CADENA DE CUSTODIA.

DELITOS INFORMÁTICOS. EVIDENCIA DIGITAL. COACCIÓN ANÓNIMA. ATAQUE INFORMÁTICO A UN MEDIO DE PRENSA. VALORACIÓN DE LA PRUEBA

El incumplimiento de los protocolos para la recolección de evidencia digital no implica necesariamente la nulidad del procedimiento. La parte que alega la violación de la cadena de custodia debe probar un perjuicio y debe valorarse el contexto en que se registró la prueba, como también la participación y los testimonios de personal calificado en materia informática. La publicación de un mensaje intimidatorio en la página web de un diario mediante la intrusión en el sistema informático constituye los delitos de coacción, acceso no autorizado a un sistema informático e impedimento de la libre circulación de un medio de prensa.

Antecedentes: El diario “El Litoral” sufrió un ataque informático en su servidor por parte de un usuario identificado como Libero. La intromisión interrumpió la difusión de la versión digital del periódico y durante el hackeo se publicaron en dicha página de internet mensajes intimidatorios hacia una fiscal provincial y los empleados del diario.

Asimismo, durante el ataque se produjo la redirección de la página web del diario hacia otra de contenidos pornográficos. Frente a esa situación, dos fiscales, acompañados por expertos informáticos se constituyeron en la sede de “El Litoral” con la finalidad de recolectar la prueba digital. El Tribunal Oral Federal de Santa Fe condenó por estos hechos a EVC como autor de los delitos de coacciones agravadas por ser cometidas de forma anónima, impedimento de la libre circulación de un medio de prensa y acceso sin autorización a un sistema informático, en concurso ideal y le impuso la pena de tres años y dos meses de prisión.

La defensa de EVC impugnó la condena y planteó la nulidad de la recolección de la prueba informática, como también la arbitrariedad de la sentencia.

Sentencia: El incumplimiento de los protocolos para la recolección de evidencia digital no implica necesariamente la nulidad del procedimiento. La parte que alega la violación de la cadena de custodia debe probar un perjuicio y debe valorarse el contexto en que se registró la prueba, como también la participación y los testimonios de personal calificado en materia informática.

La publicación de un mensaje intimidatorio en la página web de un diario mediante la intrusión en el sistema informático constituye los delitos de coacción, acceso no autorizado a un sistema informático e impedimento de la libre circulación de un medio de prensa. La Sala I CFCP rechazó el recurso de casación.

Extractos del voto del juez Diego G. Barroetaveña: Planteos de nulidad de la recolección de prueba digital "…el agravio traído a estudio por la defensa por vía del cual plantea la nulidad del procedimiento de recolección de la evidencia digital, constituye una reedición de los […] cuestionamientos ya planteados […], a los cuales el juez a quo dio […] respuesta…" "…el operativo de recolección de prueba digital llevado a cabo por personal profesional que fue controvertido por la defensa no se encuentra viciado de nulidad. Ello es así, toda vez que […], los especialistas informáticos actuaron en concordancia con los protocolos de actuación en casos análogos y siguieron los procedimientos necesarios para asegurar la fidelidad de las pruebas y constancias digitales que se recolectaron durante el ciberataque al diario…".

"…el […] actuar de la prevención resultó avalado por el representante del ministerio público fiscal quien instruyó la investigación preliminar en este caso. De hecho, fueron dos los representantes del Ministerio Público Fiscal […] que […] se presentaron en la editorial del diario, en virtud de haber tomado conocimiento sobre un presunto hackeo a la plataforma digital del referido diario".

"…la evidencia recolectada fue debidamente asegurada y constatada a través de impresiones digitales de capturas de pantallas y back up en pen drive y CD". "Ello resultó corroborado […] con las declaraciones de los oficiales [Q y Z] quienes reprodujeron de modo lineal lo actuado por escrito, resultando suficiente para reconstruir las circunstancias de modo, tiempo y lugar en que se produjo la recolección y copia forense de la evidencia digital recabada en este proceso…".

Planteos relativos a la arbitrariedad de la sentencia "…el Tribunal Oral […] tuvo por probado que […], un operador del ciberespacio denominado ´Libero´ se infiltró en forma virtual y sin autorización en el sistema privado del diario ´El Litoral´ y publicó en sus páginas web […] un mensaje intimidante dirigido al personal de la empresa, amenazó a la fiscal adjunta del Ministerio Público de la Acusación de Santa Fe, Dra. [MLN], e impidió con su acceso el correcto y libre funcionamiento de la versión digital del periódico, paralizándolo por más de cinco (5) horas, redireccionando luego las visitas a una página de pornografía llamada ´xvideos.com´".

