo y necesario castigar el asesinato de cada uno de sus clones atemporales.

Dejando aparte los detalles y giros argumentales de la trama, este escenario representa muy bien lo que efectivamente ocurre en entornos menos analógicos, tales como en el ciberespacio (López Torres, 2020, pág. 28).[1] La sinergia de componentes físicos y lógicos hacen factible manipular la información de una manera particular, algo que por otros medios no sería posible (Picotti, 2020, pág. 710).[2] Uno de ellos, es la restauración de la información de los usuarios, valiéndose de la existencia de copias de seguridad (Centro Criptológico Nacional, 2015).[3]

Así, cuando se produce un ciberincidente (indistintamente de su origen intencional o negligente) y la información almacenada resulta afectada o puesta en peligro, el contar con un respaldo actualizado o reciente de esta, permite preservar su integridad y restaurar su disponibilidad.[4]

1. El ciberespacio es la interconexión de redes de telecomunicaciones que permite la transmisión confiable de información a altas velocidades.
2. Al respecto, hay quien afirma que la evolución tecnológica ha creado una nueva dimensión llamada *infosfera*, la cual ha tenido un impacto positivo al optimizar la comunicación en ámbitos como la seguridad nacional y la producción. Además, ha dado lugar a la información digital como objeto de interés jurídico.
3. Cabe añadir que existen tipologías de copias de seguridad, estas pueden ser: completas (toda la información está actualizada), diferenciales (registra solo la información nueva/modificada desde la última completa), o incrementales (solo desde la última copia completa o diferencial).
4. Esta es una práctica clave en ciberseguridad, según el artículo 26 del Real Decreto 311/2022, de 3 de mayo, que regula al Esquema Nacional de Seguridad (ENS), dentro del capítulo de Política de seguridad y requisitos mínimos de seguridad, se prescribe para las administraciones públicas y entidades privadas destinatarias que «los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales».

En contextos analógicos, basta el menoscabo o puesta en peligro del bien jurídico para poner en discusión si está o no justificada la intervención del derecho penal. No obstante, al tratarse de datos informáticos susceptibles de restauración, esta cuestión adquiere una nueva dimensión de análisis. Pues bien, bajo dicha óptica, esta investigación esboza una respuesta al interrogante siguiente: ¿de qué manera disponer e instalar de las copias de seguridad influye en la imputación por el delito de sabotaje contra datos informáticos del artículo 264.1 del Código Penal español?

Naturalmente, para abordar esta misión es necesario no solo efectuar un análisis de los pronunciamientos doctrinarios y jurisprudenciales más relevantes, sino, además, adoptar un enfoque transversal e interdisciplinario que permita abordar las construcciones dogmáticas teniendo en cuenta esenciales conocimientos técnicos de la ciberseguridad.

Respecto a esto último, es fundamental subrayar que el derecho penal, como el derecho en general, se nutre permanentemente de la realidad social que aspira a regular, concretamente de sus valores, de su política, de sus conflictos, etc. No se construye de modo autorreferencial, sino a partir de concepciones extrajurídicas que pueden servir como punto de partida para la actividad del intérprete legal. Como se verá, esto es especialmente importante en los estudios dogmáticos sobre ciberdelincuencia, pues, tal como lo anunciaba Agustina se trata de «preservar el sistema de justicia penal de los vaivenes del legislador y de la inseguridad de una jurisprudencia huérfana de la necesaria reflexión conceptual» (Agustina, 2021, pág 769).

1. Sobre el delito de sabotaje contra datos informáticos

1.1. Descripción típica del artículo 264.1 CP

En España, el comportamiento típico doloso de menoscabo a la integridad y/o disponibilidad de datos informáticos, así como de documentos electrónicos, siempre que la acción y su resultado puedan considerarse graves respectivamente, se encuentra tipificado en el artículo 264.1 del Código Penal.[5]

Para comprender mejor el delito de sabotaje contra datos informáticos, es esencial considerar algunas nociones sobre las dinámicas y los activos valiosos en el ciberespacio. También es importante entender de qué manera, tanto el derecho comunitario como el derecho nacional, construyen la protección jurídica a los datos informáticos, a través del derecho penal. Esto nos aportará una visión panorámica y sistemática de su criminalización.

5. Artículo 264.1 del CP: «El 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 cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años». Cabe señalar que el verbo *borrar* implica la eliminación definitiva, es decir, la pérdida irrecuperable de la información. *Deteriorar* se refiere al acto de empeorar o estropear la información digital, obstaculizando su utilización efectiva. *Suprimir* implica la ocultación intencionada de la información, dificultando su acceso y recuperación.

   Vid. RODRÍGUEZ, M. (2017). *Los delitos de daños. Capítulo IX del título XIII del CP tras la reforma de la LO 1/2015*, pág. 74. Valencia: Tirant lo Blanch.

   Por otro lado, no debe confundirse dañar con alterar: el primero de estos se refiere a la destrucción e inutilización definitiva del soporte que alberga la información, lo cual impide su uso y recuperación adecuada.

