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

https://idp.uoc.edu

# Análisis del concepto de *gravedad* relativo al delito de daños informáticos

Roberto Cruz Palmera
Universidad de Valladolid

Fecha de presentación: junio 2024
Fecha de aceptación: junio 2024
Fecha de publicación: octubre 2024

## Resumen

El trabajo estudia uno de los principales problemas relacionados con el delito de daños informáticos, la ausencia de un concepto de *gravedad* previsto en la norma (art. 264 del Código Penal). Para construir una propuesta interpretativa que logre una solución al problema, se revisan los elementos estructurales del tipo y se estudia la Directiva (UE) 2013/40 del Parlamento Europeo y del Consejo para luego emitir una reflexión sobre la importancia del término *gravedad*. Seguidamente, se expone una crítica general del comportamiento delictivo, de lance en lance se expone la propuesta de solución y, por último, las conclusiones.

## Palabras clave

gravedad; daño; irrecuperabilidad

# *Analysis of the concept of* severity *in the crime of computer damage*

## *Abstract*

*This paper studies one of the main problems related to cybercrime, the absence of a concept of* severity *provided for in the norm (art. 264 of the Criminal Code). To build an interpretative proposal that solves the problem, the structural elements of the type are reviewed and the Directive (EU) 2013/40 of the European Parliament and of the Council is studied to then issue a reflection on the importance of the term* severity. *Then, a general critique of criminal behaviour is presented, followed by the proposed solution and, finally, the conclusions.*

## *Keywords*

*severity; damage; irrecoverability*

## Introducción

El precepto contenido en el art. 264.1. del Código Penal (en adelante CP) contempla el tipo básico del delito de daños informáticos.[1] El comportamiento se ubica en el Capítulo IX, «De los daños». La ubicación sistemática de la norma, como puede verse, resulta adecuada con la denominación que adopta el legislador (Marchena Gómez, 2001). Esto no solo parece idóneo a la hora de valorar el bien jurídico protegido en la norma, sino que también, por extensión, resulta adecuado en lo que atañe a la propia lógica que rige la detección de comportamientos jurídicamente relevantes en materia de imputación. Ahora bien, el precepto que regula el delito de daños informáticos cuenta con una serie de problemas que resultan de gran interés para el Derecho Penal. Sin embargo, esta investigación centrará la problemática en la ausencia interpretativa de un término polémico, una expresión valorada como fundamental por los estudiosos de la materia. La norma, por sorprendente que parezca, no contempla una interpretación auténtica de la palabra *gravedad*; pese a ello, el término es reiterativo, pues se recoge seis veces en art. 264 (y aparece en dos oportunidades en el tipo básico, art. 264.1). La ausencia de una interpretación auténtica (de la palabra *gravedad*) obliga al intérprete a diseñar criterios sopesados y prudentes para poder determinar la tipicidad del comportamiento. En efecto, la mayor o menor gravedad de la lesión del bien jurídico, o la mayor o menor peligrosidad del ataque al bien jurídico, son aspectos determinantes a la hora de medir la gravedad del hecho (Mir Puig, 2015), pero la norma exige que tanto el modo de realizar la acción como el resultado sean graves. Esta particularidad, en lo que respecta al ámbito de la teoría jurídica del delito, afecta especialmente a los tipos de resultado, como lo es el delito de daños informáticos. Este trabajo, como se advirtió, pese a la enorme complejidad que caracteriza a la norma, por razones de concretización y de delimitación, se centrará en ofrecer un análisis y una postura personal respecto al término *gravedad*, de ese modo, se podrán ofrecer respuestas a las siguientes cuestiones que engloban la problemática delimitada en la investigación: ¿cuándo se dañan de manera grave datos informáticos?, ¿de qué forma se puede valorar un resultado como grave?

## 1. Aproximación a la norma: ¿los elementos de la estructura del tipo pueden ofrecer indicios para interpretar el término *grave*?

Los elementos estructurales del tipo permiten acceder, con cierta certeza, a las principales problemáticas de toda norma penal; pues esas cuestiones, las problemáticas, yacen en la conducta del tipo, en los sujetos de la con-

1. En concreto, la norma reza como sigue: «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» (negritas fuera del original), art. 264.1 CP.

ducta, pero también en los objetos del delito. Por ende, un análisis mesurado sobre los elementos estructurales del tipo permitirá no solo acceder a los principales problemas que caracterizan al delito de «daños informáticos», sino detectar el *telos* de la norma, una cuestión ligada a la ausencia del término *gravedad*.

