República de Colombia
Corte Suprema de Justicia
Sala de Casación Penal

FERNANDO LEÓN BOLAÑOS PALACIOS

Magistrado Ponente

SP2699-2022

Radicación n° 59733

Aprobado según acta n° 176

Bogotá, D.C., tres (3) de agosto de dos mil veintidós (2022).

ASUNTO

Se resuelve la impugnación promovida por el defensor de GREIS KATERIN GUTIÉRREZ SOLANO contra la sentencia de segunda instancia proferida el 12 de noviembre de 2019 por el Tribunal Superior de Bucaramanga, mediante la cual revocó la decisión de absolver a la acusada y, en su lugar, la condenó como autora del delito de *daño informático*.

ANTECEDENTES

1. Fácticos

Desde el 10 de septiembre de 2012, GREIS KATERIN GUTIÉRREZ SOLANO se desempeñó como trabajadora de la Cooperativa de Transportadores de Tanques y Camiones para Colombia «COVOLCO» en la ciudad de Bucaramanga, primero, como analista de la oficina de recursos humanos y, a partir del 1 de agosto de 2014, como jefa de esa misma dependencia.

El 27 de enero de 2015, después de ser notificada que sería despedida a partir del día siguiente por decisión unilateral de su empleador; la trabajadora, cuya jornada laboral finalizaba a las 6:00 p.m., entre las 5:16 y las 5:26 p.m. manipuló el equipo servidor que almacenaba la información del área de recursos humanos -conectado en red con otros 3 dispositivos- y procedió a mover 64 archivos desde su ubicación en una carpeta compartida denominada NAS hasta la «papelera de reciclaje»[1].

[1] La papelera de reciclaje *«permite el almacenamiento temporal de archivos borrados, que pueden ser recuperados mientras que permanezcan en ella. Desde la papelera se pueden restaurar los archivos o carpetas al lugar del cual fueron borrados»*. AA.VV. *Informática básica*, 1ª ed., Escuela Judicial Rodrigo Lara Bonilla – Consejo Superior de la Judicatura., Bogotá, 2007, p. 27.

Con motivo del mencionado despido, la misma tarde presentaron renuncias a sus cargos Jhessica Paola García Pulido y Charys Viviana Bernal Medina, quienes también laboraban en la oficina de recursos humanos.

Al día siguiente, cuando Diana Marcela Blanco Correa, quien reemplazó en el cargo a GREIS KATERIN GUTIÉRREZ SOLANO, comunicó que no encontraba los archivos del equipo servidor, el consejo de administración de COVOLCO prohibió la manipulación del dispositivo, inclusive por el jefe de sistemas de la empresa, hasta que fuera examinado en el marco de una investigación.

2. Procesales

2.1 El 25 de noviembre de 2015, ante el Juzgado 6 Penal Municipal de Bucaramanga con función de control de garantías, se formuló imputación en contra de GREIS KATERIN GUTIÉRREZ SOLANO, Jhessica Paola García Pulido y Charys Viviana Bernal Medina, como coautoras de *daño informático* (modalidad «borrar»).

2.2 Presentado el escrito de acusación, el 26 de octubre de 2016 el Juzgado 2 Penal Municipal de Bucaramanga, con función de conocimiento, celebró audiencia durante la cual la Fiscalía formuló acusación por el mismo delito, aunque adicionó el verbo rector «suprimir».

En la misma diligencia, se autorizó la intervención como víctima a la Cooperativa de Transportadores de Tanques y Camiones para Colombia «COVOLCO».

2.3 El 13 de julio de 2017 tuvo lugar la audiencia preparatoria.

2.4 El juicio oral se realizó en varias sesiones los días 23 de febrero y 31 de octubre de 2018; 15 y 20 de febrero, 26 de abril y 10 de mayo de 2019.

2.5 En la última fecha, el Juzgado anunció que la decisión sería absolutoria para las 3 acusadas y el 28 de junio de 2019 profirió la respectiva sentencia.

2.6 Con motivo de los recursos de apelación que interpusieron fiscalía y víctima, la Sala Penal del Tribunal Superior de Bucaramanga, en fallo del 12 de noviembre de 2019, confirmó la absolución de Jhessica Paola García Pulido y Charys Viviana Bernal Medina, pero revocó la de GREIS KATERIN GUTIÉRREZ SOLANO.

2.7 Así, la corporación de segunda instancia condenó a la última como autora de *daño informático* (únicamente por «borrar» datos) y le impuso las penas de prisión por 48 meses -suspendida en forma condicional-, multa por 100 s.m.l.m.v. y la accesoria de inhabilitación para el ejercicio de derechos y funciones públicas por el mismo término de la inicial.

2.8 La acusada condenada por vez primera formuló impugnación especial; sin embargo, como no fue sustentada por ella ni por el defensor público que se le asignó cuando revocó el poder a su representante de confianza, el Tribunal la declaró desierta el 27 de mayo de 2020.

2.9 Esa determinación fue revocada el 18 de junio de 2020 por virtud del recurso de reposición instaurado por la misma procesada, quien, restablecido el término, lo aprovechó para sustentar directamente la inconformidad.

2.10 El proceso fue remitido a la Corte, pero esta, mediante auto AP066-2021 (ene. 6), decretó la nulidad por violación al derecho a la defensa técnica, a partir del momento en que GREIS KATHERIN GUTIÉRREZ SOLANO activó la garantía de doble conformidad.

2.11 Una vez el Tribunal Superior de Bucaramanga aseguró la designación de un defensor público, este sustentó la impugnación especial el 14 de mayo de 2021. En la misma fecha, un defensor nombrado por la acusada procedió en igual forma.

2.12 La referida corporación judicial concedió el recurso el 26 de mayo de 2021 privilegiando la sustentación proveniente del defensor de confianza.

ARGUMENTOS DE IMPUGNACIÓN

3. El experto Francisco Jaimes Gutiérrez informó que en la carpeta de reciclaje se encontraron 64 archivos enviados allí el 27 de enero de 2015; pero, el análisis de las pruebas deja duda sobre si la acusada fue la autora de ese traslado pudiendo haberlo sido cualquier otro empleado de la empresa, por las siguientes razones:

- Diana Marcela Blanco Correa declaró que vio a aquella manipular la computadora, pero no que ejecutara la acción de *«limpiar»*; además, fue desmentida por el perito antes mencionado cuando aseguró que *«no había carpetas en la basura, en el basurero del equipo no había nada»*.

- Jorge Alberto Rey Calderón afirmó que la recuperación de los datos solo podía hacerse utilizando programas especializados y que, aun así, no estaba garantizada; declaración que, de igual forma, resultó desvirtuada por el perito. Tampoco es creíble cuando incrimina a la acusada con base en las grabaciones de las cámaras de vigilancia, porque las imágenes no permiten determinar la operación que ejecutaba y los referentes temporales de esos dispositivos no coinciden con los registrados en el movimiento de los archivos.

- Tales testigos solo desean acompañar a los directivos de la empresa en la persecución de la empleada despedida.

