Roj: **AAN 940/2023** - **ECLI:ES:AN:2023:940A**

Id Cendoj: **28079220022023200065**
Órgano: **Audiencia Nacional. Sala de lo Penal**
Sede: **Madrid**
Sección: **2**
Fecha: **08/02/2023**
Nº de Recurso: **47/2021**
Nº de Resolución: **73/2023**
Procedimiento: **Extradición**
Ponente: **FERNANDO ANDREU MERELLES**
Tipo de Resolución: **Auto**

AUD.NACIONAL SALA PENAL SECCION 2

MADRID

Rollo de Sala: Extradición núm. 47/2021

Extradición núm. 86/2021

Procedimiento de Origen: Extradición núm. 34/2021 y 60/2021

Órgano de Origen: Juzgado Central de Instrucción núm. 5

Reclamado: Nicanor

(A)Tribunal de Distrito de Estados Unidos para el Distrito Norte de California

Caso núm. 3:21-mj-70812 MAG

(B) Tribunal de Distrito de los Estados Unidos para el Distrito Sur de Nueva York

Caso núm. 21 Cr. 536

Estados Unidos de América

ILMOS SRES. MAGISTRADOS:

D. JOSÉ ANTONIO MORA ALARCÓN (Presidente)

D. FERNANDO ANDREU MERELLES (Ponente)

Dª MARÍA TERESA GARCÍA QUESADA

AUTO: 00073/2023

En la Villa de Madrid, a ocho de febrero de dos mil veintitrés.

Vistos por la Sección Segunda de la Sala de lo Penal de la Audiencia Nacional, el Rollo de Sala nº 47/2021, correspondiente al procedimiento de extradición nº 34/2021, del Juzgado Central de Instrucción n° 5, seguido a instancias de las Autoridades Judiciales de los Estados Unidos de América, contra el ciudadano de nacionalidad británica, **D. Nicanor** , nacido en Liverpool, Inglaterra, el día NUM000 de 1.999, con pasaporte del Reino Unido nº NUM001 .

Está representado, por el Procurador de los Tribunales D. Ignacio AGUILAR FERNÁNDEZ y defendido por el letrado D. Carlos GÓMEZ-JARA DÍEZ, habiendo sido parte el Ministerio Fiscal.

El reclamado se encuentra en situación de prisión provisional, decretada en Auto de fecha 22 de julio de 2.021, habiendo sido detenido el día 21 de julio de 2.021.

ANTECEDENTES DE HECHO.

PRIMERO.- El día 21 de julio de 2.021, en DIRECCION000 (Málaga), se procedió a la detención del ciudadano de nacionalidad británica, D. Nicanor , ya circunstanciado, y ello en virtud de la orden internacional de detención registrada en Interpol con nº NUM002 , publicada el día 14 de julio de 2021, emitida por las autoridades judiciales de los Estados Unidos de América, con fines de extradición, a fin del enjuiciamiento del reclamado, al estar siendo acusado de la comisión de los siguientes cargos:

- **Cargos uno, tres y cinco**: Conspiración para cometer un delito contra los Estados Unidos, es decir, accesar una computadora sin autorización y así obtener información de una computadora protegida, en infracción de la sección 1030(a)(2) (C) del Título 18 del Código de los Estados Unidos, todo en infracción de la Sección 371 del Título 18 del Código de los Estados Unidos.

Penas: Cinco años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

- **Cargos dos y cuatro**: Intrusión en computadora, es decir, accesar intencionalmente una computadora sin autorización y así obtener información de una computadora protegida, en infracción de la sección 1030(a)(2) (C) del Título 18 del Código de los Estados Unidos, y ayudar e instigar, en infracción de la sección 2 del Título 18 del Código de los Estados Unidos

Penas: Cinco años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

- **Cargo seis**: Conspiración para cometer un delito contra los Estados Unidos, es decir, accesar intencionalmente una computadora sin autorización y con la intención de extorsionar a una persona para obtener algo de valor, y transmitir una comunicación que contiene una amenaza para que se revele información confidencial, o transmitir una comunicación que contiene una demanda o solicitud de algo de valor en relación con daño a una computadora protegida cuando ese daño ha sido causado para facilitar la extorsión, en infracción de la sección 1030(a)(7) del Título 18 del Código de los Estados Unidos, todo en infracción de la sección 371 del Título 18 del Código de los Estados Unidos

Penas: Cinco años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso

- **Cargo siete**: Comunicaciones extorsivas, es decir, transmitir a sabiendas en el comercio interestatal y extranjero, con intención de extorsionar a una persona para obtener algo de valor, una comunicación que contenía una amenaza de daño a la reputación de otra persona, en infracción de la sección 875(d) del Título 18 del Código de los Estados Unidos.