### 1.1. La conducta en el tipo básico de daños informáticos

Se trata de un delito de acción múltiple –«el que por cualquier medio [...]»– pero simuladamente se corresponde con la modalidad de tipo mixto alternativo (Otto, 2004). La norma describe seis conductas –o seis verbos típicos–; sin embargo, muchos de esos verbos son sinónimos, una cualidad que aporta poco a la correcta interpretación de la norma (Orts Berenguer y Roig Torres, 2001). Desde el punto de vista aquí defendido, la variedad de verbos parece *blindar* casi todas las posibilidades comisivas, es decir, dan una idea errónea de proteger los objetos para diversas modalidades criminológicas, pero al tratarse de expresiones muy semejantes, la mayoría de verbos se compenetran, por tanto, no logran cubrirse los escenarios presuntamente pretendidos. El primer verbo es *borrar*; que significa «desvanecer, quitar, hacer que desaparezca algo». El segundo es *dañar*; que quiere decir «causar detrimento, perjuicio, menoscabo, dolor o molestia». El tercero es *deteriorar*; lo que implica «hacer que algo o alguien pase a un peor estado o condición». El cuarto es *alterar*; que denota «cambiar la esencia o forma de algo». El quinto *significa*; que representa «hacer cesar, hacer desaparecer». El sexto verbo emana de la expresión *hacer inaccesible*; adjetivo que conlleva lo no accesible, de ese modo, se convierte aquello a lo que se accedía en algo a lo que no se puede acceder. Como puede verse, todos apuntan a una misma finalidad o a una misma dirección: deteriorar algo de modo, que su utilidad se diluya. Retomando el aspecto externo de la conducta, –«dañar»–, al tratarse de un delito de resultado, exige un efecto separado del comportamiento y una consecuencia posterior al mismo. Esto puede darse con la inutilidad de documentos electrónicos ajenos tras el acto de sabotaje (Corcoy Bidasolo, 1990) que logra eliminar la cosa. Como se expuso al inicio, al tratarse de un delito de acción múltiple, el resultado «dañar» puede producirse por cualquier medio y de distintas formas –delito de acción múltiple–; pero se exige que tanto la acción como el resultado sean graves, no de otro particular (de Urbano Castrillo, 2011).

El aspecto subjetivo del tipo está siempre determinado por el propósito consciente del peligro concreto que desprende la conducta del agente. Se trata de un delito eminentemente doloso (Greco, 2017). El conocimiento de la situación típica está determinado por la exigencia de obrar sin autorización previsto en la norma, también de operar de forma grave. Por consiguiente, quien accede a determinados datos para luego destruirlos, o quien accede a determinados documentos electrónicos para seguidamente eliminarlos, obra necesariamente de forma dolosa; no de otra manera (Velázquez Velázquez, 2020). El precepto no contiene elementos adicionales al dolo, aunque puedan derivarse resultados o consecuencias de índole económica relevante o relativos a la afectación de la seguridad del Estado, estas consecuencias no pueden asimilarse a elementos subjetivos del tipo o adicionales al dolo, pues el autor del tipo –en los elementos cognitivos previstos en el precepto – busca hacer daño; no incrementar su patrimonio de forma injustificada; no hay un fin adicional al dolo de dañar (o de cometer un sabotaje en la modalidad de tentativa, por caso). Expresado de otro modo, quien realiza esta modalidad delictiva produce un resultado que se distancia del ánimo de lucro. El comportamiento se corresponde más con un ánimo de sabotaje, dañino, injusto, pero no ostenta un ánimo de lucro (Muñoz Conde, 2023).

### 1.2. Los sujetos de la conducta típica

Es indiscutible que el tipo en cuestión requiere la intervención de tres sujetos que se hallan en una relación mutua particular. El autor o sujeto activo del delito (quien comete la infracción), el sujeto pasivo o la víctima (quien sufre el daño al bien jurídico-penal) y el Estado (encargado de imponer la sanción). El sujeto activo en este comportamiento puede ser cualquiera. La norma penal no prevé una limitación en lo que respecta a la adscripción del título de autor; por ende, se trata de un delito común. Esta cualidad permite inferir que el autor del delito no guarda una relación especial con el bien jurídico protegido en la norma. Sin embargo, es posible defender que algunas de las modalidades comisivas (o modos de perpetrar el daño) no pueden ser, en principio, realizadas por cualquiera ante la innegable necesidad de ostentar cualidades especializadas para obrar en el contexto delictivo (Benítez Ortúzar, 2020). Por ejemplo, cuando la norma prevé una agravante para quien realice el delito mediante la utilización de un código que permite acceder a la totalidad de un sistema de información que está protegido. Desde el punto de

vista defendido en este trabajo, se trata de un agravante relacionado con la superioridad que demuestra el agente ante la potencial víctima, pues, como se adelantó, en determinados contextos que describe la norma no cualquiera puede tener dominio del hecho ante la necesaria adquisición de capacidades técnicas.

El sujeto pasivo en el delito de daños informáticos es el titular del bien jurídico protegido en la norma. Al no corresponderse con un delito contra las personas, resulta lógico defender que el sujeto pasivo no tiene que ser el mismo que el individuo sobre quien se realiza físicamente la acción (Heinrich, 2016). Como puede verse, se trata de una valoración excesivamente clásica en contraposición con la era digital en la cual se enmarca el delito de daños informáticos. Es por todos conocido que esa conducta generalmente se realiza a distancia, puesto que la actividad se ejecuta en un lugar y el resultado se consigue en otro distinto (Seiler, 2022) y recae sobre «cosas».