- Por último, Kerly Johana Suárez Ramírez y Wolfang Eugenio Peña Díaz no tuvieron conocimiento directo sobre el borrado de archivos y la persona que lo ejecutó.

4. En segundo lugar, «*el hecho de que alguien moviera de una carpeta a otra unos archivos*» no es típico de daño informático porque borrar es «*hacer desaparecer … es que el dato sea desaparecido del servidor, del sistema o de la nube*». Claro que, si lo borrado no es un dato sino «*partes o componentes del sistema lógico o del sistema de información, … si se adecuan a la tipicidad, aunque luego se recuperen, porque ellos alteran el funcionamiento del sistema en general, aun por un momento*».

Entonces, bajo el entendido de que borrar datos significa desaparecerlos y en el caso juzgado estos permanecieron íntegros, la afirmación de la conducta típica vulnera el principio lógico de no contradicción. Otra interpretación es violatoria del principio de legalidad y de la concepción minimalista del derecho penal.

5. Conforme a tales premisas, solicita que se revoque la sentencia condenatoria por atipicidad de la conducta o por duda sobre su autoría.

CONSIDERACIONES

6. Como quiera que GREIS KATHERIN GUTIÉRREZ SOLANO fue condenada -por primera vez- por el Tribunal Superior de Bucaramanga; corresponde a la Corte Suprema de Justicia – Sala de Casación Penal, en la condición de superior funcional, conocer y decidir la impugnación especial promovida por los titulares de la defensa, según lo dispuesto en el artículo 235.7 de la Constitución Política -modificado por el Acto Legislativo 01/2018-.

7. Según los planteamientos del impugnante, habrá de determinarse, en primer lugar, si la conducta por la que se profirió condena es típica del delito de *daño informático*. Y, solo si tal cuestión se resuelve en sentido afirmativo, se procederá, en segundo lugar, a verificar si la prueba del proceso informa más allá de dudas razonables que la acusada es autora del comportamiento delictivo.

Con tal objetivo, previo a abordar el estudio de los argumentos de impugnación se explican las características típicas de la conducta punible en mención, especialmente las relativas a la específica modalidad atribuida a la acusada (borrar datos informáticos).

- Características típicas del delito de *daño informático.*

8. El artículo 269D del Código Penal describe el supuesto de hecho del delito en mención así: *«El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, …».* Dicha conducta constituye uno «de los atentados contra la confidencialidad, la integridad y disponibilidad de los datos y de los sistemas informáticos» (capítulo I, título VII bis).

9. Ese tipo penal busca asegurar, en términos generales, *«la protección de la información y de los datos»*, bien jurídico que fue introducido en el estatuto penal colombiano por la Ley 1273 del 5 de enero de 2009 siguiendo las directrices sustantivas trazadas por el Convenio sobre la Ciberdelincuencia, que es un tratado multilateral suscrito en Budapest el 23 de noviembre de 2001 por los Estados miembros del Consejo de Europa (y por 4 Estados no miembros: Canadá, Japón, Sudáfrica y Estados Unidos de América).

10. Así lo explicó el informe de ponencia para primer debate al entonces proyecto de ley número 042 Cámara, 123 Cámara y Senado acumulados:

> Se trata, en otras palabras, de que el ordenamiento penal colombiano se sume a las políticas penales globalizadas en materia del combate frontal contra la llamada criminalidad del ciberespacio y le brinde herramientas a la comunidad

> internacional para la persecución de estos flagelos; al mismo tiempo, se busca brindar una adecuada tutela jurídica a un bien jurídico de tanta trascendencia en el mundo de hoy como lo es el atinente a la Protección de la Información y de los Datos.
>
> Este proyecto está llamado a modernizar la legislación penal colombiana y a ponerla a la par de la de otros países, como los que integran la comunidad económica europea, que se viene desarrollando a partir de acuerdos internacionales tan importantes como el Convenio sobre cibercriminalidad suscrito en Budapest (…). Si bien, por razones obvias, Colombia no forma parte de ese organismo, ni tampoco ha firmado el susodicho Convenio, **es de vital importancia que la normatividad a expedir recoja esas directrices**, que son, además, las que las legislaciones europeas y de otros continentes empiezan a introducir en los respectivos ordenamientos jurídicos.[2] (*Negritas fuera del texto original*)

11. Años después el Convenio de Budapest, como también se le conoce, fue aprobado por el Estado colombiano a través de la Ley 1928 del 24 de julio de 2018, a partir de la invitación a adherirse que le extendiera el Consejo de Europa. Durante el respectivo debate legislativo se recordó que aquel *«es el primer tratado internacional que aborda la definición de los delitos cometidos a través de redes informáticas, …»*[3]. Tanto el convenio como su ley aprobatoria fueron declarados exequibles por la Corte Constitucional mediante sentencia C-224/2019.

12. Así las cosas, en la adecuada comprensión y aplicación de los delitos informáticos o relacionados con el empleo de ordenadores (título VII bis Código Penal), resulta de gran ayuda la remisión al contexto normativo previsto en el Convenio de Budapest, el cual, vale agregar, reguló no solo

[2] Gaceta del Congreso No 528 de 2007, p. 2.

[3] Gaceta del Congreso No 403 de 2018, p. 2.

aspectos sustantivos sino también de índole procedimental y de cooperación internacional en la lucha contra esa forma especializada de delincuencia transfronteriza.

13. La sección 1 del capítulo II de dicho Convenio tiene como «delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos», los siguientes: *«acceso ilícito»* (art. 2), *«interceptación ilícita»* (art. 3), ***«ataques a la integridad de los datos»*** (art. 4), *«ataques a la integridad del sistema»* (art. 5) y *«abuso de los dispositivos»* (art. 6).

14. De modo similar, el capítulo I del título VII bis del código nacional enlistó «los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos», así: *«acceso abusivo a un sistema informático»* (art. 269A), *«obstaculización ilegítima de sistema informático o red de telecomunicación»* (art. 269B), *«interceptación de datos informáticos»* (art. 269C), ***«daño informático»*** (art. 269D), *«uso de software malicioso»* (art. 269E), *«violación de datos personales»* (art. 269F) y *«suplantación de sitios web para capturar datos personales»* (art. 269G).

15. El delito de *daño informático*, también denominado «sabotaje informático», cobijó los ataques a la integridad de los datos definidos por el Convenio de Budapest como *«la*

comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos» (art. 4); claro está, con algunas particularidades: (i) radicó la ilegitimidad del sujeto activo en la carencia de facultad o autorización para realizar las acciones, y (ii) agregó un verbo rector (*«destruir»*) y un objeto (*«un sistema de tratamiento de información o sus partes o componentes lógicos, …»*), ambos de carácter alternativo.

16. De esa manera, en Colombia son 2 grupos de conductas los constitutivos de *daño informático*: (i) destruir, dañar, borrar, deteriorar, alterar y suprimir un dato informático, y (ii) destruir, dañar, borrar, deteriorar, alterar y suprimir un sistema de información; en ambos eventos sin que el sujeto agente cuente con autorización para realizar tales comportamientos.