   Vid. CORCOY, M. (2015). «Capítulo IX. De los daños». En: CORCOY, M. y MIR PUIG, S. (dirs.). *Comentarios al código penal: reforma LO 1/2015 y LO 2/2015*, pág. 933. Valencia: Tirant lo Blanch.

   En tanto, alterar alude a la perturbación del estado en que se encontraba la información digital, lo cual afecta su integridad y correcto funcionamiento.

   Vid. CORCOY, M. (2019). «Daños. Sabotaje informático (arts. 263-267)». En: CORCOY, M. (dir.). *Manual de derecho penal: parte especial: adaptado a las LLOO 1/2019 y 2/2019 de Reforma del Código Penal. Doctrina y jurisprudencia con casos solucionados*, pág. 580. Valencia: Tirant lo Blanch.

   Finalmente, hacer inaccesibles consiste en impedir, de manera permanente o temporal, la disponibilidad y utilización de la información.

   Vid. FISCALÍA GENERAL DEL ESTADO (2017). *Circular 3/2017, de 21 de septiembre, 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*. FGE [en línea]. Disponible en: https://www.boe.es/buscar/doc.php?id=FIS-C-2017-00003. [Fecha de consulta: 06 de octubre de 2023]. Referencia: FIS-C-2017-00003.

1.2. Cambio del paradigma de la política legislativa europea y nacional

Desde su incorporación en la versión originaria del Código Penal de 1995, este tipo penal ha sido situado en el Título XIII de los «delitos contra el patrimonio y contra el orden socioeconómico», específicamente en el Capítulo IX «de los daños» (Martínez y Lanzarote, 2018, pág. 1591).[6] Esta ubicación sistemática ha influido en su interpretación jurídica, como se explicará a continuación.

El actual texto legal es producto de la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, la misma que se originó para transponer una normativa de la Unión Europea (UE) (Castro y Vázquez-Portomeñe, 2015, pág. 796). Se trata de la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo. Aquella promueve una política legislativa, preventiva y proactiva que fortalezca las capacidades de seguridad de los usuarios de las tecnologías de la información y las comunicaciones (TIC).[7] En términos generales, plasma la idea que el derecho penal debe ser compatible con la normativa extrapenal de la ciberseguridad.

Desde las políticas europeas, el valor económico de la información y los sistemas informáticos ha convertido a la seguridad digital en una preocupación clave para los gobiernos, organizaciones y usuarios. Como consecuencia de ello, el asunto de la ciberseguridad ha sido abordado a través del paradigma de la gestión de riesgos, originario de los estándares internacionales de normalización y hoy en día es alentado por la normativa europea y nacional.[8] A partir de ahí, que las buenas prácticas en materia de ciberseguridad formen parte esencial del cumplimiento normativo tecnológico (Steele, 2004, págs.18-21).[9]

Aunque no sea usual contemplar la influencia de factores empíricos al diseñar políticas legislativas en materia criminal, ciertamente estos pueden ofrecer pautas útiles sobre las prácticas comunes en determinadas actividades reguladas, como lo es la ciberseguridad (Picotti, 2020, pág. 719).[10] En este contexto, la previsión de copias de seguridad es considerada una medida técnica clave para la gestión de riesgos respecto a la pérdida (accidental o intencional) de la información almacenada.[11]

Al examinar los casos de sabotajes con respaldo idéntico o similar de la información afectada, es imprescindible contemplar esto. Especialmente, en virtud del undécimo considerando de la Directiva 2013/40/UE, la cual «establece penas al menos para los casos que no son de menor gravedad»;[12] carácter restrictivo que ha sido transpuesto

6. El Código Penal español de 1995 incluyó los atentados contra datos informáticos como delitos patrimoniales calificados, requiriendo que el valor del daño superara los 400 euros para ser considerados como tales. Aunque en aquel momento casi no se cuestionó respecto a si merecía o no un tratamiento independiente, su inclusión fue aplaudida como un avance legislativo vanguardista.
7. Cuyo preámbulo destaca la dependencia de la UE de los sistemas de información y enfatiza su protección legal para preservar sus valores fundamentales y ciudadanos. Además, plasma que los ciberataques intencionales son la principal amenaza e insta a los Estados Miembros a tomar medidas, como se señala en el segundo considerando de la Directiva 2013/40/UE.
8. Las normas ISO (*International Organization for Standardization*) son representativas, como la ISO 31000:2018(es) para Gestión del riesgo, la ISO 27001 para seguridad de la información, la ISO 27701 para Gestión de la privacidad de la información. En el ámbito europeo, esta concepción del riesgo se refleja en normativas como la Directiva (UE) 2016/1148 (más conocida como Directiva NIS, *Security of Network and Information Systems*) y la nueva Directiva (UE) 2022/2555 (NIS 2.0), e inclusive, el propio Reglamento (UE) 2016/679 (más conocido como GDPR, *General Data Protection Regulation*). En España, se abordan aspectos relacionados en el Real Decreto Ley 12/2018 relativo a la seguridad de redes y sistemas de información y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. También en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
9. En el ámbito del *Compliance penal*, el riesgo es esencial al evaluar las decisiones dentro de la organización, sin embargo, esta cuestión no se limita a esta especialidad jurídica sino que también ha sido abordada por la teoría del derecho.
10. Con relación a este enfoque, desde la orilla del derecho penal italiano se ha afirmado que las contribuciones técnicas y regulatorias de la ciberseguridad son importantes para el ejercicio del *ius puniendi* en el entorno tecnológico, tanto en fase legislativa como judicial.
11. En el artículo 21.1 de la Directiva NIS2 se establece que las medidas para garantizar un alto nivel de ciberseguridad deben tomar en cuenta todos los peligros relacionados con redes y sistemas informáticos, siendo una de ellas la gestión de copias de seguridad. En ese sentido, respaldar la información es una práctica común, alentada por la legislación comunitaria.
12. Directiva 2013/40/UE busca un equilibrio en la penalización de delitos informáticos, evitando criminalizar daños insignificantes o la posesión de herramientas legítimas para *pentesting*, sin dejar de criminalizar los actos preparatorios ni de enfatizar en la responsabilidad penal de las personas jurídicas.