El perjudicado en este particular comportamiento delictivo encierra gran relevancia; el tipo penal, como se advirtió, contiene una serie de agravantes referidas tanto a los modos comisivos como a las consecuencias producidas (*quantum* generado). Precisamente en esta última puede cobrar cierta relevancia la figura del perjudicado,[2] esto es, todo aquel que soporta consecuencias perjudiciales directas o indirectas (Fiandaca y Musco, 2023, págs. 189-192).

### 1.3. Los objetos en el tipo básico del delito de daños informáticos

El objeto material y el objeto jurídico también juegan un rol fundamental en lo que respecta a la problemática trazada en esta investigación: la determinación del término *gravedad*.

El objeto material es la cosa sobre la que ha de recaer físicamente la acción (conocida asimismo como objeto de la acción). Los objetos en el delito de daños informáticos varían (Salvarodi, 2011). La detección está supeditada al soporte donde reposa la cosa *destruida*, *borrada*, *dañada*, *alterada* o *bloqueada* por el agente. Como se expuso a la hora de explicar la parte objetiva del tipo, el comportamiento, que produce un resultado, sobrecoge de manera negativa a datos informáticos, a programas informáticos, pero también a documentos electrónicos que reposan en dispositivos o en ordenadores; aspectos tangibles. Sin embargo, tanto datos informáticos como documentos electrónicos pueden reposar en una *cloud computing*, la cual no depende de un servicio físico instalado, pues el acceso a dicha estructura es inminentemente virtual lo que podría corresponderse –hasta cierto punto– con un aspecto intangible. En resumen, la acción desplegada por el agente la pueden sufrir diferentes clases de objetos y la forma «de llevarlo a cabo puede ser física –arrojando un líquido corrosivo sobre el disco duro de un PC, p. ej.– o lógica –inoculando un virus, ya sea por línea, ya sea mediante un dispositivo insertable–; los medios son inimaginables» (Queralt Jiménez, 2015, pág. 646).

El objeto jurídico en el delito de daños informáticos puede ser valorado como la propiedad. Sin embargo, es posible defender otra posición fuera del eje sistemático de la norma.[3] El objeto jurídico protegido es de difícil determinación y nada impediría argumentar que se trate de la propiedad representada en el valor de los datos y programas informáticos: objetos corpóreos atacados por el daño. En similar sentido, puede decirse que el bien jurídico es la seguridad de los datos informáticos (Solari Merlo, 2013). Pero la complejidad del delito permite asimismo la afectación de otros intereses que no alcanzan aún el estatus de bien jurídico, como el correcto funcionamiento de los datos almacenados en los programas o soportes informáticos. Por tanto, es posible afirmar que se trata de un delito pluriofensivo, ya que mediante el acceso a los datos viola la intimidad (o la confidencialidad). Además, en algunas modalidades comisivas se afecta tanto la propiedad –delito patrimonial– como valores colectivos de una pluralidad de perjudicados (personas que soportan consecuencias perjudiciales al afectarse la seguridad informática). Sea cual fuere el bien jurídico protegido en la norma, tanto la doctrina científica como la jurisprudencia coinciden en que la afectación y el comportamiento deben ser graves (Faraldo Cabana, 2009) –lo que justifica la problemática trazada en este trabajo–.

Al revisar los elementos estructurales de la norma se apuntaron distintas cuestiones problemáticas, como la

2. En efecto, varios supuestos se contienen en la norma, pero a título de ejemplo se exponen los siguientes: el primero, perjuicio grave a la provisión de bienes de primera necesidad; el segundo, afectación al sistema informático de una infraestructura crítica o creación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea.
3. Una de las posturas claramente defendibles es la seguridad informática, que se ve afectada ante los diversos ataques tanto cualificados en el resultado como de afectación individual.

redundancia o reiteración de comportamientos descritos en la conducta típica que complican la interpretación de la norma, la discutible condición de autor del tipo como sujeto no cualificado (o común), la variación entre sujeto pasivo y potenciales perjudicados, la compleja determinación de objetos del delito, o la discutible determinación del bien jurídico protegido en la norma. Más allá de lo anterior, lo cierto es que la apreciación del comportamiento no requiere necesariamente una cualificación económica, pues en realidad se demanda que el daño sea causado de forma «grave» y realizado de esa misma manera, «grave».