Junto a esos ataques a la **integridad** de los datos y de los sistemas, el Código Penal castiga los atentados al **funcionamiento y acceso** a los mismos, pero en el ámbito de otro tipo: el contemplado en el artículo 269B que prohíbe la conducta de quien *«sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, …».*

17. Esos 2 objetos posibles de las acciones típicas referidas o, lo que es igual, las cosas o bienes (tangibles o

intangibles) sobre las que aquellas pueden recaer; fueron definidos en el artículo 1 del tratado multilateral que, recuérdese, hoy día es vinculante en el ordenamiento jurídico interno dada su aprobación por el Congreso de la República mediante la Ley 1928/2018, así:

> a) Por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;
>
> b) por "datos informáticos" se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

18. Y, en relación con el alcance de los verbos rectores del delito de *daño informático* resulta pertinente la remisión al «Informe explicativo del Convenio de Budapest» (STE núm. 185), un documento también aprobado por el Comité de Ministros del Consejo de Europa y cuya finalidad es, precisamente, facilitar la aplicación de dicho instrumento. Así lo declaró el citado órgano comunitario:

> I. El Convenio y su Informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión (8 de noviembre de 2001) y el Convenio fue abierto a la firma en Budapest, el 23 de noviembre de 2001, con motivo de la celebración de la Conferencia Internacional sobre la ciberdelincuencia.
>
> II. El texto de este informe explicativo no constituye un instrumento que ofrezca una interpretación autorizada del Convenio, aunque por su naturaleza tal vez facilite la aplicación de las disposiciones contenidas en el mismo.

19. Con tal propósito, el memorial explicativo aclaró, en primer lugar, el fin de protección de la norma sustantiva que proscribe las distintas formas de interferencia en los datos (num. 60):

> La finalidad de esta disposición es proporcionar a los datos informáticos y a los programas informáticos una protección similar a la que gozan los objetos corpóreos contra la imposición de un daño deliberado. El interés legal protegido en este caso es la integridad y el correcto funcionamiento o utilización de los datos almacenados o de los programas informáticos.

20. Y, una vez precisó el contexto teleológico, delimitó el ámbito de cada una de las acciones que puede afectar la integridad de los datos informáticos (num. 61):

> …, los términos que "dañe" y "deteriore" como actos imbricados se refieren en particular a una alteración negativa de la integridad o del contenido de la información de los datos y programas. El "borrar" datos es el equivalente de la destrucción de un objeto corpóreo. Los destruye y los hace irreconocibles. Por "supresión" de datos informáticos se entiende cualquier acción que impida o ponga fin a la disponibilidad de los datos para la persona que tiene acceso al ordenador o al soporte de datos en que fueron almacenados. El término "alteración" se refiere a la modificación de los datos existentes. Por consiguiente, la introducción de códigos maliciosos, tales como virus y caballos de Troya, está incluido en este párrafo, tal como también lo está la modificación resultante de los datos.

21. En el análisis del caso que ocupa la atención de la Corte, por ser la modalidad típica que fundó la decisión condenatoria, es importante resaltar que *«el "borrar" datos es el equivalente de la destrucción de un objeto corpóreo. Los destruye y los hace irreconocibles.»*. Esa definición se

acompasa con la semántica del verbo que, según el Diccionario de la Real Academia Española, es *«hacer desaparecer por cualquier medio lo representado con tiza, tinta, lápiz, etc.»*, siendo una de estas otras formas adicionales de representación las simbólicas propias de la información digital.

22. Habrá de entenderse, entonces, que será típica de *daño informático* por «borrar» datos, la conducta consistente en desaparecerlos o quitarlos de modo definitivo del dispositivo o sistema de tratamiento donde se encuentren almacenados, tornándolos irrecuperables.

Un archivo digital está guardado cuando su contenido (bytes) permanece en el medio magnético. Al eliminar un archivo, el medio magnético no elimina su contenido si no que pierde su referencia o dirección de ubicación. Un borrado seguro o eliminación definitiva se da cuando se sobreescribe o se reemplaza la información donde se encontraba almacenado el archivo.

Como quiera que, según las directrices expuestas, el borrado de datos requerirá siempre la producción de un resultado material; es claro que esta modalidad delictiva admitirá la tentativa cuando el agente inicie su ejecución mediante actos idóneos e inequívocos y aquel no se produzca por causas ajenas a su voluntad (art. 27 C.P.).

23. No ha de olvidarse que el principio de lesividad solo permite tener por delictivos los comportamientos que causen o puedan ocasionar un menoscabo **efectivo** del bien jurídico que busca proteger el tipo penal (art. 11 C.P.) y que, en la misma línea, el principio de fragmentariedad restringe el castigo penal a los atentados de mayor intensidad. En consecuencia, el daño a la integridad del dato debe revestir cierta **gravedad** porque si es inocuo, insignificante o aparente para la seguridad informática no será típico siquiera.

23.1 El mismo Convenio de Budapest dispuso que las partes podían reservarse el derecho a castigar solo las interferencias de datos que comportaran *«daños graves»* (art. 4.2). Y, a pesar de que el artículo 269D no incluyó en su literalidad ese requisito, el mismo deriva, reitérese, del principio de lesividad, más aún cuando todo indica que fue esa la intención del legislador colombiano porque así lo reiteraron los ponentes, por lo menos, en 3 de las sesiones de debate a la Ley 1273/2009[4]:

> En el artículo 269D se prevé la conducta de daño informático, mediante la que se castiga la **obstaculización grave**, cometida de forma dolosa y sin autorización, contra el funcionamiento de un Sistema Informático, a través de la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos, o mediante la realización de esas conductas en relación con un sistema de tratamiento de información o sus partes o componentes lógicos. (…).

[4] Así consta en las Gacetas del Congreso No 528 de 2007 (p. 3), 645 de 2007 (p. 6) y 911 de 2008 (p. 4).

23.2 Inclusive, el proyecto de ley No 100 de 2009 Cámara, que muy tempranamente intentó modificar la redacción de los delitos consagrados en el título VII bis, incluía la exigencia de *«daño sustancial»* con el objeto de *«evitar el castigo (por puro peligro) de comportamientos poco lesivos o de actos que no implican un verdadero daño en sentido informático (lógico), pues no es lo mismo el daño de objetos muebles e inmuebles que el daño de datos»*[5].

Con ese propósito, se sugería que el artículo 269D quedara así: *«El que dañe, destruya o altere **de modo sustancial** datos informáticos o un sistema de tratamiento de información o sus partes o componentes lógicos, …»*[6]. A pesar de que esta propuesta de reforma legal no trascendió, sí denota la preocupación originaria del legislador nacional por castigar daños informáticos relevantes, significativos o sustanciales.