"…lo cuestionado por la defensa no fue la comprobación del hecho, sino la autoría y responsabilidad penal de [EVC] en los hechos tenidos por acreditados". "…el juez […] memoró el relato de [JFQ] (técnico universitario en informática de gestión y diplomado en peritajes judiciales), de [DAO] (ingeniero en sistemas y encargado del desarrollo web de la plataforma virtual) y de [MAM](gerente de Linux) quienes fueron contestes en detallar el procedimiento llevado a cabo…".

"…sopesó la declaración de [JS], periodista del diario El Litoral quien hizo referencia a una serie de publicaciones de notas periodísticas de su autoría referidas a una investigación que estaba en cabeza de la fiscal [MLN] en la cual se investigaba la posibilidad de la existencia de una asociación ilícita y estafa".

"…se expusieron datos que aún no eran de público conocimiento y se hizo referencia a la búsqueda de un hacker que se hacía llamar ´Líbero´". "…tomó en consideración el testimonio de la fiscal [MLN] quien relató ´[…]los avances obtenidos en el marco del legajo [a su cargo], haciendo énfasis en el escrito acompañado por [LE], a la postre condenado como jefe de la asociación ilícita allí investigada, que al encontrarse detenido

ofreció su colaboración para el esclarecimiento de los hechos. En su descargo [LE] precisó que para consumar los delitos realizados por la banda que lideraba se valió del hacker llamado 'Líbero', el cual se trataba de [EVC], aportando datos precisos sobre su identidad e informando que el nombrado le había confesado su participación en la intervención de los correos oficiales del Ministerio de Seguridad de la Nación meses antes de este suceso´". "…el juez […] mencionó otra causa judicial seguida contra el aquí condenado en la cual se investigaba el jaqueo a los correos oficiales del Ministerio de Seguridad de la Nación y de la cuenta de ´Twitter´ de la entonces Ministra de Seguridad […]. En ese marco, destacó que la metodología utilizada en ese hecho que se investigaba era una reiteración del modus operandi de aquel otro proceso en el cual se encontraba imputado [EVC]…".

"…del mencionado proceso surge que ´(l)os ataques informáticos provenían de diferentes direcciones IP, siendo algunas de ellas las número 23.235.227.100 administrada por la firma ´Secured Servers LLC´ con servidor en Arizona, Estados Unidos y la 190.180.41.2 radicada en La Paz, Bolivia; conexiones de red que [JFQ] identificó como empleadas los días previos y durante el acceso ilegítimo al servidor del diario, siendo determinante al explicar que este tipo de conexiones son utilizadas como dispositivos para compartir red, lo que posibilita a los usuarios acceder al servidor y reemplazar el IP original por el que otorga aquel, y así poder navegar en internet en forma anónima y oculta´".

"…el juez puso de manifiesto que este testimonio ´analizado en contexto y sumado a la similitud entre las firmas utilizadas en los accesos ilegales registrados desde enero a marzo del 2017, no hace más que confirmar que estamos ante la misma matriz delictiva, cuyo hacedor en este caso, procuraba amedrentar a los editores de un medio de comunicación e intimidar a la fiscal que seguía sus pasos; excluyendo con ello cualquier duda respecto a la intervención del encausado, quien tuvo durante más de cinco horas el pleno dominio funcional de la situación´".

"se concluyó que ´[…] la intromisión maliciosa […] que generó la caída del servidor web del diario ''El Litoral'' se encontraba relacionada pura y exclusivamente a los hechos

acontecidos […] en la esfera judicial y replicados periodísticamente. Se puede afirmar sin hesitación, que [EVC] al verse acorralado y expuesto, insertó en la portada digital una placa que permaneció estática durante varias horas cuyo contenido rezaba: ´'Diario el Litoral. En estos últimos 2 meses han estado publicando noticias que me molestan bastante. Se metieron con asuntos en los que no tenían que meterse por lo tanto a partir de hoy este diario va a publicar noticias que no involucren a personas que me importan. Sus servidores fueron hackeados y varias computadoras de sus redactores satisfactoriamente han sido infectadas. Mi objetivo es observar que hagan las cosas por el camino correcto, o sea, no publicar cualquier estupide[z]. y difamar a una persona sin medir las consecuencias. Y la fiscal [MLN] deberá pensar dos veces las pelotudeces que dice´'".

"…el judicante valoró las declaraciones testificales del personal calificado que intervino en el momento de la recolección de evidencia e intentos de cesar la amenaza, la declaración de [LE] quien identificó a [EVC] como el hacker que se hacía llamar Líbero, también comparó el modus operandi de esta causa con otra en la cual se imputó al aquí condenado por la intromisión a los correos oficiales del Ministerio de Seguridad de la Nación y la cuenta de Twitter de la entonces Ministra de Seguridad…".