## 2. El delito de daños informáticos y su regulación internacional: la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013

El delito de daños informáticos es un tipo penal relativamente reciente en comparación con el delito clásico de daños (Capítulo IX). La incorporación del delito de daños informáticos fue posible mediante la Ley Orgánica 10/95, pero su principal modificación se realizó gracias a la Ley Orgánica 1/2015. Esta última se aprobó para atender determinados compromisos internacionales como la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos. En lo que respecta a los objetivos principales de la Directiva, se buscaba «aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la cooperación entre las autoridades competentes, incluida la policía y los demás servicios especializados encargados de la aplicación de la ley en los Estados miembros, así como los organismos especializados de la Unión, como Eurojust, Europol y su Centro Europeo contra la Ciberdelincuencia y la Agencia Europea de Seguridad de las Redes y de la Información».[4] Del mismo modo, el citado compromiso buscaba «garantizar que los ataques contra los sistemas de información sean castigados en todos los Estados miembros con penas efectivas, proporcionadas y disuasorias, y mejorar y fomentar la cooperación judicial entre las autoridades judiciales y otras autoridades competentes, no pueden ser alcanzados de manera suficiente por los Estados miembros, y que, por consiguiente, debido a sus dimensiones o efectos, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad [...]».[5] Los citados pueden ser valorados como los objetivos clave trazados en la Directiva. En efecto, dichos objetivos fueron diseñados debido a una serie de problemáticas de necesaria solución en el territorio europeo tales como, ataques contra los sistemas de información, ataques vinculados a la delincuencia organizada, ciberataques a gran escala, etc. Desde el punto de vista que aquí se defiende, esos objetivos deben ser de utilidad a la hora de interpretar la norma que regula el delito de daños. Expresado de modo distinto, el *telos* de la norma debería coincidir –en mayor o menor grado– con los principales postulados de la Directiva. Agotado el estudio de ese acuerdo internacional, es posible sostener que el precepto contenido en el art. 264 del CP fue reformado en atención al objeto marcado en el art. 1 de la Directiva (UE) 2013/40, del Parlamento Europeo y del Consejo. Cuestiones como castigar el acceso no autorizado, la obstaculización, la eliminación, el deterioro, la alteración de datos, aplicar penas agravadas cuando se utilicen programas específicamente adaptados para realizar las infracciones, castigar la tentativa del delito y castigar asimismo la inducción o la complicidad, están previstas en la norma. Pero el precepto contenido en el art. 264 carece de un concepto de «gravedad». Ahora bien, la importancia de esa noción es atendida –hasta cierto punto– en la Directiva (UE) 2013/40, porque obliga a que los Estados definan o emitan conceptos de gravedad respecto a los daños; literalmente, sostiene que: **«los Estados miembros deben poder establecer qué constituyen daños graves de conformidad con su ordenamiento jurídico y práctica nacionales, tales como interrumpir los servicios del sistema de una importancia pública relevante, o causar importantes costes económicos o pérdidas de datos de carácter personal o de información sensible».**[6] En ese sentido, se defiende que el legislador ha asumido de manera

4. Considerando n.º 2 de la Directiva (UE) 2013/40, del Parlamento Europeo y del Consejo.
5. Considerando n.º 33 de la Directiva (UE) 2013/40, del Parlamento Europeo y del Consejo.
6. Considerando n.º 5 de la Directiva (UE) 2013/40, del Parlamento Europeo y del Consejo.

parcial una importante norma que regula aspectos fundamentales en la era digital y ello resulta injustificable, pues la Directiva insiste en que uno de sus objetivos es aproximar las normas de derecho penal de los Estados miembros, para que estos fijen las definiciones relativas a las infracciones penales y una de esas definiciones es, por descontado, el concepto de «gravedad». No obstante, la Directiva aporta cierta luz interpretativa que debe ser valorada por los jueces penales. Esas valoraciones son las siguientes: interrupción de servicios del sistema de una importancia pública relevante, producir importantes costes económicos, causar pérdidas de datos de carácter personal y generar pérdidas de información sensible.

Como puede verse, algunos de esos criterios adolecen de ambigüedad, como la expresión «producir importantes costes económicos», pues la cuantía no resulta siempre un baremo medidor justo que logre detectar el elemento «grave». Lo que puede ser una pérdida grande en un pequeño empresario puede ser irrelevante (o irrisorio) en una multinacional. A pesar de ello, la expresión «producir importantes costes económicos» permite aterrizar en escenarios mucho más concretos, pero es menester conectar el criterio con el contenido general de la Directiva. Agotada esta reflexión, conviene exponer algunas reflexiones sobre el término *gravedad*.

