



Poder Judicial de la Ciudad de Buenos Aires
Fuero Penal Contravencional y de Faltas

2021 - Año del Bicentenario de la Universidad de Buenos Aires

CÁMARA DE APELACIONES EN LO PPJCyF - SALA III

INCIDENTE DE APELACION EN AUTOS "NN, NN SOBRE 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGIAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL"

Número: INC 41459/2019-3

CUIJ: INC J-01-00046145-4/2019-3

Actuación Nro: 2160870/2021

Causa n° 41459/2019-3 “NN, NN SOBRE 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGIAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL”

//la Ciudad Autónoma de Buenos Aires, se reúnen los miembros de la Sala III de la Cámara de Apelaciones en lo Penal, Penal Juvenil, Contravencional y de Faltas, integrada por los Dres. Sergio Delgado, Marcelo P. Vázquez y Elizabeth A. Marum, Secretaría única, a efectos de resolver en la presente causa.

VISTOS:

I. Motiva la intervención de este tribunal el recurso de apelación presentado por la defensa técnica del Sr. C. B. contra la resolución que no hizo lugar a la nulidad planteada por dicha parte respecto del proceso y, en particular, de la cadena de custodia de la que sería la única evidencia aportada por la fiscalía, es decir, capturas de pantalla efectuadas sobre el teléfono móvil de la denunciante.

II. El 2 de junio de 2021, la jueza interinamente a cargo del Juzgado en lo Penal, Contravencional y de Faltas N° 26 resolvió rechazar el planteo de nulidad realizado por la defensa, ello con el argumento de que el cambio en el número de *hash* de la evidencia colectada se debió a un error involuntario por parte del personal del Ministerio Público Fiscal, quien dio cuenta del mismo y dejó constancia de tal situación. Asimismo, destacó que no se advierte alteración alguna en la cadena de custodia de la prueba recabada.

III. La defensa técnica impugnó esta decisión, poniendo de relieve que el procedimiento aquí llevado a cabo se encuentra viciado desde sus inicios en virtud de las discrepancias con el número de *hash*, y que por lo tanto las decisiones que fueron adoptadas como consecuencia de ello devienen arbitrarias y son, por lo tanto, inválidas en virtud de la doctrina del fruto del árbol envenenado. En este marco, consideró que todo lo actuado implica una vulneración al derecho de defensa, principio de inocencia e *in dubio pro reo* del imputado.

IV. El Fiscal de Cámara, Dr. Eduardo J. Riggi, postuló la inadmisibilidad del remedio procesal intentado o, en su defecto, su rechazo. Consideró que el auto atacado resulta irrecurrible, ya que "...a) la decisión cuestionada no está declarada expresamente apelable; y b) tampoco logró demostrar el gravamen irreparable que, en el caso concreto, tornaría viable el recurso intentado (art. 291 CPPCABA)...", y que la Fiscal de instancia fue clara en remarcar que el cambio del número de hash se debió a un error involuntario del personal del MPF, el cual asignó un número de hash en el acta de resguardo correspondiente a un modelo de acta anterior, y que cuando advirtió dicho defecto, lo corrigió colocándole el número correcto, circunstancia que fuera debidamente descripta en el informe final del 05/09/2019.

V. La defensa particular no realizó agregado alguno a su presentación, encontrándose en condiciones, pasan las actuaciones a estudio del tribunal.

Y CONSIDERANDO:

El juez Sergio Delgado dijo:

1. Admisibilidad:

En lo atinente a la forma y plazo de su presentación, el recurso sortea las exigencias establecidas por el art. 292 del CPPCABA.

Si bien, en principio, la posibilidad de recurrir decisiones como la apelada, no se haya permitida expresamente por ley, en el caso de autos resulta menester analizar los agravios que invoca la defensa a los fines de establecer la existencia o ausencia del gravamen irreparable invocado, al estar éste previsto como requisito de procedencia de los recursos en general, conforme lo dispone el art. 291 del CPPCABA.