Penas: Dos años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

- **Cargos ocho y diez**: acoso, es decir, con intención de hacer daño, hostigar y causar una angustia emocional significativa a una persona en otro estado, usando instalaciones de comercio interestatal y extranjero, entre ellos un servicio interactivo de computadora y un servicio de comunicación electrónica, para participar en una conducta que causa una angustia emocional significativa a la víctima y la coloca en un estado de temor razonable de muerte o grave lesión corporal, en infracción de la sección 2261A(2) del Título 18 del Código de los Estados Unidos.

Penas: Cinco años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

- **Cargo nueve**: Comunicaciones amenazantes, es decir, enviar a sabiendas un mensaje en el comercio interestatal y extranjero que contenía una verdadera amenaza de hacer daño a otra persona, en infracción de la sección 875(c) del Título 18 del Código de los Estados Unidos.

Penas: Cinco años de prisión, tres años de libertad supervisada: una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

El Juzgado Central de Instrucción núm. 5, incoó, en fecha 21 de julio de 2.021, el procedimiento de extradición nº 34/2021.

El Consejo de Ministros, en su reunión del día 7 de septiembre de 2021, acordó la continuación, en vía judicial, de los procedimientos de extradición.

En la citada documentación se aportaba:

a) Nota Verbal nº 579, de fecha 19 de agosto de 2.021, de la Embajada de EE.UU. en Madrid relativa a la solicitud de extradición del reclamado Nicanor , por la que adjunta documentación extradicional.

b) Denuncia penal formulada por el agente especial del FBI, R. Montgomery ante el Tribunal Federal del Distrito de los Estados Unidos para el Distrito Norte de California.

c) Declaración Jurada en apoyo de la solicitud de Orden de Aprehensión y Denuncia Penal.

d) Orden de arresto, de fecha 14 de mayo de 2021, dictada por el Tribunal de Distrito de los Estados Unidos para el Distrito Norte de California, en el caso núm. 3:21-mj-70812 MAG.

e) Textos legales

f) Ley de prescripción

SEGUNDO. - Los hechos en los que se basa la presente reclamación extradicional son los siguientes:

A. El jaqueo de Twitter - Cargo Uno

El papel desempeñado por " DIRECCION001 " en el jaqueo de Twitter de julio de 2020

8.Twitter, Inc. (Twitter") opera un servicio de microblogging y de red social utilizado por individuos y compañías de alto perfil. El 15 de julio de 2020, múltiples cuentas de individuos de alto perfil fueron afectadas, incluidas las cuentas pertenecientes al exvicepresidente Joseph Biden, al expresidente Barack Obama y a Bill Gates. Las cuentas de Twitter pertenecientes a compañías prominentes y a intercambios de criptomonedas también fueron afectadas Durante el ataque, Twitter detecto un esfuerzo coordinado de ingeniería social dirigido a los empleados de su compañía que tenían acceso a las herramientas y los sistemas internos. Twitter determino además que se atacaron aproximadamente 130 cuentas durante el incidente y que, respecto a un subconjunto de estas cuentas los atacantes lograron el control de las cuentas y enviaron Tweets desde las cuentas.

9.Durante el curso de esta investigación, las autoridades del orden público determinaron que un individuo, mencionado en la presente como "Menor 1", jugo un papel central en el jaqueo de Twitter de julio de 2020.

10.Los registros obtenidos de Discord, Inc. relacionados con los chats de individuos implicados en el jaqueo de Twitter revelaron (pie, empleando el nombre de usuario " DIRECCION002 " el Menor 1 había enviado a múltiples individuos imágenes de una herramienta administrativa interna usada por Twitter para hacer cambios en las cuentas de los usuarios, y que también se había comunicado con individuos para comprar el acceso a varias cuentas de Twitter. El 31 de julio de 2020 se aprehendió al Menor 1.

11.Un individuo que actuaba como intermediario del Menor 1 ha admitido ante las autoridades de los EE. UU. que, durante las comunicaciones a través de Discord, durante el jaqueo de Twitter, un individuo que quería comprar la cuenta de Twitter "@ DIRECCION003 " se identificó como " Nicanor " y usó una cuenta de Discord con el nombre de usuario " DIRECCION004 "

12.Los registros proporcionados por Discord corroboran que Nicanor era ese individuo. La cuenta de Discord "Deleted DIRECCION005 " tuvo varios cambios de nombres y, durante el jaqueo de Twitter, fue llamada " DIRECCION006 ". "Deleted User DIRECCION007 " se comunicó con el Menor 1 y otros intermediarios del Menor 1 y en varios chats confirmaron que su identidad era " DIRECCION001 ", que su ubicación actual era España y que provenía de Inglaterra. Específicamente, el 15 de julio de 2020, "Deleted DIRECCION005 " se comunicó con un individuo que actuaba como intermediario del Menor 1 en relación con el costo de las cuentas de Twitter "@ DIRECCION003 ", "@ DIRECCION008 ", "@ DIRECCION009 ", "@ DIRECCION010 " y "@ DIRECCION011 ". entre otras. El intermediario, a su vez le transmitió al Menor 1 que " DIRECCION012 " tenía interés en adquirir la cuenta de Twitter "@ DIRECCION003 " y también le pidió al Menor 1 que cambiara el avatar de la cuenta y el nombre de usuario por " DIRECCION012 ".