## 3. Reflexión sobre el término *gravedad* en el delito de daños informáticos

La norma contiene algunas apreciaciones que parecen medir la gravedad del comportamiento, pero se distancian de ser valoradas como criterios que permitan detectar la gravedad del comportamiento, pues el apartado segundo del art. 264 prevé una agravante mientras concurran una serie de circunstancias (Morales García, 2002). Estas son, que el hecho se realice en el marco de una organización criminal, que se detecte la causación de daños especialmente graves o que afecten a un número elevado de sistemas informáticos, que el hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad y que los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea (Velasco Núñez, 2019, pág. 51). A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones; que el delito se haya cometido utilizando alguno de los medios a que se refiere el precepto contenido en el artículo 264 ter del CP.[7] Ante la no concurrencia de las circunstancias se impondrá una pena de prisión **de seis meses a tres años**; pero si concurre alguna, se impondrá una pena de prisión **de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado**. Como puede verse, se trata de escenarios comisivos (organización criminal), de aspectos de cuantitativos que tampoco logran concretizarse (causación de daños especialmente graves o que afecten a un número elevado de sistemas informáticos), de resultados cualificados que adolecen de ambigüedad (perjuicio grave de funcionamiento de servicios o peligro grave para la seguridad del Estado) y de empleo cualificado de medios (programa adaptado principalmente para realizar el daño). Pero ninguna aporta algo para determinar la doble exigencia contenida en la norma, «de manera grave» y «resultado grave». El apartado segundo culmina con la siguiente expresión: «si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado». Se trata, una vez más, de innecesarias redundancias a la gravedad que aumentan sobremanera la problemática de la interpretación. Por último, el apartado tercero dispone que «las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero». Se trata de otra cualidad específica respecto a los objetos del delito y uso ilícito de datos, pero no aporta mucho respecto a la determinación del término *gravedad* (Serrano Tárraga, 2013, pág. 527).

7. Los medios son los siguientes: «a) un **programa informático**, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o b) **una contraseña** de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información» (negritas fuera del original).

Por todo ello, se presentan algunas soluciones posibles. La primera, acoger estrictamente las valoraciones reseñadas con anterioridad («escenarios comisivos», «aspectos cuantitativos», «resultados cualificados»...), omitiendo las expresiones «de manera grave» y «resultado grave», valorándolas como redundantes y carentes de un significado normativo. En consecuencia, cualquier daño, eliminación, alteración o deterioro de documento electrónico ajeno será catalogado como grave siempre que se atienda al resultado exigido en la norma de «eliminación del documento», por ejemplo. Así, toda conducta que logre destruir o alterar datos por medios físicos o electrónicos debe ser considerada como delito de resultado punible a efectos del art. 264. Pero un escenario como el planteado supondría la aplicación de la norma a quien, sin autorización y mediante un programa informático, eliminara el extenso *curriculum vitae* en formato electrónico que se hallara en el interior del ordenador del titular. Es razonable que la omisión de las expresiones «de manera grave» y «resultado grave» no pueden ser asumidas sin ponderación en un derecho penal democrático. Pues esta clase de interpretaciones violarían principios básicos del derecho penal como el de proporcionalidad o el de legalidad. Se impondría una pena privativa de libertad de hasta tres años por dañar un documento electrónico recuperable, probablemente inútil a los efectos de elaboración. Una sanción como esa, como se sabe, se aproxima al delito de homicidio culposo,[8] delito que protege el valor más importante en una democracia.

La segunda, aplicar exclusivamente la norma cuando se determinen los aspectos relativos a la gravedad contenidos en la Directiva. Estos son: interrupción de servicios del sistema de una importancia pública relevante, producir importantes costes económicos, casación de pérdidas de datos de carácter personal y generar pérdidas de información sensible. Como puede verse, es defendible –en cierta medida– un aspecto común, la *irrecuperabilidad*. Este aparece en los sistemas públicos esenciales y se trata de una cuestión relativa al tiempo como valor irrecuperable. Del mismo modo, se refiere a la pérdida de datos de carácter personal, es decir, dejar de tener esos datos, o no hallarlos. También se aprecia en la pérdida de información sensible y aunque se refiere a otro valor, se ubica en el mismo sentido de la *irrecuperabilidad*. Respecto al criterio relativo a importantes costes económicos, se aproxima, pero levemente. Desde el punto de vista planteado en esta investigación, las pautas que presenta la Directiva son valiosas, pero en realidad no logran abarcar una solución. Esto es así porque el texto comunitario obligaba a los Estados a definir los criterios de daño grave, lo que el legislador español paso por alto. Ahora bien, en realidad, el criterio de *irrecuperabilidad* es una valoración que se desprende de una interpretación gramatical extensiva que intenta respetar la lógica de la Directiva pero puede ser objetada como una apreciación forzada.

La primera interpretación planteada en esta sección del trabajo debe ser rechazada, pues pasa por alto los criterios de gravedad contenidos en la norma y ello no resulta adecuado en un sistema penal democrático respetuoso con el participio de legalidad penal (Mir Puig, 2015). Veámoslo mediante un supuesto: «"A", de manera arbitraria, daña el dispositivo *pendrive* de "B", donde reposa su valioso *curriculum vitae*», ¿Debe ir «A» a prisión por destruir el documento electrónico? Desde una interpretación literal que pasa por alto los criterios interpretativos, sí debería ir a la cárcel. Pues no hay que olvidar que el precepto contenido en el art. 264 del CP dispone que: «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». Nótese que tanto la expresión de «manera grave» como la locución «resultado producido fuera grave» son indispensables para poder aplicar la norma. Como se expuso arriba, quien pasa por alto tales expresiones aplica el precepto desmedidamente, lo que conlleva una interpretación sesgada, desviando la aplicación de la norma al ámbito de la injusticia. Volviendo al ejemplo citado, el comportamiento se realiza con una de las modalidades posibles (medio físico), se ejecuta sin autorización (de manera arbitraria), agota un resultado mediante uno de los verbos típicos (daña el dispositivo *pendrive*), pero igualmente se corresponde con uno de los objetos descritos (*curriculum vitae* en soporte electrónico).