23.3 En el derecho comparado, resulta paradigmático el caso de España cuyo estatuto penal condiciona la tipicidad del daño informático a un doble juicio de gravedad: el de la acción y el del resultado, exigencia que parece excesiva y conlleva algunas dificultades interpretativas como lo ha

[5] Gaceta del Congreso 691 de 2009.
[6] Ibidem.

reconocido el Tribunal Supremo de ese país[7], pero que resulta muy importante para remarcar la necesidad de excluir interferencias informáticas inocuas, insignificantes o irrelevantes. En efecto, dispone el artículo 264 ibidem:

> 1. 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 texto original*)

Ese especial requisito del daño informático ilícito ha sido explicado por el Tribunal Supremo de España en los siguientes términos:

> La primera conclusión a la que conduce el análisis del tipo es que los daños informáticos son atípicos cuando el resultado -en su descripción más básica- no es grave. (…). Se trata de una gravedad por el daño funcional que entorpece el sistema operativo. La constatación de ese daño será evidente, claro es, cuando sea imposible recuperar la plena operatividad del sistema. También podrá entenderse que se alcanza la gravedad típica -con inspiración en la Circular de la Fiscalía General del Estado núm. 3/2017- en supuestos en los que el retorno operativo del sistema exija grandes esfuerzos de dedicación técnica y económica.[8]

---

[7] *«La gravedad se adueña de la descripción del tipo básico y de los tipos agravados. No basta con que el resultado sea grave, lo ha de ser también la acción de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesible el sistema o los datos que éste incorpora. No es fácil modular la gravedad de una acción sin la referencia que proporciona su resultado que, al exigirlo el legislador, ha de ser también grave. Se trata pues, de una gravedad encadenada, acumulativa, que no siempre podrá afirmarse sin dificultad. (…).».* STS 220-2020 del 22 de mayo (proceso 3019-2018).
[8] Ibidem.

23.4 A nivel internacional también se expresan voces de doctrinantes en el mismo sentido con fundamento en las directrices del Convenio de Budapest:

> … la relevancia jurídico penal de la destrucción o inutilización de datos de sistemas informáticos, relevancia que normalmente se identifica con la gravedad de dicho comportamiento en atención a la naturaleza de los datos (v. gr. militares, científicos, artísticos o meramente triviales); su volumen (gran o escasa cantidad de datos); las posibilidades de recuperarlos (por ejemplo, porque se encuentran respaldados); etc. Dicha exigencia típica no sólo se plantea en el Convenio sobre Ciberdelincuencia del Consejo de Europa, de 2001 (véase Declaraciones al Convenio, así como sus artículos 4° y 5°), sino que también es postulada a nivel doctrinal, para limitar la tipicidad de un comportamiento que, a diferencia de los daños comunes, no se encuentra asociado a la cuantía del objeto dañado.[9]

24. Una cuestión de especial atinencia para el caso que se juzga es si la posibilidad de restauración o recuperación de los datos excluye la tipicidad de la conducta de *daño informático* en la modalidad de «borrar».

24.1 La Corte no pretende dar una respuesta absoluta al tema, entre otras razones, porque el tipo penal en mención describe un número amplio de hipótesis alternativas, de manera que, por ej., lo que se concluya respecto al borrar datos quizás no sea aplicable de manera automática cuando esta conducta recae en un sistema informático. Además, la velocidad exponencial de los avances tecnológicos conlleva

---

[9] MAYER, Laura; VERA, Jaime. *El documento como objeto material de las falsedades documentales y del sabotaje informático en el Derecho penal chileno*. Polít. crim. Vol. 14, Nº 27 (Julio 2019), Art. 12, pp.419-455[http://politcrim.com/wpcontent/uploads/2019/05/Vol14N27A12.pdf], pie de página 435.

un ritmo igualmente acelerado de su uso por parte de los delincuentes cibernéticos; por tanto, existirán comportamientos humanos que puedan configurar daños informáticos que aun hoy escapan a la imaginación.

24.2 De otra parte, no puede olvidarse que la materia de los cibercrímenes es una creación legislativa de época reciente, tanto a nivel nacional como internacional, que en muchas de sus particularidades no alcanza a explicar de manera satisfactoria la tradicional teoría del delito, especialmente porque acontecen, por regla general, no en el mundo físico sino en el ciberespacio con todo lo que esto implica en el ámbito de la conducta penalmente relevante.

25. Siendo así, se formularán unas consideraciones generales y la posición que finalmente se adopta es la que resuelve la singularidad de la situación jurídica (*daño informático* por borrar datos) y fáctica (mover archivos desde su ubicación original en el dispositivo hasta la «papelera de reciclaje») que ahora se estudia.

25.1 De acuerdo al espíritu y finalidad de la legislación internacional, acogida por Colombia primero como referente técnico y después como norma vinculante, con la prohibición de las interferencias a los datos informáticos se busca proteger, principalmente, la integridad de estos y las plurales formas de atentados suponen distintos grados de afectación a ese bien jurídico; así, por regla general, el borrado y la supresión acarrean el máximo daño (destrucción o

desaparición), mientras que el deterioro y la alteración suponen uno parcial o de menor entidad.

25.2 Según esos criterios de interpretación aunado al literal derivado del significado del verbo «borrar», la conservación integral del dato o archivo en el dispositivo de almacenamiento desvirtúa su desaparición y, con ello, la consumación de la acción típica aludida, pero también, en principio, de cualquier otra de las que configura el delito porque el bien jurídico (integridad del dato) se mantuvo a salvo y ni siquiera corrió peligro. Claro está, diferente sería que la posibilidad de restauración sea solo parcial porque en este evento sí se habrá materializado la lesión, aunque no por la vía del borrado sino del deterioro o alteración.

26. Ahora, podría oponerse que la eliminación así sea temporal de un dato o archivo de su ubicación en el dispositivo de almacenamiento de que se trate (disco duro p. ej.) entorpece o dificulta la accesibilidad o disponibilidad de tales formas de representación simbólica de la información, siendo esta otra cualidad o faceta del bien jurídico protegido como bien lo indica la denominación del capítulo I del título VII bis del Código Penal. Tal argumento es válido, pero amerita las siguientes precisiones:

26.1 Los delitos introducidos por la Ley 1273/2009 (título VII bis), ciertamente, constituyen «atentados contra la confidencialidad, la integridad y la disponibilidad de los

datos y sistemas informáticos»; sin embargo, no todos afectan simultáneamente esos 3 componentes de la seguridad informática o, por lo menos, no lo hacen en la misma medida, de modo similar a lo que ocurre con las plurales formas de ataque al bien jurídico de la libertad, integridad y formación sexuales (título IV).

Así, por ejemplo, es evidente que la *«interceptación de datos informáticos»* lesiona, principalmente, la confidencialidad; el *«daño informático»*, la integridad del dato o del sistema; y la *«obstaculización ilegítima de sistema informático o red de telecomunicación»*, la disponibilidad de estos.

26.2 Aun cuando los supuestos típicos del *daño informático* (destruir, dañar, borrar, deteriorar, alterar y suprimir), suponen también al final un menoscabo a la disponibilidad de los datos; esto ocurre de manera indirecta o colateral porque los verbos rectores alternativos entrañan -y presuponen-, en primerísimo lugar, un atentado a la integralidad de aquellos.