13.Ademas, el intermediario del Menor 1 les informó a las autoridades de los EE. UU. que conocía el nombre " Nicanor ", que pertenecía a un jáquer que usaba el nombre de usuario de Twitter "@ DIRECCION013 " y el seudónimo en lima " DIRECCION001 ". Los registros proporcionados por Twitter corroboran que el usuario de la cuenta de Twitter "@ DIRECCION013 " estaba visualizando cuentas implicadas en el jaqueo con el objeto de determinar si tales cuentas estaban suspendidas o activas y que después averiguaba con los intermediarios si podía comprar esas cuentas. El 15 de Julio de 2020, "@ DIRECCION013 " visualizó al menos diez cuentas a las que posteriormente accedió el atacante o que fueron controladas durante el jaqueo de Twitter. Entre

estas cuentas figuraban, entre otras, "@ DIRECCION003 ", "@ DIRECCION008 ", "@ DIRECCION009 ", @ DIRECCION010 " y "@ DIRECCION011 ", las mismas cuentas solicitadas por "Deleted User DIRECCION007 ".

14.Los registros de Twitter obtenidos sobre "@ DIRECCION013 " revelan el nombre de usuario " Nicanor ". Mas aun, en múltiples mensajes, el usuario de la cuenta "@ DIRECCION013 " se define a sí mismo como " DIRECCION001 " y declaró que la cuenta "@ DIRECCION013 " había reemplazado a su cuenta "@ DIRECCION001 ". El 4 de julio de 2020, "@ DIRECCION013 " envió un mensaje con un enlace para un video que contenía el audio de un individuo que hablaba, y durante el curso de esta investigación, las autoridades de los EE. UU. identificaron la voz de Nicanor en la parte de audio del video. El 15 de julio de 2020, "@ DIRECCION013 " publico un mensaje público que incluía una imagen de la herramienta administrativa interna de Twitter que estaba entrando a una cuenta afectada durante el jaqueo de Twitter. Además, las direcciones de IP de inicio de sesión más recientes de la cuenta "@ DIRECCION013 " coincidían con las usadas para iniciar sesión en la cuenta de Discord "Deleted DIRECCION005 ".

B. Identificación de " DIRECCION001 " como Nicanor

15.Desde fines de 2018, agentes del orden público de la Fuerza Operativa REACT, una fuerza operativa con sede en California compuesta por agencias locales, estatales y federales dedicadas a los delitos de alta tecnología, comenzaron a recibir información acerca de la actividad ilegal de un individuo que usaba el seudónimo en línea de " DIRECCION001 ". A partir de enero de 2019, un individuo que se identificaba como " DIRECCION001 " comenzó a comunicarse con los agentes del orden público de REACT, usando múltiples números de teléfono de Google Voice. Durante sus comunicaciones en 2019 y 2020, el individuo que finalmente se identificó como " Nicanor " admitió que usaba el seudónimo " DIRECCION012 " y explico que se había mudado a España debido a las amenazas de muerte que recibía en relación con la actividad ilegal en la que estaba implicado.

16.Despues de que se conociese públicamente el jaqueo de Twitter el 15 de julio de 2020, REACT recibió una serie de mensajes de texto de un individuo que se identificaba como " Nicanor " y que usaba el número NUM003 . El individuo también llamo a REACT y envió mensajes a través de la línea para informantes en internet identificándose como " Rubén " y " DIRECCION012 ", usando el número NUM004 , la dirección de correo DIRECCION014 , y la dirección de IP NUM005 . Las autoridades de los EE.UU. han vinculado a la dirección de IP NUM005 con otras cuentas que se cree que han sido usadas por Nicanor .

17.El 23 de julio de 2020, REACT y los agentes del FBI llamaron a Nicanor al número de teléfono NUM004 . Los agentes de REACT reconocieron la voz porque era la del individuo que anteriormente se había identificado como Nicanor . Las autoridades de los EE. UU. Se dirigieron a Nicanor como "Sr. Nicanor " y " Rubén ", y el hizo referencia a su seudónimo en línea " DIRECCION001 ". En cuanto al jaqueo de Twitter del 15 de julio de 2020, Nicanor admitió que, durante el jaqueo de Twitter, él había estado en un chat con otros individuos, cuyos nombres especificó y que son conocidos por las autoridades de los EE.UU. debido a su participación en el jaqueo de Twitter. Nicanor le pregunto a uno de los individuos sobre la compra de algunas cuentas de Twitter, y el individuo acepto conseguir cuentas para revenderlas y obtener una ganancia. Uno de los individuos envió una fotografía de las herramientas administrativas de Twitter, que Nicanor publicó posteriormente en Twitter. Si bien Nicanor negó haber comprado la cuenta de Twitter "@ DIRECCION003 ", confirmó que a su pedido el nombre de la cuenta "@ DIRECCION003 " fue cambiado por " DIRECCION012 ". Nicanor admitió además que hablo con un individuo, a quien llamó " DIRECCION002 " en un chat grupal.