"Paralelamente, de modo genérico y como un punto más a tomar en consideración, el juez a quo hizo mención a que el aquí condenado se encontraba altamente cualificado para desarrollar, sin dificultad alguna, los hechos investigados en el presente proceso". Planteos relativos a la calificación jurídica "…la defensa cuestionó la calificación jurídica otorgada y entendió que no se encontraba configurado el delito de amenazas coactivas agravadas". "…el juez del tribunal entendió que ´[EVC] al insertar los mensajes en la página web de 'El Litoral', coaccionó expresamente tanto al medio de comunicación como a la fiscal [MLN]; así surge literalmente de las palabras y conceptos volcados en el mismo´".

"Asimismo, adicionó que ´La acción típica del delito atribuido consiste en hacer uso de dicha amenaza para obligar a otro a hacer, no hacer o tolerar algo. Para lograr el objetivo pretendido y consumar el delito se debe utilizar un medio idóneo para alarmar y

amedrentar, cuestión harto probada tanto en la faz objetiva como subjetiva. En efecto, los dichos volcados provienen de una persona evidentemente capacitada para producir daño o gravamen irreparable en el destinatario; así lo demostró y lo estaba haciendo en la página web del periódico y, con el antecedente de [EVC] como integrante de una asociación ilícita que fuera investigada por la fiscal [MLN] se demuestra también, potencialmente, las consecuencias que podrían suceder a la persona…´".

"…a partir de una sensata valoración de las probanzas precedentemente analizadas el juez a quo consideró debidamente probado que el propósito que [EVC] tuvo con sus amenazas ´fue obligar a no hacer –a no publicar en el caso del medio de información y a callarse y no actuar en el caso de la fiscal-, constituyendo tal característica la situación típica de la coacción´".

"A su vez, hizo hincapié en que ´el propio artículo 149 ter del Código Penal, en su inciso primero, agrava el monto de la pena 'si las amenazas fueren anónimas'. En lo que hace al bien jurídico protegido, tanto en aquella figura basal como en esta, resulta ser la libertad individual de la persona, menoscabando las posibilidades de ejecución de acciones futuras por parte de la víctima y, en el caso concreto, la libertad psíquica que encuentra su expresión en la intangibilidad de las determinaciones´".

"…los agravios […] sobre la calificación jurídica […] se tratan de una mera reedición de aquellos que fueron debidamente abordados en el fallo condenatorio". Determinación de la pena "…las expresiones utilizadas por el juez de mérito para sustentar la cuantificación de la condena impuesta […] satisfacen el requisito de motivación que exige la decisión atacada…".

"…al momento de fijar la sanción, el juez de juicio consideró como circunstancias agravantes que ´la peligrosidad de [EVC], no se revela quizás a través de los cánones ortodoxos propios de los delitos que exigen violencia sino por el contrario, advierto que el diversificado despliegue que hizo para ocultar sus rastros consiste en una acción fría que proviene de su mente calculadora, premeditada e insensible, revelando así su alto grado de desprecio por las normas y pautas de convivencia social. La extensión del daño ha sido sin dudas de enorme proyección, logrando con sus acciones causar el efecto

deseado en los destinatarios. Las consecuencias de su conducta no solo fueron en desmedro de una empresa privada, de la libertad de prensa o de una funcionaria pública, sino también en perjuicio de la sociedad en su conjunto y consecuentemente el reproche debe ser mayor´".

"En función de la ponderación efectuada, el tribunal de juicio estimó acertado alejarse dos meses del mínimo legal previsto para los delitos atribuidos e imponerle a [EVC] la pena de tres años y dos meses de prisión…".

Extractos del voto del juez Carlos A. Mahiques "…La resolución impugnada se encuentra suficientemente fundada en las pruebas reunidas en las actuaciones, sin que se adviertan fisuras lógicas en el razonamiento en punto al grado de participación del nombrado en el hecho aquí juzgado…".

"…el unívoco plexo probatorio reunido en autos fue rigurosamente analizado por el tribunal de origen, y los agravios planteados sólo evidencian una opinión diversa sobre la cuestión debatida y resuelta…". "…En cuanto a la individualización de la pena, […] la respuesta punitiva dada por el tribunal resulta proporcional a la intensidad antijurídica del hecho y, por ende, a la responsabilidad del autor (CSJN, Fallos 314:441 y 318:207) y resulta acorde con la pena requerida por el Fiscal de Juicio a la hora de efectuar la acusación".

Extractos del voto del juez Daniel Antonio Petrone "…la evidencia digital es toda información guardada o transmitida en formato binario que sea introducida en un proceso con fines probatorios […]. Una de sus características principales es la volatilidad, lo cual conlleva que sea frágil y fácil de alterar, dañar o destruir".

"…las tareas de identificación, recolección, obtención y preservación de la evidencia digital de forma tal que pueda ser utilizada en el marco de un proceso se han tornado fundamentales y, en ese marco, el mantenimiento de la cadena de custodia de esa

evidencia es ineludible a los efectos de garantizar su credibilidad, legitimidad, identidad, integridad y pureza; en definitiva, su validez probatoria".