26.3 Por si lo anterior fuera poco, la conducta de **impedir u obstaculizar el *«acceso normal*** *a un sistema informático,* ***a los datos informáticos allí contenidos****, …»,* constituye un tipo autónomo (art. 269B) cuya salvaguarda prioritaria, como se desprende de la misma descripción

típica, sí es la disponibilidad de los datos -y de los sistemas tecnológicos de la información y las comunicaciones-.

27. En gracia de discusión, podría admitirse la tipicidad de un borrado temporal de datos informáticos cuando la recuperación o restauración de estos sea onerosa porque demande la adquisición de personal o programas especializados o porque tarde mucho tiempo, p. ej.

27.1 Pero, aun esa hipótesis no excluye que si lo ejecutado fue la eliminación del dato no del ordenador sino de un directorio o carpeta específicos -lo que en sentido estricto no constituye una acción de borrar ni de ninguna otra de *daño informático*- y este se pueda restaurar -en su total extensión- con relativa facilidad a su ubicación original en el disco duro; la conducta es atípica porque no tendría la más mínima idoneidad para afectar la integridad del dato y tampoco su disponibilidad.

27.2 Así ocurre, p. ej., cuando a pesar de que el lenguaje técnico denomine a la acción *«borrar»* o *«eliminar»*, esta solo consista en el traslado del archivo desde su posición original de almacenamiento en el disco duro hasta la «papelera de reciclaje», carpeta esta que, de no intentarse su vaciado, permite un retorno inmediato e íntegro de aquel. Ello es así porque, recuérdese, ese compartimento constituye un espacio de *«almacenamiento temporal de archivos borrados, que pueden ser recuperados mientras que permanezcan en*

ella»[10], es decir, desde ella *«se pueden restaurar los archivos o carpetas al lugar del cual fueron borrados»*[11].

27.3 En todo caso, cualquiera sea el sentido o alcance que se asigne a los verbos rectores alternativos del tipo de *daño informático*, algunos de los cuales parecen redundantes o que se sobreponen[12], lo que deviene incuestionable es que ninguno de aquellos podrá sancionar la conducta que carece de idoneidad para lesionar o poner en peligro efectivamente la integridad de los datos informáticos almacenados en un dispositivo, que es el bien jurídico principal que busca proteger la prohibición típica.

28. Antes de pasar al estudio del caso sometido a decisión, importante resulta traer a colación fragmentos de la sentencia de casación 220/2020 (proceso 3019-2018) en la que el Tribunal Supremo de España absolvió al acusado del ilícito de *daño informático* por considerar que la recuperación de los archivos, a los que inclusive modificó el nombre, en la «papelera de reciclaje» no configuraba un daño típicamente relevante. Así describió los hechos juzgados en lo que resulta pertinente:

---

[10] AA.VV. *Informática básica*, 1ª ed., Escuela Judicial Rodrigo Lara Bonilla – Consejo Superior de la Judicatura., Bogotá, 2007, p. 27.
[11] Ibidem.
[12] El proyecto de ley No 100 de 2009 Cámara propuso reducir las acciones típicas a «dañar», «destruir» y «alterar» con la siguiente justificación: *«A su vez, se introduce el delito de daño informático en el artículo 269D del C. P., al que se le da una redacción en la que se opta por simplificar los verbos rectores, algunos redundantes o previstos por otros comportamientos.»* (Gaceta del Congreso 691 de 2009).

> Esa tarde en que el acusado permaneció en su despacho aprovechó para acceder a su ordenador y usuario y borrar de su ubicación en la carpeta "escritorio" 54 carpetas que contenían 1074 archivos informáticos, … que contenían documentos relacionados con el funcionamiento de la oficina (…).
>
> (…).
>
> Dichos archivos, a los que el acusado les había cambiado previamente la denominación y el icono, pudieron finalmente ser recuperados el lunes 13 de julio por el informático Sr. Anibal en la papelera de reciclaje del equipo del Sr. Luis, en donde habían sido ubicados por el sistema operativo tras su eliminación.

Y así descartó la relevancia típica de ese suceso:

> No resulta fácil, a partir de esa descripción, concluir la gravedad de una acción de borrado y de cambio de la denominación de los archivos que, una vez eliminados, quedaron incluidos en la papelera de reciclaje y fueron ahí recuperados. Ni los daños, ni la perturbación del sistema, ni su gravedad -todos ellos, elementos del tipo objetivo- se incluyen en el factum.
>
> (…).
>
> (…). El borrado de 54 carpetas que incluyen 1074 archivos, que al ser eliminados se alojan en la papelera de reciclaje y sobre los que el acusado no vuelve a intentar ninguna acción destructiva, no alcanza la relevancia típica exigida por el art. 264.1 del CP.

Inclusive, desechó la posibilidad de considerar que lo ejecutado fuera punible a título de tentativa:

> La Sala no puede aceptar ese razonamiento que, si bien se mira, elude la gravedad del resultado -presupuesto del tipo- degradando los hechos a un delito intentado. No existe obstáculo conceptual para apreciar un tipo de imperfecta ejecución, (…). En el presente caso, el resultado se produjo. Luis hizo todo aquello que quería hacer. Y esa acción produjo el resultado asociable a su verdadera entidad, que no es otro que el traslado a la papelera

de reciclaje de los archivos borrados y su eventual recuperación por todo usuario que así lo quisiera.

Se reitera, a pesar de que es diferente la literalidad del tipo de *daño informático* en España, la exigencia de que este comporte cierta gravedad (en la acción y/o en el resultado) para que pueda predicarse su potencialidad de vulnerar los componentes de la seguridad informática, especialmente, la integridad de los datos y de los sistemas; debe entenderse también incorporada en la ley penal colombiana.

- Examen del argumento de atipicidad en el caso juzgado.

29. La premisa fáctica de la condena consistió en que GREIS KATHERIN GUTIÉRREZ SOLANO, una vez notificada de que había sido despedida por su empleadora, sin tener autorización para ello, removió 64 archivos de su ubicación en una carpeta compartida NAS, relativos a diferentes temas del área de recursos humanos que ella dirigía, los cuales quedaron alojados en la «papelera de reciclaje»[13] del disco duro[14] del equipo servidor de esa dependencia[15].

[13] Reitérese que la papelera de reciclaje *«permite el almacenamiento temporal de archivos borrados, que pueden ser recuperados mientras que permanezcan en ella. Desde la papelera se pueden restaurar los archivos o carpetas al lugar del cual fueron borrados»*. AA.VV. *Informática básica*, … Ob. cit., p. 27.
[14] Marca Seagate Barracuda, serial No 9VMBFAQJ, 320 gigas.
[15] Equipo marca DELL Optiplex 780.