INCIDENTE DE APELACION EN AUTOS "NN, NN SOBRE 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGIAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL"

Número: INC 41459/2019-3

CUIJ: INC J-01-00046145-4/2019-3

Actuación Nro: 2160870/2021

En este sentido, al advertirse que existen discrepancias respecto del número de *hash* de la prueba colectada por el MPF, circunstancia que pone en duda el resguardo de la cadena de custodia, no puede más que concluirse que podrían estar siendo vulnerados derechos de raigambre constitucional del encausado como son la defensa en juicio, el debido proceso y el principio de inocencia, y que por lo tanto el gravamen que se le estaría irrogando sería de imposible reparación ulterior, dado que se cuestiona una decisión que admite someterlo a juicio en base a una prueba que, se alega, no ha sido preservada conforme a derecho. Este agravio (el ser sometido a un proceso en base a una prueba alterada) no podrá ser subsanado, incluso, por una sentencia definitiva absolutoria, que no habrá evitado el enjuiciamiento contrario a la ley.

Por ello el recurso debe ser admitido formalmente.

2. Procedencia:

El planteo expuesto por la defensa particular del imputado tiene por objeto cuestionar la práctica pericial efectuada sobre el teléfono móvil de la denunciante, ello en tanto la captura de pantalla del mismo, donde se visualizaría un intercambio de mensajes entre aquella y el Sr. C. B., se ha visto viciada por un cambio en el número de hash que la identificara, encontrándose de esa manera vulnerada la cadena de custodia de dicha prueba.

Asimismo, el recurrente expone que esa sería la única prueba con la que contaría el MPF, y que por lo tanto no existiría sustento probatorio para haber llegado a estas instancias en el proceso.

Ahora bien, entiendo importante realizar algunas consideraciones básicas sobre el carácter que la prueba o evidencia digital ostenta, máxime cuando nuestro

ordenamiento procesal no recepta suficientemente el modo en que dichos elementos deben ser obtenidos, procesados y resguardados, justamente por estar dotados de características especiales.

El Licenciado en Sistemas de la Universidad Tecnológica Nacional (UTN), Darío Piccirilli, docente, autor y perito especializado del Poder Judicial de la Nación por más de dos décadas, define a la informática (o computación) forense como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional¹. A través de esta disciplina se nos permitirá comenzar a laborar protocolos de actuación para preservar y resguardar esa evidencia, mediante una adecuada técnica de secuestro como así también, y principalmente, la construcción de una cadena de custodia que impide que esa evidencia sea adulterada.

Ello pues la evidencia digital, se caracteriza primordialmente por su volatilidad. Así, *“La volatilidad es una de las características más relevantes de la evidencia electrónica y debe interpretarse en términos de inestabilidad de la prueba. La evidencia digital tiene una capacidad amplia y fácil de transformarse y si no se toman los recaudos necesarios, puede eliminarse total e inmediatamente. La posibilidad de que eso suceda significarían que la prueba pierda valor probatorio o que desaparezca por complemento como evidencia de un hecho delictivo.”*².

Estas características hacen que la evidencia digital pueda ser fácilmente copiada o transformada. Esto es observado tanto como una ventaja, por lo fácil de su recolección y análisis simultáneo, como una desventaja, pues también puede poner en riesgo su autenticidad³.

Para garantizar la autenticidad de la evidencia, existen Códigos de Detección de Manipulaciones (MDC), Detección de Modificaciones, o Códigos de Integridad de Mensajes (MIC). Todos ellos son comúnmente llamados códigos *hash*⁴.

Este código *“...es la huella digital de la información electrónica que permite comprobar que no se alteró la prueba original y que, en consecuencia, asegura la*

1 PICCIRILLI DARIO A. “La Forensia como Herramienta en la Pericia Informática”, Revista Latinoamericana de Ingeniería de Software, Buenos Aires, 2013, 1(6): 237-240, ISSN 2314-2642; Pág 238.

2 Delle Donne, Carla P., *La extracción de prueba electrónica de teléfonos celulares y la garantía de defensa en juicio*, LA LEY 12/02/2020, p. 4. Sueiro, C. Christian; *La prueba digital en la criminalidad informática. A propósito del nuevo Código Procesal Penal*, en *El Debido Proceso Penal* N° 1, Ledesma / Lopardo, Ed. Hammurabi, Buenos Aires, 2015. P. 10.

3 *Ibidem*.