8. El precepto contenido en el art. 142 del CP contempla una pena para el homicidio culposo de uno a cuatro años. Concretamente, señala el legislador: «el que por imprudencia grave causare la muerte de otro, será castigado, como reo de homicidio imprudente, con la pena de prisión de uno a cuatro años». A todo esto, se trata de la misma pena aplicable –prisión de seis meses a tres años– al delito de amenazas, al de coacciones, al de matrimonio forzado, al delito de estafa; comportamientos que ostentan un desvalor de resultado sobradamente superior en comparación con el supuesto delictivo planteado.

En varias secciones de la Directiva, se contienen aspectos problemáticos como la pérdida de datos informáticos. Esta cuestión es valorada como un problema de difícil solución en Europa, ya que logra alcanzar consecuencias significativas en diversos ámbitos, desde el personal hasta el empresarial, pero también afecta a nivel gubernamental.[9] En lo que atañe a la pérdida de datos informáticos a nivel empresarial, esta puede derivarse en un impacto en las empresas, principalmente en el marco financiero, pues la recuperación de ciertos datos genera pérdidas económicas que en algunos eventos resulta irremediable. Es lógico suponer que, si los datos no pueden recuperarse, la empresa soportará pérdidas financieras significativas. Otra cuestión relacionada es la pérdida de ingresos. Si una empresa depende de los datos «robados» para sus actividades ordinarias, es irrefutable que estemos ante un caso de gravedad y no de otro particular. Igualmente, en algunas entidades, la pérdida de datos conlleva la imposición de multas, por ejemplo, cuando se trata de información sensible o regulada (como historias clínicas, informes médicos, valoraciones psicológicas, ficheros con datos personales e información sensible, etc.). Además, esa seguridad o buen funcionamiento en los sistemas de información trazados en la Directiva, también puede conllevar la degradación de la confianza de los clientes. Casi nadie negaría que la pérdida de datos afecta en algunos casos la confianza cuando se trata de información personal o de información financiera. Aparece en esta variante también la imagen reputacional, ya que la pérdida de datos puede perjudicar la reputación de la compañía, cuestión que repercute en las relaciones con clientes, con socios, con proveedores... Ahora bien, el buen funcionamiento en los sistemas de información trazados en la Directiva afecta asimismo a ciudadanos de manera individual, es asumible por casi todos que la pérdida de datos personales, como datos bancarios, fotografías íntimas, documentos importantes —aun desde un plano subjetivo—, puede comprometer la privacidad y la seguridad de los ciudadanos. De ello se despliegan factores como la pérdida irreparable, porque tanto fotos como videos pueden perderse para siempre, afectando emocionalmente a los titulares. Otro aspecto similar es el relativo a los costos que supone la recuperación de esos datos, pues dicho proceso puede ser elevado en términos económicos, pero también puede ser incosteable para algunos, de esta forma la recuperación puede también resultar imposible a efectos técnicos. Ahora bien, esta última cuestión engloba una pérdida de tiempo, un elemento importante a la hora de valorar la gravedad del comportamiento. El tercer ámbito es el gubernamental, o el relativo al Estado, puesto que es innegable que la pérdida de datos en entidades gubernamentales puede comprometer la seguridad nacional, especialmente si involucra información clasificada. En sentido similar, la pérdida de datos puede interrumpir la prestación de servicios públicos, afectando a la ciudadanía en general y a la correcta operatividad del gobierno representado por el ministerio u otras entidades. Del mismo modo, la pérdida de datos puede afectar a la confianza de la ciudadanía general respecto a la capacidad de gestión de las respetivas administraciones. Como puede verse, esta valoración puede servir, por un lado, para argumentar la importancia de las normas que regulan la protección de la información en el ámbito informático, pero por otro, para determinar circunstancias verdaderamente graves en tres ámbitos: el empresarial, el personal y el gubernamental (todos trazados en la Directiva).

Expuesto lo anterior, se da respuesta a las preguntas planteadas al inicio de la investigación: ¿cuándo se dañan de manera grave datos informáticos o documentos electrónicos?, ¿cómo se valora el resultado como grave? Nótese que en ambos interrogantes aparece la gravedad, por una parte, en el *modus operandi* del comportamiento, por otra parte, en el resultado... Por consiguiente, se sostiene que la tipicidad estaría condicionada a un doble juicio de gravedad: el de la acción y el del resultado. Se trata de una exigencia excesiva que, como se advirtió, dificulta la interpretación de la norma. Pese a ello, esa connotación es necesaria para desechar las acciones insignificantes a efectos de imputación (Manna, 2017, pág. 240).

9. Esta particularidad se describe textualmente actualmente en la norma penal que fue reformada por la citada Directiva. Pues el art. 264.2 4.ª, señala que: «Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias. **Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea**. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones» (negritas fuera del original).