30. En punto de la tipicidad, la sentencia de segunda instancia consideró que el delito de *daño informático* no presupone la *«pérdida definitiva de los archivos cuya eliminación se pretendió»*[16]; por tanto, la conducta examinada es típica desde el momento en que esos datos fueron *«quitados del sistema de tratamiento de los mismos, el cual para el caso … era Network Attachaed Storage, tecnología de almacenamiento conectado en red desde un servidor, el cual se permitía recopilar y recuperar datos desde otros computadores»*[17].

Además, advirtió, la papelera de reciclaje es un *«área de almacenamiento* [que] *guarda los archivos previa supresión definitiva, siendo una medida para evitar el borrado accidental de datos»*[18].

Por último, indicó que esa operación fue ejecutada por la acusada de manera abusiva porque la autorización de la Cooperativa *«incluía el acceso y manejo de los datos informáticos en aras de cumplir con sus ocupaciones como jefe de recursos humanos, …, no así la de eliminar los archivos almacenados en la Network Attachaed Storage (NAS), dado que evidentemente dicho proceder afectaría el trabajo de la dependencia a la cual se encontraba adscrita»*[19].

---

[16] Página 27, sentencia de segunda instancia.
[17] Ibidem.
[18] Página 28, ibidem.
[19] Página 36, ibidem.

31. Por el contrario, el fallo de primera instancia había concluido que los hechos eran atípicos, básicamente, porque se demostró que los 64 archivos reposaban en la papelera de reciclaje; o sea, que *«estaban en el equipo, si bien es cierto, en una ubicación diferente, de fácil recuperación para el usuario, …»*[20]. En ese orden, *«la acción realizada por la investigada Greis Katerin fue pasar dichos archivos a otra carpeta, dentro de la misma plataforma informática conocida como el TRASH CAN (papelera de reciclaje)»*[21].

Adicionalmente, recordó que el motivo por el cual no se recuperó la información de manera inmediata y sencilla no fue la acción de la acusada sino, exclusivamente, la decisión del empleador:

> …, si los directivos de la empresa COVOLCO hubiesen permitido al ingeniero de sistemas JORGE REY CALDERON, vinculado a dicho establecimiento, examinar el equipo, hubiera encontrado los archivos en el dispositivo, evitando los costos que dice se causaron, ese fue el querer de la directiva y como dice el profesional la orden del Consejo fue "que no hiciera absolutamente nada", entonces, para una persona con conocimientos mínimos en informática sabe que con ubicar cualquier archivo en la papelera de reciclaje y dar clic en restaurar, de inmediato vuelven los archivos a su lugar…[22]

[20] Página 23, sentencia de primera instancia.
[21] Página 24, ibidem.
[22] Ibidem.

32. En ambas sentencias se tienen como premisas probatorias indiscutibles, las que tampoco son controvertidas por impugnante en esta oportunidad:

32.1 Que el perito Helver Francisco Jaimes Gutiérrez examinó el disco duro del equipo servidor del área de recursos humanos de COVOLCO y en este encontró, **alojados en la «papelera de reciclaje»**, un total de 64 archivos con nombres tales como: *«novedades conductores»*, *«dotación 2014»*, *«llamados de atención»*, *«liquidaciones y desprendibles»* *«nómina»*, *«procesos disciplinarios»*, *«seguridad social»*, *«vehículos»*, *«carnets por entregar»*, *«cesantías 2012»*, *«correspondencia consejo»*, *«autorización horas extras y suplementarios»* y *«control de permisos»*, entre otros.

Agréguese que el perito dictaminó que tales archivos se conservaron íntegros explicando que *«… el hash es la identificación única, como la huella digital de cada archivo, este hash no se repite, es un código único para este archivo, y que nos da la integridad de que este archivo no ha sido modificado»*[23].

Siendo así, le asiste razón al defensor cuando alega que el supuesto fáctico anotado desvirtúa los siguientes contenidos probatorios:

[23] A partir del minuto 16:28, sesión de juicio oral del 31.10.2018.

(i) El testimonio de Diana Marcela Blanco Correa, quien reemplazó en el cargo a GREIS KATERIN GUTIÉRREZ SOLANO, cuando aseguró que en los computadores *«no había información, estaban en limpio, solo los programas propios del equipo Windows, Word, Paint, pero* ***no había carpetas en la basura, en el basurero del equipo no, no había nada»***[24]. Y,

(ii) El testimonio de Jorge Alberto Rey Calderón, jefe de sistemas de la empresa, cuando afirmó que la recuperación de los archivos presuponía la adquisición de programas informáticos especializados y que, aun así, no había certeza sobre el éxito de dicho procedimiento.

32.2 Que enteradas las directivas de la empresa al día siguiente (27 de enero de 2015) que la carpeta compartida NAS se encontraba vacía, prohibieron que se ejecutaran operaciones en el equipo servidor; por lo que, a pesar de que el ingeniero Jorge Alberto Rey Calderón pensó en recuperar la información de manera inmediata, ni siquiera pudo intentarlo. Así lo declaró este en juicio: *«en el momento en que se pudo verificar que la información no estaba, lo primero que uno piensa es recuperar la información, pero la orden del*

[24] Minutos 18:15 - 18:32, sesión de juicio oral del 20.02.2019.

Consejo fue que no se hiciera absolutamente nada al equipo porque ellos iban a tomar medidas …»[25].

La misma sentencia condenatoria así lo reconoció al valorar el referido testimonio:

> **Documentos que no fueron restablecidos por orden del Consejo de la Cooperativa**, cuyos integrantes advirtieron que tomarían las acciones correspondientes, motivo por el cual se optó por la conservación del computador en el departamento de sistemas, sin que se pudiere hacer un cambio rápido de los datos existentes en el mismo, pues que, *«el equipo se desconectó, se dejó solamente la CPU y para poder ingresar se necesitaba el usuario y la contraseña, si se quisiera utilizar pero quedó aparte»* (Record: 1:42:24 a 1:42:56), hasta que acudió la Fiscalía para extraer el disco duro, …[26]

33. Sintetizando lo anterior, desde el punto de vista jurídico-penal, la acción de GREIS KATERIN GUTIÉRREZ SOLANO consistió, exclusivamente, en trasladar 64 archivos desde la carpeta NAS a la «papelera de reciclaje» del equipo servidor, la totalidad de los cuales permaneció inalterada.

Mal puede afirmarse, entonces, que la acusada «borró» datos informáticos porque ni estos desaparecieron del dispositivo de almacenamiento (disco duro del equipo servidor en red) ni se tornaron ilegibles; por el contrario, se insiste, se conservaron íntegros. Y, la razón por la que no fueron restaurados a su ubicación original de manera

---

[25] Minuto 1:20:47, sesión de juicio oral del 31.10.2018.
[26] Página 14, sentencia de segunda instancia.

inmediata, y quizás muy sencilla, fue que los directivos de la empresa impidieron cualquier intento de hacerlo. De esa manera, la eventual afectación a la disponibilidad de los datos no obedeció al comportamiento de la procesada sino a una medida de su empleador.