4 Sueiro, C. Christian; *La prueba digital en la criminalidad informática...* Ob. Cit. p. 16.



INCIDENTE DE APELACION EN AUTOS "NN, NN SOBRE 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGIAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL"

Número: INC 41459/2019-3

CUIJ: INC J-01-00046145-4/2019-3

Actuación Nro: 2160870/2021

autenticidad e integridad de la prueba digital. El hash constituye el rastro principal que identifica a la prueba y que posibilita verificar que esa evidencia contenida en el dispositivo secuestrado es la misma que se encontraba almacenada en el momento del secuestro y que es exactamente la misma que se extrajo y que, luego, se examinará.”⁵. Estos códigos difícilmente puedan ser alterados o modificados⁶.

A este respecto, y como bien lo trae a colación la jueza *a quo*, resulta relevante tener presente que la Guía de obtención, preservación y tratamiento de evidencia digital, presentada y aprobada en el marco de la XVII Reunión Especializada de Ministerios Públicos del Mercosur establece la necesidad de que las copias o imágenes forenses presenten un cálculo hash, ello atento a que por su volatilidad, la evidencia digital es “...frágil, fácil de alterar y dañar o directamente de destruir (...) Con esto nos estamos refiriendo a que dicha evidencia, en su estado natural, no nos deja entrever qué información es la que contiene en su interior, sino que resulta ineludible para ello, examinarla a través de instrumentos y procesos forenses específicos.”⁷, y que el cálculo del hash en la copia forense “...permitirá verificar si la misma fue alterada con posterioridad a su obtención. Si pasado un tiempo de realizada la misma alguien plantea que fue alterada, bastará calcular el hash para ver si es el contenido es el mismo del originalmente obtenido (en este caso, se demuestra que la copia no fue manipulada).”

⁵ Delle Donne, ob. cit.

⁶ Sueiro, ob. cit.

⁷ Disponible en <https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf>, página 9.

Se exige el cálculo del hash sobre cualquier copia forense para asegurar que ella no se vea alterada con posterioridad de su realización, circunstancia fundamental para garantizar la cadena de custodia de una prueba.

Teniendo en cuenta los parámetros delineados, debo destacar que se desprende de los actuados que la obtención y resguardo de la información colectada por el MPF mediante la captura de pantalla del teléfono móvil de la denunciante no se efectuó correctamente, ello en tanto el código *hash* que debería identificarla fue modificado en el transcurso del proceso, circunstancia que no permite garantizar su autenticidad. En efecto, no puede perderse de vista que: *“Para que la extracción de la prueba sea un acto procesal válido, debe registrarse el primer hash obtenido. La documentación del primer hash es un acto de gran trascendencia a los efectos de la identificación de la prueba, porque, si bien es cierto que la extracción de la prueba se puede repetir indefinidamente mediante la utilización de las herramientas forenses que impidan que se modifique la prueba, no menos cierto es que si las partes no fueron notificadas de la realización de ese acto nunca podrán controlar que el primer acceso al dispositivo secuestrado se efectuó siguiendo las buenas prácticas sobre extracción de la evidencia digital, no podrán corroborar que el hash obtenido corresponde al valor que tenía la prueba en el momento del secuestro, así como tampoco podrán verificar que la prueba no fue contaminada. Es decir, si las partes del proceso no fueron notificadas de la medida de extracción de información digital de un teléfono celular secuestrado podrían no solo cuestionar su valor probatorio, sino también plantear la nulidad del acto porque, aunque la extracción se repita, no tendrían forma de corroborar que el primer hash corresponde a una extracción no viciada. Solo podrían confirmar que el hash de una nueva y posterior extracción coincide con el primer hash, pero eso no asegura que ese primer hash sea el valor que arrojó la primera extracción. Lo expuesto anteriormente demuestra que la extracción de la información de todo dispositivo electrónico... es una medida única e irreproducible ...”*⁸.

El error involuntario presuntamente cometido por el personal del MPF no puede ser subsanado por el reemplazo del *hash*, ya que ello no permite asegurar que la prueba oportunamente colectada no hubiese sido adulterada con posterioridad.

⁸ Delle Donne, p. 5 (ob. cit.).