en la ley nacional como el requisito de la doble gravedad en el artículo 264.1.[13]

2. La dogmática penal frente a la previsión de copias de seguridad: principales posturas

En un primer momento, podría pensarse que en el supuesto fáctico que motiva esta investigación no genera mayor controversia, ya que el sujeto pasivo de la acción cuenta con una fuente confiable y accesible para recuperar la integridad y disponibilidad de su información. No obstante, desde una revisión panorámica de la dogmática conceptual se advierten posturas divergentes. Así las cosas, algunas niegan la relevancia penal de estos casos, mientras que otras, encuentran motivos suficientes para su criminalización y sanción.

Algún sector de la doctrina se ha preocupado en sostener que deben abordarse como tentativas inidóneas punibles, pues, el momento consumativo quedaría reservado para la «destrucción» definitiva y completa de los datos informáticos (Andrés, 2015, págs. 354-355),[14] o cuando las copias también hubiesen sido afectadas, o solo consten en soporte analógico (Romeo, 1996, pág. 440).[15] Otro argumento es que existiría desvalor del resultado, y por ende consumación, únicamente cuando la copia no pudiera instalarse en un breve espacio temporal, bien sea por no encontrarse en la misma sede física o, cuando debido a su gran volumen fuese inevitable la interrupción de los servicios informáticos (Conal, 2022, págs. 152-153). Inclusive, se ha planteado la posibilidad de la «tentativa relativamente inidónea al no haber permanencia del daño inicial producido» (Gorjón, 2021, pág. 105). En cualquier caso, existe escepticismo sobre si la tentativa es compatible con el valor de la seguridad jurídica, esencialmente debido a su carencia de respuestas conclusivas para todos los escenarios en que se hubiera generado un respaldo (Balea, 2021).

Por su parte, un segundo sector considera que la previsión de copias idénticas podría restar la gravedad exigida a nivel de tipicidad, esencialmente porque el menoscabo no sería susceptible de valoración económica (Martínez y Lanzarote, 2018, págs. 1592-1593). En este sentido, sería un supuesto de atipicidad.

Frente a tales posturas menos criminalizadoras, otra estima que realmente el delito estaría consumado, pero no agotado. Considera que todo menoscabo contra datos

13. Se han planteado numerosas críticas a la redacción actual del artículo 264.1 del Código Penal, en particular a las expresiones «de manera grave» y «cuando el resultado producido fuera grave». Así, un sector de la doctrina sostiene que la incorporación de la expresión resultaba incomprensible, ya que no existen maneras graves o leves de comportarse.

    Vid. QUERALT, J. (2015). *Derecho penal español: parte especial*, pág. 647. Valencia: Tirant lo Blanch; CORCOY, M. (2015). «Capítulo IX. De los daños». En: CORCOY, M. y MIR PUIG, S. (dirs.). *Comentarios al código penal: reforma LO 1/2015 y LO 2/2015*, pág. 933. Valencia: Tirant lo Blanch.

    Inclusive se ha aseverado que la redundancia en la exigencia de la gravedad puede deberse a una cautela excesiva del legislador por excluir de la persecución penal los casos de menos relevancia.

    Vid. DE LA MATA, N. (2016). «Los delitos contra la integridad y disponibilidad de datos y sistemas informáticos después de la LO 1/2015». En: BACIGALUPO, S., FEIJOO, B. y ECHANO, J. (coord.). *Estudios de Derecho Penal: homenaje al profesor Miguel Bajo*, pág. 1101. Madrid: Editorial Universitaria Ramón Areces.

    De modo más reciente, en este mismo sentido crítico se ha afirmado que la alusión a que la conducta hubiera generado un riesgo grave es una cuestión ya resulta desde la imputación objetiva.

    Vid. NICOLÁS, P. (2023). «El delito de daños informáticos ante nuevos escenarios tecnológicos». En: ROMEO, C. y RUEDA, M. (coord.). *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial. Volumen I: ciberseguridad y ciberdelitos*, pág. 270. Granada: Editorial Comares.