La lógica marca que el resultado «grave» debe estar unido al modo comisivo, pues no es posible determinar una consecuencia grave sin la utilización de medios que permitan alcanzar la connotada gravedad. En ese marco, el *modus operandi* está supeditado a la gravedad del resultado. Así, la expresión «de manera grave» debe ser considerada como accesoria respecto al resultado («resultado grave»).[10] Pero también la lógica marca que la conducta que carece de idoneidad para poner en peligro el objeto jurídico (o para lesionarlo) debe ser rechazada (Marinucci, págs. 457-459).

Se presentan los criterios interpretativos para valorar la gravedad del comportamiento. Así, la acción podrá ser «grave» siempre que:

- sea imposible recuperar la plena operatividad del objeto;
- devolver las cosas a su estado anterior requiera complejidad técnica y esfuerzos económicos en atención a la situación personal del perjudicado;
- se den los comportamientos «borrar» y «dañar» que siempre serán valorados como graves al suponer la pérdida definitiva del objeto, mientras que la «alteración» o el «deterioro» ostentarán una valoración parcial nunca estimada como grave;
- el esfuerzo que suponga la elaboración de los datos afectados debe estar siempre presente en el análisis de la valoración, respetando también siempre la situación personal (intelectual, emocional, física, etc.) del perjudicado.

Como puede verse, no es posible ofrecer una solución global al problema, en primer lugar, porque el tipo penal es tanto alternativo como de acción múltiple y esto permite revelar elevadísimas formas de realizar los actos tipificados. En segundo lugar, porque en la actual era digital la vertiginosa velocidad de los avances tecnológicos se asume como imparable, e igualmente imparable se aprecia el perfeccionamiento de las técnicas comisivas por parte de los delincuentes informáticos. Por ende, es innegable que existirán comportamientos humanos que puedan crear daños informáticos, pero que todavía son inimaginables. Sin embargo, los criterios ofrecidos en este trabajo pueden contribuir a una aplicación más justa y coherente con los postulados donde se asienta el derecho penal social, democrático y de derecho.

## Conclusiones

La dinámica criminológica en el delito de daños informáticos se distancia del ánimo de lucro. El comportamiento debe asociarse mejor a un ánimo de sabotaje, de daño, o de destrucción.

La gravedad del delito de daños informáticos no puede asociarse a un criterio sistemático como el previsto en el art. 236 del CP que regula los daños clásicos. Se ha demostrado que la afectación va más allá de criterios económicos, pues el comportamiento afecta también otros valores constitucionales como la intimidad o la privacidad. Además, no es posible estimar la afectación en una cuantía de 400 euros, pues la cifra no logra ser objetiva y tampoco cubre valores intangibles relacionados en algunos documentos, datos o programas en creación, por ejemplo. En similar sentido, el comportamiento delictivo debe ser valorado como delito pluriofensivo, ya que en la dinámica comisiva se afectan programas informáticos y datos, pero también se viola la seguridad de los datos u otros intereses como la intimidad o la privacidad.

El delito de daños informáticos no prevé una limitación en lo que respecta a la adscripción del título de autor, pero es posible defender que se trata de un delito especial encubierto, pues en algunas modalidades no pueden ser realizadas por cualquier sujeto y otras solo pueden ser ejecutadas en ámbitos laborales donde se tiene acceso o permisos telemáticos que permiten dañar el objeto jurídico.

En el delito daños informáticos, la tipicidad parece estar condicionada a un doble juicio de gravedad, pero se ha demostrado que el *modus operandi* está supeditado a la gravedad del resultado.

El escenario planteado amerita defender una reforma del precepto o, en contraposición, se podría optar por las valoraciones compartidas en este trabajo.

10. A todo esto, aunque en el precepto contenido en el art. 2 de la Directiva (UE) 2013/40 del Parlamento Europeo y del Consejo se recojan varias definiciones, esta guarda silencio en lo que respecta al modo de obrar grave. Por ello, parece conveniente defender que se trate de una redundancia por parte del legislador español a la hora de redactar la norma.

## Referencias bibliográficas

BENÍTEZ ORTÚZAR, I. (2020). «Delitos contra el patrimonio y el orden socioeconómico». En: Morillas Cuevas, L. (dir.). *Sistema de Derecho Pena. Parte especial*, págs. 647-678. Madrid: Dykinson.

CORCOY BIDASOLO, M. (1990). «Protección penal del sabotaje informático. Especial consideración a los delitos de daños». *Revista Jurídica La Ley*, n.º 1, págs. 1000-1010.

DE URBANO CASTRILLO, E. (2011). «Los delitos informáticos tras la reforma del CP de 2010». *Revista Aranzadi Doctrinal*, n.º 9, págs. 163-176.

FARALDO CABANA, P. (2009). *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, págs. 133-136. Valencia: Tirant lo Blanch.

FIANDACA, G.; MUSCO, E. (2023). *Diritto penale. Parte generale*, 8.ª ed. Turín: Zanichelli Editore.