INCIDENTE DE APELACION EN AUTOS "NN, NN SOBRE 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGIAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL"

Número: INC 41459/2019-3

CUIJ: INC J-01-00046145-4/2019-3

Actuación Nro: 2160870/2021

Atento a lo dicho, la información obtenida no podrá ser –eventualmente- utilizada, al no poderse ya cotejar su fidelidad. Por ello concluyo que la diligencia practicada ha sido definitiva e irreproducible (art. 97 del CPPCABA).

Por todo lo expuesto, corresponde hacer lugar a la nulidad propuesta por la defensa particular del Sr. B., y declarar no admisible como prueba para el debate la captura de pantalla efectuada al teléfono móvil de la denunciante, ello atento a que su hash se vio alterado y que no fue preservada debidamente por quienes tenían la obligación de hacerlo.

En consecuencia, se propone al acuerdo: I) Hacer lugar a la nulidad postulada por la defensa; y II) Declarar inadmisibile para el debate la captura de pantalla del teléfono móvil de la denunciante.

Así voto.

Los Dres. Elizabeth A. Marum y Marcelo Pablo Vázquez dijeron:

Coincidimos con nuestro colega preopinante en lo atinente a la admisibilidad del recurso de apelación, pero diferimos en cuanto a la solución de fondo aplicable al caso, por los motivos que pasaremos a exponer.

En primer término, es necesario destacar que, en el caso, la defensa consideró que se había modificado el código “hash” con el que se había resguardado el material probatorio en el que la Fiscal de grado había basado la investigación –en particular, las capturas de pantalla de las que surgía la conversación que el imputado habría tenido con la damnificada a través de la red social Instagram–; que, por consiguiente, se había vio-

lado la cadena de custodia y que, en esa medida, correspondía declarar la nulidad de aquél resguardo, así como de todo lo actuado en su consecuencia.

La magistrada de grado, por su parte, precisó en primer lugar que el “*hash*” podía definirse como la conversión de determinados datos en un número de longitud fijo no reversible, que tiene por objeto corroborar la identidad de un archivo, así como preservar la integridad de los datos –esto es, asegurar que la información no haya sido alterada de ningún modo–.

Y, en esa línea, añadió que era necesario distinguir entre: no contar con un código de identificación y que, por error, el código original hubiera sido modificado por personal idóneo del Ministerio Público Fiscal. Siendo que aquellos habían dado cuenta de la circunstancia y solucionado el inconveniente, asignando el “*hash*” pertinente, y dejando constancia de ello en el mismo informe –lo que, en efecto, había sucedido en el caso–.

A mayor abundamiento, la *a quo* agregó que no se había tratado de un error de cálculo en el código “*hash*”, sino que, por el contrario, en el acta de resguardo correspondiente al caso se había dejado consignado el número de “*hash*” del modelo de acta que se había utilizado, y no se había modificado por el generado luego de realizar la descarga y el almacenamiento de las capturas de pantalla brindadas por la denunciante.

La defensa, por su parte, interpuso un recurso de apelación contra tal decisión, en el que consideró que el material probatorio electrónico en el que el Ministerio Público Fiscal había basado su acusación se encontraba viciado y debía ser declarado inválido, en razón de que la prueba había sido manipulada y, en esa medida, se había roto la cadena de custodia.

En esa lógica, añadió que el objetivo de la cadena de custodia era acreditar lo que llegaba a manos del juzgador, que debía ser exactamente lo mismo que lo que se había recolectado el día que se produjo la correspondiente extracción forense del dispositivo electrónico.

A la vez, la parte impugnante agregó que el valor entregado por una huella “*hash*” tiene la característica de ser único para un determinado conjunto de datos, y que cualquier cambio en esos datos –así sea en uno de sus caracteres– entrega un “*hash*” di-



INCIDENTE DE APELACION EN AUTOS "NN, NN SOBRE 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGIAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL"

Número: INC 41459/2019-3

CUIJ: INC J-01-00046145-4/2019-3

Actuación Nro: 2160870/2021

ferente. Y, en esa medida, concluyó que cualquier alteración de dicho código implicaba que la copia forense había sido manipulada.

En virtud de todo eso, solicitó la nulidad de aquella prueba, así como del procedimiento basado en ella.