18.Las autoridades de los EE.UU. analizaron los rastros en relación con los números de Google Voice NUM003 y NUM004 . Con base en las direcciones de IP asociadas con ambas cuentas, las autoridades pudieron vincular las cuentas con las cuentas de internet usadas por Nicanor durante el transcurso de su conducta delictiva descrita en la presente en relación con el jaqueo de Twitter de julio de 2020 y otras conductas delictivas de 2019-2020 (que se tratan a continuación).

19.Como se mencionó anteriormente, en múltiples mensajes enviados desde la cuenta "@ DIRECCION013 " el usuario dijo que la cuenta "@ DIRECCION013 " reemplazaba a su cuenta "@ DIRECCION001 ". Los registros obtenidos de la cuenta de Twitter "@ DIRECCION001 " revelaron que el 4 de mayo de 2018 el usuario "@ DIRECCION001 " publicó un mensaje que mencionaba las "fotos de la niñez" del usuario e incluyo una imagen de un pasaporte del Reino Unido de Nicanor , donde consta la fecha y el lugar de nacimiento. Las autoridades del Reino Unido han confirmado que la fecha y el lugar de nacimiento de Nicanor coinciden con la información que figura en la imagen del pasaporte.

20.Ademas, las autoridades de los EE. UU. han podido vincular las otras cuentas de internet con Nicanor , incluida la cuenta de Snapchatl. DIRECCION015 ". Las autoridades de los UU. analizaron los registros proporcionados por Snap Inc. sobre esta cuenta de Snapchat. Estos registros incluían una fotografía del 30 de agosto de 2019 de un pasaporte del Reino Unido de Nicanor , donde constaban la fecha y el lugar de nacimiento, y el número del pasaporte. Con base en las conversaciones mantenidas con la Agencia Nacional de Crímenes (National Crime

Agency) del Reino Unido, la fecha de nacimiento, el lugar de nacimiento y el número de pasaporte del Reino Unido de Nicanor coinciden con la información de la imagen del pasaporte.

21.El FBI también ha analizado los archivos de audio y video que contienen grabaciones de voz de las cuentas "@ DIRECCION013 " de Twitter, "@ DIRECCION001 " de Twitter y DIRECCION015 " de Snapchat, conjuntamente con otras cuentas relacionadas con Nicanor . El FBI ha confirmado que la voz que se escucha en estas grabaciones es la voz del individuo que ha hablado con los agentes de REACT y que se identificó como Nicanor .

22.Las pruebas en apoyo del jaqueo de Twitter se exponen más detalladamente en los párrafos 25-83 de mi declaración jurada en poyo de la denuncia, la cual se anexa a la declaración jurada del fiscal en la Prueba A.

B. El jaqueo de la cuenta de TikTok de la Victima 1- Cargos Dos v Tres

23.TikTok es un servicio de red social para compartir videos que se Lisa para crear videos cortos que se pueden compartir o almacenar pública o privadamente. TikTok permite a sus usuarios interactuar entre si a través de comentarios sobre los videos, mensajes directos y chats en vivo. Desde el 14 hasta el 15 de agosto de 2020, alguien accedió sin autorización y tomo el control de la cuenta de TikTok de la Victima 1 La cuenta de TikTok de la Victima 1 es una de las cuentas de TikTok más vistas y con más seguidores. El nombre de usuario de TikTok de la Victima 1 se cambió por " DIRECCION016 " y la sección biográfica de la cuenta se cambió para incluir el mensaje " DIRECCION001 DIRECCION016 n crippin". Además, se publicaron múltiples videos en la cuenta durante el tiempo en que estuvo afectada.

24.Los registros proporcionados por TikTok revelaron que primero accedieron a la cuenta mediante una dirección de IP particular y que el primer dispositivo móvil para acceder a la cuenta durante la afectación también se usó para acceder a la cuenta de TikTok " DIRECCION017 ", la cual está vinculada con la cuenta de Twitter "@ DIRECCION018 ". Los registros de Twitter revelaron direcciones de IP relacionadas con la cuenta "@ DIRECCION018 " que han podido vincular esa cuenta con cuentas de internet usadas por Nicanor , incluida la cuenta de Instagram "@ DIRECCION019 ". Además, en múltiples mensajes enviados desde la cuenta "@ DIRECCION013 ", el usuario dijo que el usaba la cuenta "@ DIRECCION018 ". Como se mencionó anteriormente, el usuario de la cuenta "@ DIRECCION013 " declaro que esa cuenta reemplazaba a su cuenta "@ DIRECCION001 ", desde la cual el usuario había publicado la imagen de un pasaporte de Nicanor .