34. Vale aclarar que aunque la sentencia de segunda instancia, con base en los fotogramas extraídos de los videos de las cámaras de vigilancia, afirma que GREIS KATERIN GUTIÉRREZ SOLANO borró archivos desde su computador y también desde el equipo servidor -asignado a Olga Patricia Rueda-; lo cierto es que el perito informático solo encontró archivos que fueron enviados a la «papelera de reciclaje» el 27 de enero de 2015 entre las 5:16 y las 5:26 p.m., rango este que correspondería con el tiempo, en que según esas mismas imágenes (31 a 44), la acusada manipuló, únicamente, el dispositivo servidor.

Así pues, los archivos fueron removidos desde el mismo equipo que almacenaba los datos informáticos y los compartía en red a los demás computadores de la oficina de recursos humanos, lo que descarta que, como lo concluyó la decisión condenatoria, aquellos desaparecieran del sistema que permitía su procesamiento, pues siempre estuvieron allí solo que en una ubicación diferente. De todas formas, no sobra recordar que un sistema informático puede estar conformado por un *«conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos*

permitan el tratamiento automatizado de datos en ejecución de un programa».

Por último, se insiste, lo atribuido a la acusada no fue la obstaculización del acceso a los 64 archivos, que es una conducta punible diferente (art. 269B) a la de daño informático y que, además, fue resultado de la decisión adoptada por las directivas de COVOLCO de apagar el equipo y no permitir su operación.

35. De otra parte, podría pensarse que la utilización del software «Encase» por parte del perito informático de la Fiscalía para detectar los archivos en la «papelera de reciclaje», permite inferir que esta labor revestía alguna complejidad -como lo dio a entender Jorge Alberto Rey Calderón- y, por ende, que la conducta de la acusada y/o su resultado fueron graves.

Tal inferencia fue desvirtuada con la declaración del mismo experto porque en esta se advierte que el «Encase» es un software de naturaleza forense que, como tal, permite realizar una búsqueda sobre una imagen del disco duro, y no directamente sobre este, con el propósito de evitar el riesgo de alteración de la evidencia[27]. La siguiente fue la explicación

[27] En la Guía No 13 sobre Evidencia Digital, Seguridad y Privacidad de la Información, del Ministerio de las Tecnologías de la Información y las Comunicaciones, 2016, el numeral 11.4 prescribe: *«En un análisis de datos **nunca se debe trabajar sobre la imagen original suministrada**. Debe realizarse una copia master y a partir de esta, se reproducen las imágenes que*

del procedimiento técnico que adelantó, en la que aflora el entendimiento propuesto:

> … en este caso se hace posteriormente una imagen forense para trabajar sobre la imagen, o sea, yo copio y hago una imagen forense, ¿qué es una imagen forense? eso es una copia bit a bit de la información contenida en este disco duro, ya que yo trabajo sobre la imagen forense, yo no trabajo sobre el disco duro. Posteriormente, yo tengo esa imagen forense, **yo trabajo sobre ella para preservar la integridad de este disco duro que vuelve a su respectivo contenedor** …[28]
>
> (…).
>
> Seguido a esto, de la creación de la imagen **se hace la indexación con el software Encase, ¿qué es la indexación? es coger esa imagen y montarla a otro software que nos permite hacer búsquedas de archivos** por carpetas, por fechas de eliminación, se pueden hacer diferentes tipos de filtros para ubicar esta información, …[29]

36. Pasando a otro tema, como se indicó al inicio, la tipicidad del delito de *daño informático* en Colombia demanda un ingrediente normativo consistente en que el sujeto activo carezca de facultades para ejecutar el borrado, supresión o alteración de los datos -o del sistema-, siendo tan importante ese requisito que es el que torna ilegítima la actuación, según lo aclaró el mismo «Informe explicativo del Convenio de Budapest» (numeral 38):

> Una particularidad de los delitos incluidos es el requisito expreso de que la conducta en cuestión sea llevada a cabo de manera "ilegítima". Esto refleja la idea de que la conducta descrita no siempre es punible per se, sino que puede ser legal o justificada,

---

se requieran.». Y, en el numeral 11.2 recomienda utilizar herramientas de extracción de imágenes como Linux dd o **Encase Forensic Software** para *«la generación de las imágenes de datos que conciernen al caso en investigación»* (págs. 19-21).

[28] A partir del minuto 14:38, sesión de juicio oral del 31.10.2018.
[29] A partir del minuto 15:16, ibidem.

> no sólo en aquellos casos en que corresponde aplicar una defensa legal clásica, como el consentimiento, la defensa propia o la necesidad, sino también cuando otros principios o intereses conducen a la exclusión de la responsabilidad penal. El término "ilegítimo" deriva su significado del contexto en que está utilizado. Así, sin restringir la manera en que las Partes pueden aplicar el concepto en su derecho interno, **puede referirse a una conducta realizada sin facultades para hacerlo** (ya sean de orden legislativo, ejecutivo, administrativo, judicial, contractual o consensual) o a una conducta que no está de otro modo comprendida dentro de las justificaciones, excusas y defensas legales establecidas o los principios pertinentes con arreglo a las leyes nacionales.

Cabe advertir que la acusación omitió indicar el supuesto fáctico que permitiría tener por cumplido ese elemento típico en la conducta de GREIS KATERIN GUTIÉRREZ SOLANO, ni siquiera afirmó la inexistencia de esa facultad en el ámbito laboral. En últimas, entonces, habría imputado una conducta relativamente atípica comprometiendo así, desde ese momento inicial del juzgamiento, cualquier posibilidad de éxito de la pretensión punitiva. Al efecto, se llama la atención de la Fiscalía General de la Nación, como en otras oportunidades, para que cumpla con el deber de formular una relación clara y suficiente de los hechos jurídicamente relevantes.

Por su parte, la sentencia -condenatoria- de segunda instancia, sin preocuparse por la eventual adición a la imputación fáctica, consideró que la procesada no contaba con autorización que le permitiera borrar archivos de la oficina de recursos humanos solo porque estos resultaban importantes para el funcionamiento de la empresa.

Es decir, estimó que el ingrediente típico estaba satisfecho, primero, sin indicar las pruebas que acreditaron la carencia de facultades de la acusada, en el ámbito de sus funciones, para alterar o mover los archivos digitales de la oficina que regentaba y, segundo, infiriéndola del contenido de estos documentos, cuando la cuestión no dependía de ello sino de establecer si la relación laboral le confería o no una prerrogativa de tal naturaleza.

Al margen del problema de adecuada imputación, el asunto merecía especial mayor atención porque el testigo Jorge Alberto Calderón Rey -jefe de sistemas- manifestó que GREIS KATERIN GUTIÉRREZ SOLANO, Jhessica Paola García Pulido y Charys Viviana Bernal Medina manejaban computadores que contaban con **permisos** para borrar los archivos del equipo servidor, situación que imponía esclarecer el alcance de esas autorizaciones porque de esta cuestión dependía la ilicitud o no de la acción atribuida a la acusada.