GRECO, L. (2017). «Dolo sin voluntad/Wilful misconduct without will». *Nuevo Foro Penal*, n.º 13, págs. 10-38. DOI: https://doi.org/10.17230/nfp.13.88.1

HARRO, O. (2004). *Grundkurs Strafrecht -Allgemeine Strafrechtslehre, De Gruyter Lehrbuch*, 7.ª ed. Berlín: De Gruyter.

HERINRICH, B. (2016). *Strafrecht Allgemeiner Teil*, 5.ª ed. Stuttgart: Kohlhammer W. DOI: https://doi.org/10.17433/978-3-17-031058-2

MANNA, A. (2017). *Corso di Diritto Penale. Parte Generale*, 4.ª ed. Milán: Wolters Kluwe Italia.

MARCHENA GÓMEZ, M. (2001). «El sabotaje informático entre los delitos de daños y desórdenes públicos». En: LÓPEZ ORTEGA, J.M. (dir.). *Cuadernos de derecho judicial. Ejemplar dedicado a: Internet y derecho penal*, n.º 10, págs. 353-366.

MARINUCCI, G.; Dolcini, E.; Gatta, G.L. (2023). *Manuale di Diritto Penale. Parte Generale*, 12.ª ed. Milán: Giuffrè.

MIR PUIG, S. (2015). *Derecho Penal. Parte General*, 10.ª ed. Barcelona: Reppertor.

MORALES GARCÍA, O. (2002). «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la conveción del consejo de Europa sobre Cyber-Crime». *Cuadernos de derecho judicial,* n.º 9, págs. 11-20.

MUÑOZ CONDE, F. (2023). *Derecho Penal. Parte especial*, 25.ª ed. Valencia: Tirant Lo Blanch.

ORTS BERENGUER, E.; ROIG TORRES, M. (2001). *Delitos informáticos y delitos comunes cometidos a través de la informática*, passim. Valencia: Tirant lo Blanch.

QUERALT JIMÉNEZ, J. (2015). *Derecho Penal español. Parte Especial*, 7.ª ed. Valencia: Tirant Lo Blanch.

SALVARODI, I. (2011). «Los nuevos delitos informáticos introducidos en el Código Penal Español con la Ley Orgánica N. 5/2010». En: PÉREZ ÁLVAREZ, F. (ed.). *Delito, pena, política criminal y tecnología de la información y la comunicación en las modernas ciencias penales*, pág. 39. Salamanca: Ediciones Universidad de Salamanca.

SEILER, S. (2022). *Strafrecht Allgemeiner Teil II: Strafen und Maßnahmen*, 10.ª ed. Viena: Verlag Österreich.

SERRANO TÁRRAGA, M.D. (2023). «Lección 15. Los delitos de daños». En: SERRANO TÁRRAGA, M.D. (coord.). *Derecho Penal. Parte Especial*, pág. 530. Valencia: Tirant Lo Blanch.

SOLARI MERLO, M.N. (2013). «El legislador penal ante la innovación tecnológica. Los daños informáticos en el dilema entre la reflexión filosófica y la práctica jurídico científica». En: PÉREZ ÁLVAREZ, F. (ed.). *Delito, pena, política criminal y tecnología de la información y la comunicación en las modernas ciencias penales*, págs. 2011-213. Salamanca: Ediciones Universidad de Salamanca.

VELASCO NÚÑEZ, E. (2019). «Tipos delictivos (Parte Primera)». En: VELASCO NÚÑEZ, E.; SANCHIS CRESTO, C. *Delincuencia informática. Tipos delictivos e investigación con jurisprudencia tras la reforma procesal y penal de 2015*, págs. 51-52. Valencia: Tirant lo Blanch.

VELÁZQUEZ VELÁZQUEZ, F. (2020). *Fundamentos de Derecho Penal. Parte General*, 3.ª ed. Valencia: Tirant Lo Blanch. DOI: https://doi.org/10.2307/j.ctv1k03p43.9

**Cita recomendada**

CRUZ PALMERA, Roberto (2024). «Análisis al concepto de *gravedad* relativo al delito de daños informáticos». *IDP. Revista de Internet, Derecho y Política*, núm. 41. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i41.429600



**Sobre la autoría**

Roberto Cruz Palmera
Universidad de Valladolid
rcruz@uva.es

Profesor ayudante doctor de Derecho Penal en la Universidad de Valladolid. Sus líneas de investigación en los últimos años abarcan temáticas relativas a la Parte General del Derecho Penal (por caso, la preparación delictiva, la tentativa, los actos preparatorios) y a la Parte Especial del Derecho Penal (por caso, el estudio del delito de nombramiento ilegal, el delito de cohecho, el delito de *grooming* o ciberacoso sexual a menores, entre otros). En la actualidad, cuenta con cuatro monografías de autoría única, más de una veintena de artículos en revistas especializadas y numerosos capítulos de libro en obras colectivas, tanto en España como en el extranjero.