25.Ademas, las autoridades de los EE. UU. obtuvieron los registros de la cuenta " DIRECCION020 " de Snapchat. Los registros de la cuenta de Snapchat revelaron las direcciones de IP relacionadas con otras cuentas usadas por Nicanor . Las imágenes y comunicaciones de la cuenta " DIRECCION020 " contenían múltiples capturas de pantalla de la cuenta de Twitter "@ DIRECCION013 ", referencias a " DIRECCION001 " y capturas de pantalla de chats donde aparecía el nombre de usuario de Discord " DIRECCION006 ". La cuenta también contenía cientos de imágenes, archivos de audio y archivos de video del usuario de la cuenta, que se que coinciden con la voz y la imagen de Nicanor .

26.La cuenta " DIRECCION020 " de Snapchat también contenía mensajes de chat e imágenes en relación con la afectación de la cuenta de TikTok de la Victima 1. Durante las dos semanas anteriores a la afectación de la cuenta de TikTok de la Victima 1, el usuario de la cuenta " DIRECCION020 " se comunicó con otros individuos para hablar sobre varios individuos conocidos y también sobre sus números de teléfono, entre ellos, el de la Victima 1. Un individuo, con quien se comunicó el usuario de la cuenta " DIRECCION020 ", solicitó un reconocimiento de la cuenta "@ DIRECCION021 " de Twitter si se lograba afectar la cuenta de TikTok de la Victima 1. El 14 de agosto de 2020, el usuario de la cuenta " DIRECCION020 " envió una comunicación que contenía una captura de pantalla de la página con el

perfil de la cuenta de TikTok de la Victima 1, lo cual indicaba que había iniciado sesión. El 15 de agosto de 2020, publicaron videos en la cuenta de TikTok de la Victima 1 con referencias a " DIRECCION001 ", la cuenta "@ DIRECCION021 " de Twitter, los cuales contenían una voz que yo sabía que era la de Nicanor .

27.Las pruebas en apoyo del jaqueo de la cuenta de TikTok de la Victima 1 se exponen más detalladamente en los párrafos 84-96 de mi declaración jurada en apoyo de la denuncia, la cual se anexa a la declaración jurada del fiscal en la Prueba A.

C. El jaqueo de la cuenta de Snapchat de la Victima 2 y subsiguiente tentativa de extorsión y acoso - Cargos Cuatro, Cinco, Seis, Siete y Ocho

28.Snapchat es una aplicación muy conocida para enviar y recibir mensajes, fotografías y videos que "se autodestruyen". Snapchat, suministrada por Snap, Inc., es una aplicación de mensajería que ofrece múltiples formas de comunicación entre sus usuarios. Desde el 13 hasta el 15 de junio de 2019, alguien accedió y tomo el control de la cuenta de Snapchat de la Victima 2. La Victima 2 es una personalidad publica y fue una de las noticias en los medios que la cuenta de Snapchat de la Victima 2 había sido jaqueada, que se habían obtenido

fotografías de desnudos de la cuenta y que los jáqueres habían hecho intentos para extorsionar a la Victima 2 con la amenaza de difusión de las fotografías de los desnudos.

29.Como se mencionó, las autoridades de los EE UU. analizaron los registros de Snap relacionados con la cuenta de Snapchat " DIRECCION015 ". Como se mencionó anteriormente, se publica una fotografía del pasaporte de Nicanor desde esta cuenta el 30 de agosto de 2019. Además, los registros de la cuenta de Snapchat revelaron las direcciones de IP relacionadas con otras cuentas usadas por Nicanor .

30.El 13 de junio de 2019 el usuario de la cuenta " DIRECCION015 " envió un video de la pantalla de un teléfono celular que gababa en la red Vodafone del RU con el reloj que marcaba las 22:06 (lo cual indicaba que estaba en una zona horaria UTC +1) a un iPhone que estaba recibiendo una serie de notificaciones de la aplicación de Snapchat. Momentos después, el usuario envió una captura de pantalla de la página con el perfil de Snapchat de la Victima 2,10 cual demostraba que el usuario había iniciado sesión. Horas después, el usuario de la cuenta " DIRECCION015 " envió numerosas fotografías de desnudos de la Victima 2 a múltiples personas.

31. Los registros de la cuenta de Snapchat de la Victima 2 revelan que mientras la cuenta estuvo afectada, se publicaron mensajes mencionando las cuentas " DIRECCION015 " de Snapchat, "@ DIRECCION001 " de Twitter y " DIRECCION019 " de Instagram, en los que decían que publicarían las fotografías de los desnudos de la Victima 2 cuando las cuentas de los medios sociales alcanzaran a un determinado umbral de seguidores. Además, las IP de inicio de sesión de la cuenta de Snapchat de la Victima 2 mientras estuvo afectada coinciden con las direcciones de IP usadas para iniciar sesión en otras cuentas relacionadas con Nicanor .