"el ´Protocolo General de Actuación Para Las Fuerzas Policiales y De Seguridad en la Investigación u Proceso de Recolección de Pruebas en Ciberdelitos´, aprobado por Resolución 234/2016 del Ministerio de Seguridad (B.O. 07/06/2016) –citado por la defensa-, ha sido diseñado para regular la actuación de las fuerzas de seguridad en la investigación y recolección de pruebas en el marco de los ciberdelitos…".

"…mediante Resolución nº 76/16 del 31 de marzo de 2016, la Procuración General de la Nación había aprobado la ´Guía para la obtención, preservación y tratamiento de evidencia digital´, recomendando a todos los integrantes del Ministerio Público Fiscal que ajusten su proceder a los lineamientos de ese documento…".

"…surge la importancia de implementar los mecanismos de preservación de los datos e información capturada que hasta aquí se reseñaron al momento de recolectar la denominada evidencia digital o electrónica en el marco de un proceso determinado. Particularmente, el cálculo del valor hash se presenta como uno de los métodos actualmente al alcance y que resulta apto para preservar la integridad y la cadena de custodia en aquellos casos en los que las pruebas no son tangibles, a diferencia de lo que ocurre con el secuestro de evidencia física como serían armas, estupefacientes, y demás rastros y objetos en el marco de una investigación".

"…si bien los protocolos dictados sobre la materia contienen recomendaciones para un correcto obrar de las fuerzas de prevención al momento de recolectar evidencia digital, no contemplan específicamente el modo adecuado de colectarla mientras se está intentando contener un ataque informático". "…si bien es deseable lograr una metodología de intervención adecuada y uniforme para una efectiva obtención y preservación de la evidencia digital para que, llegado el caso, pueda ser aceptada legalmente en un proceso judicial, no puede dejar de admitirse un margen razonable de actuación por fuera de los protocolos establecidos, no solo porque existen incontables fuentes potenciales de evidencia digital […] que pueden encontrarse almacenadas en diversos tipos de dispositivos informáticos -cada uno en condiciones particulares-, sino

también por el contexto en el que pueda tornarse necesaria esa obtención y por los recursos técnicos con los que se cuente en ese momento, todo lo cual condiciona la identificación, recolección y preservación de la evidencia".

"…el modo adecuado de proceder dependerá de cada situación particular, debiendo examinarse si en determinadas circunstancias los mecanismos utilizados resultaron idóneos para asegurar la integridad de los datos e información obtenida". "…la conclusión a la que arriba el a quo con relación a la nulidad planteada resulta una derivación razonada de las circunstancias comprobadas del caso y del derecho aplicable, ante la cual la mera afirmación de que la cadena de custodia no fue preservada ante la falta de asignación de un hash o utilización de un bloqueador de escritura no alcanza para acreditar la invalidez pretendida".

"…si bien como se dijo los protocolos y guía mencionados los establecen como prácticas deseables, atendiendo a la premura en la que el personal interviniente se encontraba inmerso a los fines de hacer cesar el ataque y tomando en consideración los restantes recaudos adoptados, su omisión en este caso no conlleva a la nulidad del acto".

"…resulta dirimente el respaldo que la evidencia digital inicialmente obtenida encuentra en las declaraciones de los testigos que intervinieron en el procedimiento original como así también en el resultado de las diligencias llevadas a cabo con posterioridad, evidencia que fue hasheada y que corrobora los datos oportunamente extraídos". "…las alegaciones de la parte en torno a que, frente a las omisiones advertidas, ´[…] alguien podría haber estado modificando todos los datos que ellos estaban visualizando, copiando, imprimiendo, pasando de un dispositivo a otro, pudiéndose alterar inclusive de forma maliciosa la IP una vez que se activaron los registros [… y que] no podemos saber si esa evidencia que se extrajo, es exactamente la misma que la que se encontraba en los dispositivos, o sufrió algún tipo de modificación entre tanta manipulación de los archivos´ no alcanzan para acreditar la violación a la cadena de custodia que sostiene y a declarar la invalidez pretendida, reduciéndose su argumentación a una construcción hipotética".

"…la premisa sostenida por la defensa se sustenta en una mera formalidad y no se verifica, más allá de las alegaciones que en abstracto se realizan, un perjuicio concreto para el imputado, teniendo en cuenta el criterio restrictivo que rige en materia de nulidades, el agravio sostenido debe ser rechazado…".

Votos Diego G. BARROETAVEÑA, Carlos A. MAHIQUES, Daniel Antonio PETRONE

Descarga: **https://old.pjn.gov.ar/02_Central/ViewDoc.Asp?Doc=174747&CI=INDEX100**