    Sin perjuicio de las objeciones, la incorporación de la cualidad de «grave» en el art. 264.1 CP era necesaria, en virtud de los compromisos de armonización legislativa. En particular, las reformas de 2010 y 2015 responden a la transposición de la Directiva 2013/40/UE, y a los efectos del Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia hecho en Budapest el 23 de noviembre de 2001 (Boletín Oficial del Estado número 226, de 17 de setiembre de 2010, págs. 78847-78896).
14. En un trabajo anterior, referido al texto legal del CP 1995 sostuvo que, con independencia de la previsión o no de copias de seguridad, la «destrucción» de elementos lógicos consuma el delito. Vid. Andrés, 2009, pág. 422.
15. Esta problemática fue anticipada respecto al anterior Código Penal.

informáticos es subsumible en el artículo 264.1, indistintamente de si el afectado cuenta o no con copia de seguridad. Si contase con aquellas, esto podría influir en la graduación punitiva y de la reparación civil, más no en la determinación del grado de desarrollo del delito. La falta de agotamiento respondería a que, pese al resultado típico y desvalor de resultado, la buena diligencia del sujeto pasivo mitiga los efectos perjudiciales desencadenados por el autor (Balea, 2021).

A favor de la consumación también se ha aseverado que basta con la sustancial perturbación operativa de los servicios y con la valorización de los costes de recuperación, ello, de modo independiente de la cuantía por el perjuicio civil (Fernández, 2018, pág. 15). Desde esta óptica, el desvalor de resultado se encontraría en el resultado típico derivado del acto doloso, al margen de la concurrencia o no de respaldos.

3. Desentrañando las construcciones teóricas: entre viejos y nuevos intereses de tutela penal

Así, la problemática ha suscitado diversas interpretaciones, en virtud al alcance y contenido otorgado al bien jurídico-penal. En este sentido, la postura que defiende la tentativa inidónea punible y «relativamente inidónea», aunque no adopta una postura clara respecto al bien jurídico, orienta la discusión a la comprobación del desvalor del resultado. Para sus defensores, no cabe duda que el comportamiento típico ha producido un resultado típico, aunque sus efectos no sean socialmente relevantes o cuanto menos intolerables. Esta concepción resulta sumamente sugerente respecto a las singularidades de la dogmática penal aplicada a la ciberdelincuencia, empero, no aporta un criterio para delimitar aquellos escenarios en los que si bien se produce la interrupción temporal del servicio, realmente la escasa lesividad penal no justificaría la activación al ius puniendi.

Distinto es el supuesto de aquella postura que encuentra en los costes patrimoniales de recuperación un baremo para distinguir la consumación de la tentativa (Benítez, 2021, pág. 672; Fernández y Martínez, 2020, pág. 143; Palomino y Meilán, 2022, págs. 398-399; Galán, 2019, pág. 169; Borja, 2022, pág. 360).[16] Siguiendo este razonamiento, la subsunción de los hechos no representaría mayor dificultad, pues basta con verificar el valor patrimonial derivado del objeto material afectado (Rodríguez, 2017, pág. 78; Conal, 2022, pág. 149). Tal afirmación da lugar a examinar la valoración del perjuicio económico de los datos informáticos.

Al respecto, la Fiscalía General con su Circular número 3/2017,[17] como el Tribunal Supremo (TS) con las sentencias 220/2020 del 22 de mayo[18] y 91/2022[19] del 07 de febrero, de manera implícita y en términos generales, han deslizado el criterio de que la gravedad debe examinarse con un indicador cuantitativo,[20] tal como ocurre cuando la recuperación de la operatividad del sistema afectado no es técnicamente viable, o cuando resulta excesivamente onerosa. A esta concepción cabe formulársele algunas críticas. En principio, los tipos penales de sabotaje contra datos informáticos gozan de independencia penológica respecto a los daños comunes, lo cual significa que los criterios interpretativos de «valor de mercado» y «daño y perjuicio» del art. 263 no deberían formar parte del análisis (Fernández, 2010, pág. 251). Además, en la medida en que los objetos materiales de esta figura destacan por su intangibilidad (inmaterialidad), los criterios desarrollados

16. Postura defendida por quienes consideran que, dada su ubicación entre los delitos contra el patrimonio y contra el orden socioeconómico, el artículo 264.1 es una expresión de criminalidad patrimonial.
17. Fiscalía General del Estado (2017). Circular 3/2017, de 21 de septiembre, 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.
18. Se trata del caso de un empleado público que «borró» 1074 de los ficheros del Registro de la Propiedad, los cuales finalmente fueron «recuperados» de la papelera de reciclaje. Estos hechos inicialmente fueron subsumidos como tentativa de delito de daños informáticos (SAP Badajoz, 130/2018, 23 de julio, ECLI:ES:APBA:2018:761), posteriormente, el TS absolvió al acusado por falta de tipicidad, argumentando que la recuperación de los archivos no constituye gravedad de acción (ES:TS:2020:1520).
19. Caso en que la información sobre descuentos, condiciones de envío y métodos de pago de una empresa no se pudo recuperar. TS ratificó que la gravedad se presenta cuando la recuperación del sistema es imposible o implica esfuerzos técnicos y económicos considerables (ES:TS:2022:528).
20. Desde la reforma de la LO 5/2010 la figura del artículo 264.1 dejó de ser una modalidad agravada de los daños comunes, lo que hace que no se requiera una cuantía mínima para considerar típica a la conducta.

para los daños del art. 263 no le serán aplicables sin mayor esfuerzo (Tejada, 2019, pág. 63).