32.El 15 de junio de 2019, el usuario de la cuenta "cute" de Snapchat envió una captura de pantalla a " DIRECCION015 " con el texto de una conversación entre un número de teléfono y un individuo que decía que él/ ella había jaqueado la cuenta de la Victima 2 y le indicaba a la Victima 2 que publicara un tweet porque de lo contrario "todo el mundo en internet [estará] mirando tu mierda personal". El FBI sabe que el número de teléfono pertenece a la Victima 2.

33. La Victima 2 informó a las autoridades del orden publico, entre ellas a las autoridades de los EE. UU., que la Victima 2 había recibido un mensaje de texto de un jáquer, quien afirmaba que había obtenido los "desnudos" de la Victima 2 y que el "no se los mostraría a nadie ni los filtraría" si la Victima 2 publicaba un tweet agradeciendo a varios individuos, entre ellos a " DIRECCION001 " por devolver las cuentas [de la Victima 2]". El individuo proporciono prueba de las fotografías a la Victima 2 usando las imágenes que " DIRECCION015 " había compartido con otras personas. Los mensajes de texto entre el individuo y la Victima 2 incluían el extracto que el usuario de la cuenta " DIRECCION022 " le he había enviado a " DIRECCION015 ".

34.Subsiguientemente, el 15 de junio de 2019, la Victima 2 publicó en Twitter que había sido "amenazado(a) con mis propios desnudos", y publicó capturas de pantalla del mensaje de texto con el individuo que la/lo había estado extorsionando, en la que incluía un número de teléfono. Poco después, el usuario de la cuenta " DIRECCION022 " le envió un mensaje a " DIRECCION015 " diciendo, "[Victima 2] filtro mi GVoice [Google Voice]".

35.Las pruebas en apoyo del jaqueo de la cuenta de Snapchat de la Victima 2 y los delitos relacionados se exponen más detalladamente en los párrafos 97-107 de mi declaración jurada en apoyo de la denuncia, la cual se anexa a la declaración jurada del fiscal en la Prueba A.

D. Swatting v el acoso informativo de la Víctima 3 - Cargos Nueve y Diez

37.Los informes presentados en junio de 2020 ante el Departamento de Policía de Garden Grove ("GGPD", por sus siglas en ingles) en Garden Grove, California, y otras agencias del orden público relacionan a Nicanor con varios incidentes de swatting .

38.En el primer informe se describe un incidente ocurrido el 25 de junio de 2020 en el cual el GGPD envió a sus agentes a una residencia (mencionada en la presente como "Residencia 1") en relación con un individuo armado y peligroso que amenazaba con matar a su esposa e hijos. Mientas los agentes se dirigían al lugar, la persona que los había llamado aviso a la Autoridad de Bomberos del Condado de Orange (OCSD, por sus siglas en ingles) que en la Residencia 1 había un incendio y también le dijo al OCSD que él estaba en la Residencia 1 y que iba a matar a su esposa e hijos. Los agentes del GGPD se comunicaron con los ocupantes de la Residencia 1 y se enteraron de que ellos no habían llamado a las autoridades del orden público. Una segunda denuncia presentada ante el GGPD describía un incidente similar en la escuela secundaria el 25 de junio de 2020. Una tercera amenaza ocurrida el 25 de junio de 2020 fue publicada en la plataforma de comunicación social Reddit, tomo de punto a un restaurante y panadería en Garden Grove y usó un lenguaje similar al de las dos amenazas anteriores. En una cuarta amenaza ocurrida el 25 de junio de 2020, el individuo llamó al Departamento del Alguacil del Condado de Orange ("OCSD", por sus siglas en ingles) y amenazó con hacer volar un aeropuerto a menos que enviaran dinero a la Residencia 1, y también subsiguientemente llamó para decir que el tenía un arma y que acababa de matar a su esposa en la Residencia 1. La información del abonado del número

de teléfono y la dirección de correo asociadas con estas denuncias los vinculaban con otras cuentas que se sabía que eran usadas por Nicanor . El FBI ha confirmado que la voz de la llamada que fue gabada coincide con la voz de Nicanor .

39. Luego de investigar las denuncias presentadas ante el GGPD, el GGPD se comunicó con un menor (mencionado en la presente como la "Victima 3") quien vivía cerca de la Residencia 1 y tenía un nombre similar al nombre que figuraba en las denuncias con las amenazas La Victima 3 informó que cuatro días antes de los incidentes, el/ella se había reunido con un varón de 21 años de edad llamado " Nicanor " en un chat de Discord, quien le había dicho que era de España. La Victima 3 identificó el seudónimo de Instagram de " Nicanor " como "@ DIRECCION019 ". " Nicanor " comenzó a enviarle a la Victima 3 mensajes sexualmente inapropiados y amenazantes, aún después de que la Victima 3 le había dicho a " Nicanor " que él/ella tenía 16 años. La Victima 3 también dijo que Nicanor había hecho una llamada en vivo a la policía por Discord. La Victima 3 creía que " Nicanor " fue quien hizo esas llamadas de emergencias falsas.