Ahora bien, aclarado ello, corresponde establecer, en primer término, que, tal como hemos expresado en diversos precedentes de la Sala que originalmente integramos, la declaración de invalidez de un acto posee carácter excepcional, y que priman los principios de conservación y trascendencia de los actos procesales. En consecuencia, se debe afirmar que la nulidad sólo resultaría procedente de advertirse algún vicio sustancial o la afectación de garantías constitucionales.

En este sentido, hemos expresado en diversas oportunidades que para declarar la nulidad de un acto procesal es necesario cumplir con ciertos requisitos, entre ellos, la demostración (carga específica) por parte de quien la alega, del perjuicio concreto e irreparable que le ocasiona el acto, a su entender viciado y que no puede subsanarse sino con el acogimiento de la sanción y, por otro, del interés o provecho que le ocasionaría tal declaración –*“principio de trascendencia”*– (Causas N° 6690/2020-0-0 *“Incidente de apelación en autos F. B., E. s/art. 14 1er párrafo - Ley 23737”* rta. el 14/12/2020; N° 10184/2020-1 *“Incidente de apelación en autos ‘D., L. J. S/art. 71 BIS - difusión no autorizada de imágenes y grabaciones íntimas’”*, rta. el 17/05/21, entre muchas otras).

Por tanto, para que un acto sea alcanzado por la declaración de invalidez, debe haber conculcado algún derecho, causando un perjuicio efectivo. Pues las nulidades de

los actos procesales, además de constituir un remedio extremo, sólo proceden cuando de la violación de las formalidades que la ley establece derive un perjuicio real y concreto para la parte que lo invoca.

Sentado ello, corresponde hacer ciertas precisiones terminológicas respecto de los conceptos que aquí entran en juego.

En efecto, la defensa señaló como agravio que se había roto la cadena de custodia, entre los datos que contenían los elementos secuestrados y los que finalmente fueron corroborados en la pericia, en la medida en que se había modificado el código “hash” que había sido asignado a las capturas de pantalla extraídas del celular de la denunciante.

Ahora bien, ya hemos manifestado en un precedente de la Sala que originalmente integramos que, cuando hablamos de la **cadena de custodia**, corresponde precisar que es “...*el conjunto de procedimientos de seguridad destinados a garantizar que los elementos de prueba materiales que se incorporan y exhiben en el juicio oral guarden identidad física con el material que ha sido hallado, recolectado e incautado en el lugar donde se afirma que ocurrió el delito o hecho de relevancia penal, y que se encuentra en idénticas condiciones fenomenológicas a las que allí tenían, o sea: que no hayan sido alterados, contaminados, destruidos, dañados o sustituidos*” (Godino, Federico Lucio y Pérez Sasso, Christian Andrés; “*Cadena de Custodia: procedimientos para resguarda los elementos probatorios*”; pág. 17; Hammurabi; 1º Edición, 2020, citado en la Causa Nro. 47207/2019-1, “*Incidente de apelación en autos ‘NN s/ 128 I parr – delitos atinentes a la pornografía infantil’*”, rta. el 24/11/20).

A su vez, la cadena de custodia de la evidencia digital “[s]e inicia al momento de incorporación del elemento de prueba y debe registrar la información que permita comprender acabadamente cuál es el efecto, cuál es la evidencia, de qué forma fue recolectada y preservada” (Presman, Gustavo Daniel; en el libro *Cibercrimen II*; pág 311; Ed. BdeF; 2020).

En esa línea, y continuando con los casos de evidencia digital, se ha afirmado que resulta aconsejable “...*realizar una copia forense de los dispositivos de almacenamiento con anterioridad al resto de las pericias, a fin de poner a resguardo el dispositivo original y operar libremente dicha copia*” (Sain, Gustavo - Azzolin, Horacio; “*Del-*



INCIDENTE DE APELACION EN AUTOS "NN, NN SOBRE 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGIAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL"

Número: INC 41459/2019-3

CUIJ: INC J-01-00046145-4/2019-3

Actuación Nro: 2160870/2021

tos Informáticos. Investigación Criminal, marco legal y peritaje"; pág 34; Reimpresión; Ed. BdeF; 2020, citado en la Causa Nro. 47207/2019-1, "*Incidente de apelación en autos 'NN s/ 128 1 parr – delitos atinentes a la pornografía infantil'*", rta. el 24/11/20).