Por otra parte, la postura de la consumación sin agotamiento ciertamente parece aludir a la lesividad de los pilares de la seguridad informática materializados en la confidencialidad, integridad y/o disponibilidad de la información (Fernández y Martínez, 2018, pág. 191),[21] empero, no estima necesario considerar la valorización económica, sino que basta con la mera interrupción de la funcionalidad operativa.

Este enfoque proporciona un análisis contextualizado de la ciberdelincuencia, pero no ofrece una concepción más restrictiva del sentido interpretativo del tipo penal. Al considerar cualquier afectación a la seguridad informática como delito, incluso si el daño es reversible o hay formas alternativas de recuperación, se amplía significativamente la criminalización de conductas punibles. Sostener aquello puede generar dudas al examinar si realmente existió o no gravedad en la lesividad material, así como al establecer la proporcionalidad de las sanciones.

Finalmente, la concepción de la atipicidad es interesante, ya que implicaría dotar de significado al elemento típico de doble gravedad; tarea que no es sencilla de abordar, por lo que resulta comprensible que se insista en el criterio de la cuantía económica, a pesar de las objeciones planteadas.

4. Algunos apuntes para una reflexión más profunda

Realmente la cuestión de las copias de seguridad es trasladable a cualquier escenario en que la información afectada pudiera recuperarse.[22] Lo cual nos conduce, nuevamente, por los senderos de la dogmática penal, en particular, los aspectos relacionados con la tipicidad (resultado típico) y la lesividad (desvalor de acción y desvalor del resultado) (Laurenzo, 1992, pág. 127),[23] con base en las características del objeto material.

Para desarrollar esta idea, será útil el argumento principal de la inicial referencia fílmica.[24] Según la trama, el personaje Phil experimenta infinitud de muertes, algunas autoinfligidas y otras causadas por terceros (nos centraremos en esta última variante). En principio, la destrucción de su soporte vital, que coincide con el objeto material, podría considerarse como un caso de homicidio. Sin embargo, el cuerpo de Phil tiene la capacidad de «restaurarse», lo que significa que vuelve a su estado original cada mañana. Con lo cual, a pesar de las numerosas «muertes», no se produce una afectación real al bien jurídico de la vida humana independiente. Fuera de la ficción, no podríamos llegar a una conclusión similar, debido a la fragilidad e irreparabilidad del objeto material.

Así las cosas, en el ciberespacio, los datos informáticos se asemejan más al cuerpo del protagonista que a los objetos del entorno analógico (Palomino, 2006, págs. 65-66).[25] La manipulación de comandos y software ofrece diversas posibilidades, como la interacción, representación y manipulación de información en formato digital (digitalización), un almacenamiento, procesamiento y transmisión eficientes (escalabilidad), automatización para reducir la intervención manual, acceso remoto a información y servicios (accesibilidad), y la capacidad de restaurar información eliminada mediante copias de seguridad, historiales de versiones anteriores y técnicas de recuperación de datos, entre otras.

21. Así, «la confidencialidad (protege los datos de manera que sean conocidos solo por las personas autorizadas y permanezcan vedados para el resto), integridad (impide que la información contenida en fichero pueda ser alterada o modificada de manera incorrecta y sin autorización de su titular) y disponibilidad (accesibilidad de los datos cuando sea preciso y por quien esté facultado para ello)».
Existen suficientes referencias de estos pilares en las normativas más relevantes: el Convenio de Budapest del 2001 promueve la criminalización de actos que los afecten, la Directiva 2013/40/UE trata la integridad de datos en delitos informáticos, y las LO 5/2010 y LO 1/2015 armonizan la legislación nacional con las normativas europeas.
22. Un ejemplo ilustrativo es el caso de los archivos «recuperados» de la papelera de reciclaje, el cual motivó la STS 220/2020, 22 de mayo de 2020, antes citada.
23. En el estudio se plasman las tres acepciones diferentes del resultado en la dogmática penal: resultado naturalístico, resultado típico y desvalor de resultado
24. Siempre permitiendo alguna licencia creativa al momento de interpretar el argumento de la trama, aunque justificada a los fines expositivos de esta investigación.
25. Frente a los delitos analógicos, los ciberdelitos requieren un profundo conocimiento interdisciplinario de las dinámicas cibernéticas.

En algunos casos, la pérdida de información debido a actos dolosos de sabotaje informático, como los enumerados en el artículo 264.1 (desvalor de acción), podrían llevar a un resultado típico, empero, ello no equivale a la producción de un desvalor de resultado. Esencialmente, porque la restauración automática o manual de toda la información, desvirtúa tanto la lesión, como la puesta en peligro del bien jurídico. Esto da forma a un supuesto de atipicidad absoluta, no debido a la carencia total o parcial de gravedad, sino a la cualidad de restauración/reparabilidad del objeto (in)material del delito.