40. Las autoridades de los EE.UU. entrevistaron a la Victima 3, quien confirmó que la información que el él/ella le había proporcionado anteriormente al GGPD era exacta. Además, la Victima 3 declaró que " Nicanor " empezó a llamar a varios familiares de la Victima 3 el 16 de julio de 2020 desde el número de teléfono NUM003 , un número de Google Voice que usó para comunicarse con REACT seguidamente del jaqueo de Twitter. En cada llamada que les hizo a los familiares de la Victima 3 " Nicanor " los amenazó con matar a la persona con la que estaba hablando. En las múltiples conversaciones que mantuvo con " Nicanor " la Victima 3 tomo conocimiento de que " Nicanor " había nacido en el Reino Unido y que había cursado la escuela en España. La Victima 3 se enteró de que el nombre de " Nicanor " era " Nicanor " cuando la Victima 3 le pidió a " Nicanor " que confirmara su nombre.

41. Las autoridades de los EE. UU. obtuvieron registros de la cuenta " DIRECCION019 " de Instagram, de la cuenta " DIRECCION023 " de Discord y de la cuenta " DIRECCION020 " de Snapchat, cada una de los cuales reveló comunicaciones con y sobre la Victima 3. En los mensajes de la cuenta " DIRECCION020 " de Snapchat, el usuario de la cuenta " DIRECCION020 " declaro "Yo te "doxe" y llame a tu mama" . El 24 de junio de 2020, un día antes de los incidentes de swatting, el usuario de la cuenta " DIRECCION020 " le dijo a la Victima 3, "keep my name our ur mouth (sic) (mantén mi nombre en tu boca).

Los mensajes de la cuenta " DIRECCION023 " de Discord incluían el nombre de la Victima 3, de la escuela secundaria, la dirección de Residencia 1 y varias cuentas de medios sociales pertenecientes a la Victima 3 Los registros de LP de cada una de estas cuentas, junto con las cuentas relacionadas con la amena7a publicada en Reddit y las amenazas hechas usando un número de Google Voice que llamó al GGPD y a OCSD, demuestran una superposición con otras cuentas usadas por Nicanor .

42. Las pruebas en apoyo del swatting y del acoso informático contra la Victima 3 se exponen rads detalladamente en los párrafos 108-121 de mi declaración jurada en apoyo de la denuncia, la cual se anexa a la declaración jurada del fiscal en la Prueba A.

II. LA IDENTIFICACION DE Nicanor

43. Como se afirmó anteriormente, el usuario de la cuenta "@ DIRECCION001 " de Twitter y el usuario de la cuenta ' DIRECCION015 " de Snapchat anteriormente había publicado imágenes de un pasaporte que identificaba al usuario de estas cuentas como " Nicanor ". Por otro lado, el usuario de la cuenta "@ DIRECCION013 " de Twitter afirmo que la cuenta "@ DIRECCION013 " reemplazaba a su cuenta " DIRECCION001 ". El usuario de "@ DIRECCION013 " también dijo que él era el dueño de la cuenta "@ DIRECCION018 " de Twitter. La cuenta "@ DIRECCION018 " se usó para crear la cuenta " DIRECCION017 " de TikTok.

44.En las cuentas "@ DIRECCION013 " y "@ DIRECCION001 " de Twitter y la cuental " DIRECCION015 " de Snapshot se publicaron archivos de audio y video que contenían grabaciones de voz. Los agentes de REACT escucharon las grabaciones de voz y dijeron que ellos creen que la voz coincide con la de la persona que anteriormente hablo con dos y que se identifica como Nicanor .

45.Las cuentas de Snapchat y Twitter también tenían una importante superposición de IP con otras cuentas que se creía que eran usadas por Nicanor y que estaban relacionadas con el jaqueo de Twitter, con la afectación de la cuenta de TikTok de la Victima 1, con la afectación de la cuenta de Snapchat de la Victima 2 y con los subsiguientes intentos de extorsión y amenazas informáticas de la Victima 3. Las direcciones de LP superpuestas también se usaron para iniciar amenazas informáticas y el incidente de swatting, así como para iniciar sesión en las cuentas de Twitter y Snapchat que se sabía que Nicanor usaba.

46. Como se afirmó anteriormente, el individuo que se comunicó con la fuerza operativa REACT y que hablo con las autoridades de los EE. UU. fue quien se comunicó con los agentes de REACT desde enero de 2019 y se identificó como " Nicanor " y " DIRECCION001 ". El individuo que hablo con la Victima 3, que uso la cuenta

" DIRECCION019 " de Instagram y la cuenta " DIRECCION020 " de Snapchat confirmó que su nombre era " Nicanor ".