Asimismo, la certificación "*hash*" –utilizada en el caso– constituye uno de los modos más utilizados en la actualidad para dotar a la evidencia digital de credibilidad y verificabilidad, en la medida en que aquella tiene la función de corroborar la identidad del archivo y asegurar que la información no fue alterada por personas no autorizadas u otros medios desconocidos (*ibidem*, págs. 36-37).

En la misma línea, asiste razón a la magistrada de grado, en cuanto afirma que el "*hash*" se define como la conversión de determinados datos en un número de longitud fija no reversible, que tiene como funciones primordiales la autenticación –en tanto permite corroborar la identidad de un archivo– y la preservación de la integridad de los datos –toda vez que asegura que la información no haya sido alterada por personas no autorizadas u otro medio desconocido–.

Ahora bien, reseñado ello, cabe adelantar que también coincidimos con la *a quo*, en cuanto a que la nulidad planteada no puede prosperar.

Ello, en la medida en que, si bien asiste razón a la defensa, en cuanto a que el valor entregado por una huella "*hash*" tiene la característica de ser único para un determinado conjunto de datos, y a que cualquier cambio en esos datos entrega un código diferente, lo cierto es que, en el caso, la Fiscal de grado ha sido clara en cuanto a que no ha habido una modificación en dicho código, sino que, antes bien, se ha producido un

error material en el acta en la que se plasmó la actividad llevada a cabo por el Centro de Investigaciones Judiciales.

Así, en el marco de la audiencia en la que la jueza de grado decidió no hacer lugar al planteo incoado por los defensores particulares del Sr. B., la Dra. Dupuy explicó que, cuando recién se había realizado la denuncia, se le solicitó a la Sra. L. A. R., madre de la damnificada, que concurriera a la sede del Cuerpo de Investigaciones Judiciales para efectuar la preservación de la conversación que la joven habría tenido con el imputado, a través de la red social Instagram.

A la vez, la Fiscal explicó que, en esa oportunidad, el personal del CIJ había realizado una videograbación de la pantalla del celular aportado por R., donde constaba la conversación en cuestión, y que, después, ese archivo fue “*hasheado*”.

Y añadió que, luego de que ese archivo fuera “*hasheado*”, se había llevado a cabo el acta de resguardo de la prueba, y que, en ella, se había dejado el número de “hash” correspondiente al archivo anterior, en virtud de un error involuntario, y no porque la prueba en cuestión hubiera sido modificada o manipulada.

A mayor abundamiento, la titular de la acción explicó que, simplemente, en virtud de un error humano, se había dejado allí un número de “*hash*” anterior, y que, por lo demás, ello había sido inmediatamente subsanado, en el informe del que la defensa pretendió extraer la nulidad en cuestión.

En efecto, del relato brindado por la Dra. Dupuy –sobre quien pesa el deber de objetividad contemplado por el artículo 6 del CPPCABA– surge que lo que ocurrió fue que se dejó asentado, en el acta de resguardo, un código que pertenecía a otra investigación, y que estaba consignado en el acta que se había utilizado de modelo, así como que ello fue inmediatamente advertido, y subsanado por el personal del CIJ, a través de la modificación del acta, y de la incorporación del código “*hash*” correcto.

Y, en esa medida, no queda más que afirmar que no ha habido una modificación del código de “*hash*” que se le asignó a los archivos resguardados ni, por consiguiente, una violación de la cadena de custodia –lo que, por lo demás, puede verificarse con la filmación realizada por el personal del CIJ al llevar a cabo la descarga y el resguardo del material digital–. Ello así, toda vez que, según surge de las constancias de la presente, aquél código permaneció inalterado, y la modificación se presentó únicamente



INCIDENTE DE APELACION EN AUTOS "NN, NN SOBRE 131 - CONTACTAR MENOR DE EDAD POR INTERMEDIO DE TECNOLOGIAS PARA COMETER DELITOS DE INTEGRIDAD SEXUAL"

Número: INC 41459/2019-3

CUIJ: INC J-01-00046145-4/2019-3

Actuación Nro: 2160870/2021

en el acta de resguardo. Lo que se traduce en un error de tipeo involuntario sobre el acta del cual no puede derivarse más que su corrección al advertirlo, como lo hace cualquier operador judicial con un yerro material, que nada tiene que ver con el proceso penal, y como, en efecto, lo hizo el CIJ.