Es irrelevante para la sanción penal los perjuicios económicos derivados de la temporal falta de disponibilidad de la información, o los gastos del procedimiento técnico. Para tales supuestos, la responsabilidad civil extracontractual y la entidad del resarcimiento por daños y perjuicios, podría brindar una protección jurídica más conveniente a los intereses del perjudicado. De lo que se trata aquí, es de evitar expandir el alcance del injusto penal más allá de las barreras lingüísticas del texto legal, por esto, el enfoque basado en las consecuencias no resulta compatible con una interpretación restrictiva.

Inclusive, en escenarios en los que la pérdida parcial o total de datos informáticos es inevitable, debido a la elevada dificultad técnica de su instalación, o al contenido incompleto o desactualizado de los respaldos, existe un resultado típico y un menoscabo al bien jurídico; no obstante, esta descripción no basta para determinar si se cumple o no con la gravedad típica.

En particular, conviene subrayar que en el ciberespacio se amplía considerablemente la «superficie de exposición» de los bienes jurídicos en general, y con mayor razón, respecto a la indemnidad de la información. Así, no es deseable que la respuesta penal abarque todas y cada una de estas acciones maliciosas que ponen en peligro o dañan a la información, ya que la reacción punitiva puede replegarse ante otros mecanismos legales o extralegales. Por lo tanto, no toda pérdida de información debido a una copia de seguridad no disponible, incompleta o desactualizada, sería suficiente para justificar la criminalización.

En este sentido, la técnica legislativa del artículo 264.1 cobra mayor relevancia, pues no bastará con la lesividad al bien jurídico en cuestión, sino que esta debe superar determinado umbral de significancia. Así, para no vaciar el contenido del tipo penal, la cualidad de «grave» no debe interpretarse por la forma de ejecución del delito, ni por los efectos del mismo.[26] Sino que la gravedad debe estar determinada por las propias características de la información afectada.

Antes bien, aunque no fuese el objetivo principal de este estudio, es importante considerar algunos criterios para determinar la relevancia intrínseca de la información. Factores como la titularidad, el formato o el volumen de los ficheros pueden sugerir relevancia, pero no son determinantes por sí solos. Esta puede depender, realmente, de su utilidad, actualidad, exclusividad e importancia para el ejercicio de derechos de su titular.

Sin perjuicio de lo anterior, no debe perderse de vista que el tratamiento de la información es complejo y requiere comprender las características del objeto material del delito para evaluar la gravedad del artículo 264.1 del CP de manera realista, coherente y menos arbitraria. Para los problemas dogmáticos en el ciberespacio no existen soluciones sencillas.

Conclusiones

El delito de sabotaje contra datos informáticos del Código Penal español ha evolucionado y seguirá evolucionando, de modo correlacional, con la normativa comunitaria de lucha contra la ciberdelincuencia y con los estándares de normalización en materia de ciberseguridad. Como consecuencia de ello, las interpretaciones del tipo penal deben atender a un enfoque interdisciplinario y a un sentido restrictivo.

La doctrina nacional y la jurisprudencia del Tribunal Supremo han abordado al dilema de la reparabilidad de la información afectada, principalmente, desde la perspectiva del injusto penal, es decir, desde el desvalor de la acción y el desvalor del resultado. Lo cual conduce a interpretacio-

26. No se debe confundir la gravedad del tipo básico con la presente en modalidades agravadas que suponen una construcción más específica de los elementos típicos.

nes discrepantes, según el alcance y contenido que se le asigne al bien jurídico-penal.

Una perspectiva más coherente con las singularidades de la dogmática de los daños informáticos, es partir de las características intrínsecas del objeto (in)material del delito, esto es, la información afectada. De ahí que la restauración automática o manual de toda la información, en razón a la previsión e instalación de copias de seguridad, conlleve un supuesto de atipicidad absoluta debido a la cualidad de reparabilidad del objeto sobre el cual recayó la acción.

En casos de pérdida total o parcial de la información, bien sea por carecer de respaldos o por la imposibilidad de su instalación, debe optarse por una interpretación restrictiva de la ley penal y únicamente perseguirse cuando se cumpla con el elemento típico de la doble gravedad. Entre otros factores, la relevancia de la información (que puede depender de la utilidad, actualidad, exclusividad e importancia para su titular, etc.) desempeñará un papel importante para dicho análisis.

Referencias bibliográficas

AGUSTINA, J. R. (2021). «Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?». *Estudios Penales y Criminológicos*, vol. 41, págs. 705-777. DOI: https://doi.org/10.15304/epc.41.7433

ANDRÉS, A. (2009). «Los daños informáticos en el Derecho penal europeo». En: ALVAREZ, F. (ed.). *La adecuación del derecho penal español al ordenamiento de la Unión Europea*, págs. 411-426. Valencia: Tirant lo Blanch.