En efecto, durante el contrainterrogatorio, uno de los defensores preguntó: «*al momento de borrar un archivo ¿dice usted que se puede borrar desde cualquiera de los equipos de los que están ahí?*»[30], a lo que el testigo respondió «*depende del tipo de permisos que tuvieran,* ***ellas tenían todos los permisos****, pues porque eran las de recursos humanos, de*

[30] Minuto 1:29:03 (audio 2), sesión de juicio oral del 31.10.2018.

pronto la niña del Sena o ese equipo era el que tenía acceso de solo lectura»[31].

Entonces, ni la acusación imputó correctamente la carencia de facultades para manipular los archivos de la oficina de recursos humanos ni la sentencia de segunda instancia reparó en las consecuencias de esa omisión y, por el contrario, la tuvo por demostrada sin fundamentos probatorios razonables. No obstante, aun cuando en gracia de discusión tal falencia pudiera tenerse por subsanada; de todas maneras, la conducta de trasladar los archivos desde una carpeta compartida hasta la «papelera de reciclaje», en el mismo disco duro, sigue siendo atípica de borrar datos informáticos.

37. Por si fuera poco todo lo anterior, existen razones que permiten dudar sobre una actuación dolosa por parte de GREIS KATERIN GUTIÉRREZ SOLANO, específicamente sobre si tuvo el propósito de borrar datos informáticos:

37.1 Ella manipuló el equipo servidor para realizar la acción por la que resultó enjuiciada, en presencia no solo de sus compañeras Jhessica Paola García Pulido y Charys Viviana Bernal Medina, sino también de Diana Marcela Blanco Correa, quien había sido designada por el consejo de administración para reemplazarla y por ello se presentó en la

[31] Minuto 1:29:08, ibidem.

oficina, la tarde del 27 de enero de 2015, a recibir el puesto de trabajo[32].

Y, además, el comportamiento de la procesada se desarrolló en un lugar monitoreado permanentemente por 2 cámaras de vigilancia, al punto de quedar grabado en su integridad y este registro constituyó evidencia del juicio -introducida con el investigador Fabio Augusto Piñerez Cruz[33]-.

Tales circunstancias debían ser conocidas por la acusada, aun la existencia de los dispositivos de monitoreo, porque llevaba más de 2 años laborando en la empresa. Por tanto, es poco probable que tuviera la intención de cometer una conducta delictiva contra su empleador a sabiendas de que dejaba un gran número de evidencias que la incriminarían; por el contrario, en ese contexto es más factible que ningún propósito ilícito guiara su conducta.

37.2 En cumplimiento de sus tareas como jefa de recursos humanos hacía más de 4 meses (1 de agosto de 2014), y quizás desde 2 años antes que había ingresado a la Cooperativa (10 de septiembre de 2012)[34], operaba sistemas de cómputo, como lo dejaron ver las imágenes de videos de las cámaras de seguridad y los testimonios de Diana Marcela Blanco Correa y Jorge Alberto Rey Calderón.

---

[32] Minutos 52:08 – 52:14, sesión de juicio oral del 20.02.2019.
[33] A partir del minuto 5:55, sesión de juicio oral del 31.10.2018.
[34] El contrato de trabajo a término indefinido de GREIS KATERIN GUTIÉRREZ SOLANO fue introducido como prueba documental No 4.

Ese hecho permite inferir que GREIS KATERIN GUTIÉRREZ SOLANO contaba con habilidades informáticas, por lo menos con las más básicas; no obstante, limitó su conducta, por su propia voluntad, a enviar archivos a la «papelera de reciclaje».

37.3 Ese mismo factor temporal, es decir, los casi 3 años que tenía de ser empleada de COVOLCO, indica que es muy probable que supiera de la existencia de copias de respaldo de los archivos de la empresa (back up) realizadas hasta diciembre de 2014, como lo afirmó el jefe de sistemas Jorge Alberto Calderón Rey[35].

Si tenía ese conocimiento, o cuando menos existiría duda sobre ello, la acusada pudo estar convencida de que su acción con los datos informáticos sería aún más inocua y ello desdice algún propósito malicioso.

37.4 La conducta que suscitó el juicio fue realizada entre las 5:16 y las 5:26 p.m., es decir, cuando faltaban más de 30 minutos para la finalización de la jornada laboral que, según el director administrativo de COVOLCO Wolfang Eugenio Peña Díaz, era a las 6:00 p.m.[36].

De otra parte, no se probó en el juicio la concurrencia de alguna circunstancia externa que impidiera a la procesada adelantar actos posteriores que le tomarían solo unos

[35] A partir del minuto 1:19:25 (audio 2), sesión de juicio oral del 31.10.2018.
[36] A partir del minuto 50:48, sesión de juicio oral del 15.02.2019.

segundos o minutos adicionales, por ejemplo: vaciar la «papelera de reciclaje», si es que su cometido era el borrado de los archivos.

En otras palabras, ella realizó toda la conducta que se propuso, la que **no consistió** en el inicio de ejecución, a través de actos idóneos e inequívocos, de borrar datos informáticos. Por tanto, tampoco habría lugar a predicar una eventual tentativa conforme a los presupuestos establecidos en el artículo 27 del C.P.

38. En conclusión, se absolverá a GREIS KATERIN GUTIÉRREZ SOLANO por el delito de *daño informático*, por atipicidad de su conducta debido, principalmente, a que no borró datos informáticos, sin olvidar que no le fue imputada la carencia de facultades para desarrollar una acción de tal naturaleza y que existen dudas sobre el dolo.

39. Como consecuencia de la decisión absolutoria, se ordenará al juez de primera instancia que proceda a (i) cancelar las medidas cautelares que se hayan impuesto a la acusada y cualquier requerimiento derivado de la presente actuación; y, (ii) oficiar a las entidades que corresponda para que actualicen sus bases de datos manuales o electrónicas.

En mérito de lo expuesto, **la Corte Suprema de Justicia, Sala de Casación Penal**, administrando justicia en nombre de la República y por autoridad de ley,

RESUELVE

Primero: **Revocar** la sentencia condenatoria impugnada y, en su lugar, **absolver** a GREIS KATERIN GUTIÉRREZ SOLANO por el delito de *daño informático*.

Segundo: **Ordenar** al juez de primera instancia que cancele las medidas cautelares impuestas a la acusada y cualquier requerimiento derivado de la presente actuación; y que oficie a las entidades que corresponda para que actualicen sus bases de datos manuales o electrónicas.

Contra esta decisión no proceden recursos.

Notifíquese, cúmplase y devuélvase.

FABIO OSPITIA GARZÓN
Presidente

JOSÉ FRANCISCO ACUÑA VIZCAYA

MYRIAM ÁVILA ROLDÁN

FERNANDO LEÓN BOLAÑOS PALACIOS

GERSON CHAVERRA CASTRO

DIEGO EUGENIO CORREDOR BELTRÁN

LUIS ANTONIO HERNÁNDEZ BARBOSA

HUGO QUINTERO BERNATE

NUBIA YOLANDA NOVA GARCÍA

SECRETARIA