En este sentido, también es necesario poner de manifiesto otras dos circunstancias que contribuyen al hecho de que la nulidad planteada por la defensa no pueda prosperar. La primera de ellas, relativa a que el resguardo de la conversación entre la damnificada y el imputado constituye un acto reproducible, que podría ser llevado a cabo nuevamente de resultar necesario, y la segunda, atinente a que el alegado vicio en el resguardo de la evidencia –y, por consiguiente, en la cadena de custodia– fue advertido e inmediatamente subsanado por quienes habían llevado a cabo el resguardo al momento de presentar el correspondiente informe,, ya en el año 2019.

Por lo demás, de la lectura del recurso intentado se advierte que, sin perjuicio de que la defensa del Sr. B. ha alegado la violación de la cadena de custodia, así como la modificación del código “hash”, y la manipulación de los datos que aquél pretendía preservar, no ha explicado de qué manera se habría producido tal violación, o bien, de qué modo aquella información se ha visto manipulada, ni ha contrarrestado de ningún modo la explicación brindada por la Fiscal de grado en el marco de la audiencia en la que se trató el planteo, y, en la misma línea, tampoco ha especificado de qué forma lo ocurrido le generaría la conculcación de algún derecho.

En ese sentido, hemos manifestado en numerosos precedentes que la garantía de defensa tiene carácter sustancial, y no meramente formal, y que, en virtud de ello, es

necesario que quien alegue su conculcación demuestre cuáles han sido los perjuicios concretos padecidos (Causa Nro. 46231-00-CC/11 “*Perrone, Gabriel Ricardo s/infr. art. 189 bis CP*”, rta. el 31/8/2015; Nro. 47207/2019-1, “*Incidente de apelación en autos ‘NN s/ 128 I parr – delitos atinentes a la pornografía infantil’*”, rta. el 24/11/20, entre otras).

Siendo así, y al no apreciarse, en el marco de las presentes, una situación que habilite a los suscriptos a declarar la nulidad solicitada, o bien, un perjuicio para el recurrente en virtud de la modificación del código “*hash*” en el acta de resguardo del caso, no cabe hacer lugar al planteo defensista, pues la sanción de invalidez tiene como objetivo subsanar los perjuicios efectivos que pudieran surgir del mencionado acto, y en el caso no se advierte que se haya afectado algún derecho o interés legítimo de la defensa como para que se declare nulo.

En esa medida, consideramos que corresponde confirmar la decisión de la magistrada de grado en cuanto fuera materia de agravio. Así votamos.

Por lo expuesto, el tribunal, por mayoría,

RESUELVE:

I. CONFIRMAR la decisión de la magistrada de grado dictada el 2 de junio de 2021, en cuanto resolvió “*II. RECHAZAR el planteo de nulidad referido a la pérdida de la cadena de custodia de una captura de pantalla del celular de la denunciante*”.

II. TENER PRESENTES las reservas formuladas.

Regístrese, notifíquese mediante medios electrónicos y, oportunamente, remítase al Juzgado de origen mediante el sistema EJE, a sus efectos.

Ante mí:



Poder Judicial
Ciudad de Buenos Aires

JUZGADO N°26|EXP:41459/2019-3 CUIJ J-01-00046145-4/2019-3|ACT 2160870/2021

Protocolo N° 327/2021

FIRMADO DIGITALMENTE 05/10/2021 14:38



Sergio Delgado
JUEZ/A DE CAMARA
CÁMARA DE
APELACIONES EN LO
PPJCyF - SALA III



Marcelo Vazquez
JUEZ/A DE CAMARA
CÁMARA DE
APELACIONES EN LO
PPJCyF - SALA I



**Elizabeth Adriana
Marum**
JUEZ/A DE CAMARA
CÁMARA DE
APELACIONES EN LO
PPJCyF - SALA I



María Teresa Doce
SECRETARIO/A
CÁMARA DE
APELACIONES EN LO
PPJCyF - SALA III