ANDRÉS, A. (2015). «Comentario previo a los artículos 264, 264 bis, 264 ter, 264 quater, 265, 266, 267». En: GÓMEZ, M. (ed.). *Comentarios prácticos al código penal. Delitos contra el patrimonio y socioeconómicos (artículos 234-318 bis)*, págs. 347-374. Pamplona: Aranzadi.

BALEA, A. (2021). «Copias de seguridad, delitos de daños informáticos y grado de ejecución». *Diario La Ley* [en línea]. Disponible en: https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAEAC2NQQvCMAyFf429CLKpQzz0MncUER3eszZ0hdpom0737w-1q4JE88iXvWTDNPb5ZG7LeOfKBEYLKc6Q433WfCiqGletqsTO1aK3AclHQkdF1_XV-wh4GXSlK-FIM7y8TEEC6YBWkaIUd6nWDyDthTbCH9_nprdddXUpvNet9s1YQpC6Bv3mFkVKN341HEPz4j-JDOewaGW9HIXhlaQH-__pi3Mcj1wvH69MkF6B4wHCBjtP_cDcRPoufMAAAA=WKE. [Fecha de consulta: 06 de octubre de 2023].

BENÍTEZ, I. (2021). «Capítulo 26. Delitos contra el patrimonio y el orden socioeconómico (VIII). "De la alteración de precios en concursos y subastas públicas", "De los daños", "Disposiciones comunes a los delitos patrimoniales"». En: MORILLAS, L. (ed.). *Sistema de derecho penal. Parte especial*, págs. 637-688. Madrid: Dykinson.

BORJA, E. (2022). «Lecciones XVIII. Delitos contra el patrimonio y el orden socioeconómico (I): Introducción general». En: GONZÁLEZ, J. (coord.). *Derecho Penal Parte especial*, págs. 357-365. Valencia: Tirant lo Blanch.

CASTRO, M.; VÁZQUEZ-PORTOMEÑE, F. (2015). «La reforma de los delitos de daños: arts. 263, 264, 264 bis 264 ter 264 quáter, 265, 266.1 y 266.2 CP». En: GONZÁLEZ, J. (ed.). *Comentarios a la Reforma del Código Penal de 2015*, págs. 791-801. Valencia: Tirant lo Blanch.

CENTRO CRIPTOLÓGICO NACIONAL (2015). *Guía de seguridad (CCN-STIC-401). Glosario y abreviaturas*. CCN [en línea]. Disponible en: https://www.ccn-cert.cni.es/es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html. [Fecha de consulta: 01 de abril de 2021].

CONAL, I. (2022). *Ciberseguridad y derecho penal*. Navarra, España: Thomson Reuters Aranzadi.

CORCOY, M. (2015). «Capítulo IX. De los daños». En: CORCOY, M. y MIR PUIG, S. (dirs.). *Comentarios al código penal: reforma LO 1/2015 y LO 2/2015*, págs. 931-938. Valencia: Tirant lo Blanch.

CORCOY, M. (2019). «Daños. Sabotaje informático (arts. 263-267)». En: CORCOY, M. (dir.). *Manual de derecho penal: parte especial: adaptado a las LLOO 1/2019 y 2/2019 de Reforma del Código Penal. Doctrina y jurisprudencia con casos solucionados*, págs. 572-582. Valencia: Tirant lo Blanch.

DE LA MATA, N. (2016). «Los delitos contra la integridad y disponibilidad de datos y sistemas informáticos después de la LO 1/2015». En: BACIGALUPO, S., FEIJOO, B., y ECHANO, J. (coords.). *Estudios de Derecho Penal: homenaje al profesor Miguel Bajo*, págs. 1089-1108. Madrid: Editorial Universitaria Ramón Areces.

FERNÁNDEZ, C. (2018). «El delito de daños y el espionaje empresarial: dos ataques compatibles contra la información como bien inmaterial». *InDret. Revista para el análisis del derecho*, vol. 1/2018, págs. 1-27 [en línea]. Disponible en: https://indret.com/wp-content/uploads/2020/05/1352b.pdf

FERNÁNDEZ, D.; MARTÍNEZ, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia*. Navarra: Aranzadi.

FERNÁNDEZ, D.; MARTÍNEZ, G. (2020). *Ciberdelitos*. 2.ª ed. Barcelona: Ediciones Experiencia.

FERNÁNDEZ, J. (2010). «Daños informáticos: art. 264.1 CP». En: ALVAREZ, F.; GONZÁLEZ, J. (dirs.). *Consideraciones a propósito del Proyecto de Ley de 2009 de modificación del Código Penal*, págs. 249-252 (conclusiones del Seminario interuniversitario sobre la reforma del Código Penal celebrado en la Universidad Carlos III de Madrid). Valencia: Tirant lo Blanch.

GALÁN, A. (2019). *Los ciberdelitos en el ordenamiento español*. Barcelona: Editorial UOC.

GORJÓN, M. (2021). «Sabotaje informático a infraestructuras críticas. Análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código Penal. Especial referencia a su comisión con finalidad terrorista». *Revista de Derecho Penal y Criminología*, vol. 25, págs. 77-124.

INSTITUTO NACIONAL DE CIBERSEGURIDAD (2018). *Copias de seguridad: una guía de aproximación para el empresario*. INCIBE [artículo en línea]. Disponible en: https://www.incibe.es/empresas/guias/copias-seguridad-guia-aproximacion-el-empresario. [Fecha de consulta: 07 de junio de 2022]

LAURENZO, P. (1992). *El resultado en derecho penal*. Valencia: Tirant lo Blanch.

LÓPEZ TORRES, J. (2020). *Ciberespacio & ciberseguridad. Elementos esenciales*. Ciudad de México: Tirant lo Blanch.

MARTÍNEZ, C.; LANZAROTE, P. (2018). «Capítulo IX. De los daños». En: DEL MORAL, A. (dir.). *Código Penal: Comentarios y jurisprudencia (aprobado por Ley Orgánica 10/95 de 23 de noviembre)*, págs. 1568-1602. Granada: Editorial Comares.

NICOLÁS, P. (2023). «El delito de daños informáticos ante nuevos escenarios tecnológicos». En: ROMEO, C. y RUEDA, M. (coord.). *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial. Volumen I: ciberseguridad y ciberdelitos*, pág. 259-274. Granada: Editorial Comares,.

PALOMINO, J.; MEILÁN, G. (2022). «Los delitos de daños informáticos (arts. 264 a 264 quáter CP)». En: ORTEGA, E. (ed.). *Derecho penal 2022*, págs. 395-415. Valencia: Tirant lo Blanch.

PALOMINO, J. (2006). *Derecho penal y nuevas tecnologías. Hacia un sistema informático para la aplicación del Derecho penal*. Valencia: Tirant lo Blanch.

PICOTTI, L. (2020). «Capitolo XIV. Cybercrime e diritto penale». En: PARODI, C. y SELLAROLI, V. (dir.). *Diritto penale dell'informatica. Reati della rete e sulla rete*, págs. 709-723. Milano: Giuffrè Francis Lefebvre.

QUERALT, J. (2015). *Derecho penal español: parte especial*. Valencia: Tirant lo Blanch.

RODRÍGUEZ, 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.

ROMEO, C. (1996). «Delitos informáticos de carácter patrimonial». *Revista iberoamericana de derecho informático*, vol. 9, págs. 413-441.

RUEDA, M. (2022). «Los ataques de denegación de servicios como ciberdelito en el Código Penal español». *Revista Penal*, vol. 49, págs. 183-216.

STEELE, J. (2004). *Risks and Legal Theory*. Oxford: Bloomsbury Publishing.

TEJADA, E. (2019). «Capítulo 20: la tipificación penal de los ataques a los sistemas informáticos». En: CAMACHO, A. (dir.). *Tratado de derecho penal económico*, págs. 875-963. Valencia: Tirant lo Blanch.

VELASCO, E.; SANCHÍS, C. (2019). *Delincuencia informática. Tipos delictivos e investigación con jurisprudencia tras la reforma procesal y penal de 2015*. Valencia: Tirant lo Blanch.

Cita recomendada

REQUEJO-PASSONI, Wendy (2024). «El dilema de las copias de seguridad en el delito de sabotaje contra datos informáticos en el derecho penal español». *IDP. Revista de Internet, Derecho y Política*, núm. 41. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i41.420591

Sobre la autoría

Wendy Requejo-Passoni
Universidad de Salamanca
wrequejopassoni@usal.es
ORCID: https://orcid.org/0000-0001-9952-2199

Licenciada en Derecho por la Universidad de San Martín de Porres (Perú). Docente en la Universidad de Lima y Adjunta de Docencia en la Pontificia Universidad Católica del Perú durante el año 2022.

Máster en Derecho Penal por la Universidad de Salamanca (20/21), con el Trabajo de Fin de Máster *Ciberataques de ransomware: Tratamiento político-criminal y estudio dogmático para su regulación en el ordenamiento peruano*. Máster en Derecho de la Ciberseguridad y Entornos Digitales por la Universidad de León (22/23), con el Trabajo de Fin de Máster *Relevancia e imposibilidad de recuperar la información afectada: Una interpretación del requisito de gravedad del delito de sabotaje contra datos informáticos (artículo 264.1) del Código Penal Español desde la perspectiva de la ciberseguridad*.

Actualmente, cursando el doctorado en el Programa de Estado de Derecho y Gobernanza Global de la Universidad de Salamanca. Línea de investigación: derecho penal y ciberseguridad.

Publicaciones destacadas: «Avances y Retrocesos de la Política-Criminal Relativa a los Delitos contra Datos y Sistemas Informáticos en el Perú». En: *Ciberseguridad, cibercrimen y nuevas tecnologías*. ISBN Volumen: 978-607-99416-0-4. «Interpretación sistemática de la normativa penal peruana sobre delincuencia organizada: apuntes de sus presupuestos dogmáticos». *Vox Juris*, ISSN 1812-6804, Vol. 39, n.º 1, 2021, págs. 209-221.