47. Nicanor nació el NUM000 de 1999 en el Reino Unido y es un ciudadano del Reino Unido. Nicanor es varón y tiene el cabello castaño. Nicanor tiene pasaporte del Reino Unido con el número NUM001 .

48.Se sabe que Nicanor utiliza los seudónimos " DIRECCION001 " y " DIRECCION012 ", como se ha visto en las comunicaciones en varias plataformas de los medios sociales y en fuentes de dominio publico, y se refirió a si mismo mediante su seudónimo en la entrevista con el FBI.

49.Se adjuntan a la presente declaración jurada en la pestaña 1 imágenes parciales de dos de los pasaportes del Reino Unido de Nicanor encontradas en las cuentas de los medios sociales utilizadas por Nicanor . En los pasaportes constan el nombre completo de Nicanor (Nicanor), el pasaporte del Reino Unido número (NUM001), la nacionalidad (ciudadano británico), la fecha de nacimiento (NUM000 99), el sexo (M) y el lugar de nacimiento (DIRECCION024). También se adjuntan a la presente declaración jurada en la Pestaña 1 dos fotografías que se cree que son de Nicanor , las cuales se encontraron en las cuentas de los medios sociales utilizadas por Nicanor .

TERCERO. - Celebrada por el Juzgado Central de Instrucción nº 5 la comparecencia prevista en el artículo 12 de la Ley de Extradición Pasiva en fecha de 1 de febrero de 2019, el reclamado manifestó que no consentía a la entrega a las autoridades reclamantes y que no renunciaba al principio de especialidad extradicional.

Mediante resolución de fecha 23 de noviembre de 2021, se acordó elevar el procedimiento de extradición a la Sección Segunda de la Sala de lo Penal de la Audiencia Nacional, donde tuvo entrada el 23 de diciembre de 2.021.

CUARTO. - Evacuado el traslado del procedimiento, al Ministerio Fiscal y a la defensa del reclamado, por el Ministerio Fiscal se presentó informe por el que interesaba se acceda a la solicitud de extradición formulada.

Por la defensa del reclamado se mostró su oposición a la entrega extradicional, interesando se deniegue la misma en base a las alegaciones formuladas en su escrito.

QUINTO. - Señalada la vista para el día 10 de marzo de 2022, esta tuvo lugar, y en la misma el Ministerio Fiscal interesó la acumulación al presente procedimiento del procedimiento de extradición seguido en esta misma Sección de la Sala de lo Penal de la Audiencia Nacional con el núm. 86/2021, seguido por la misma autoridad requirente frente al mismo reclamado, y procedente del Juzgado Central de Instrucción núm. 1, extradición núm. 60/2021.

La defensa del reclamado no se opuso a dicha acumulación, acorándose en dicho acto por el Tribunal.

SEXTO. - La acusación formal en que se fundamenta esta ampliación de solicitud extradicional se basa en los siguientes cargos:

CARGO UNO

(Asociación delictuosa para cometer intrusiones informáticas)

El gran jurado imputa que:

Generalidades de la conducta delictiva

1.Aproximadamente entre marzo de 2019 y mayo de 2019, Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, participaron en una estratagema para usar intercambios de SIM a fin de realizar intrusiones cibernéticas con el objeto de robar criptomonedas con un valor aproximado de $784,000 en moneda de los Estados Unidos de una compañía de criptomonedas ubicada en Manhattan ("Compañía-1").

2.Durante una intrusión cibernética, conocida como ataque de intercambio de SIM, los actores de la amenaza cibernética obtienen el control del número de teléfono móvil de la víctima vinculando ese número a una tarjeta de módulo de identidad del suscritor ("SIM") controlada por los actores de la amenaza, lo que resulta en la desviación de las llamadas y los mensajes de la víctima a un dispositivo no autorizado malicioso controlado por los actores de las amenazas. Después, estos actores usan normalmente el control del número de teléfono móvil de la víctima para obtener el acceso no autorizado a cuentas de la víctima registradas con ese número de teléfono móvil,

3. Durante todos los tiempos pertinentes a la acusación formal, la Compañía-1 proporcionó una infraestructura de monederos y software relacionado para efectuar intercambios de criptomonedas en todo el mundo. Aproximadamente entre marzo de 2019 y mayo de 2019, Nicanor , alias " DIRECCION001 ", el acusado, y

sus coconspiradores perpetraron con éxito ataques de intercambio de SIM cuyos objetivos eran al menos tres ejecutivos ("Ejecutivo-1", "Ejecutivo-2" y "Ejecutivo-3") de la Compañía-1,

4. Después de realizar con éxito un ataque de intercambio de SIM cuyo objetivo era el Ejecutivo-1 el 30 de abril de 2019 o alrededor de esa fecha, Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, lograron obtener un acceso no autorizado a múltiples cuentas y sistemas informáticos de la Compañía-1.

5. El 1 de mayo de 2019 o alrededor de esa fecha, usando su acceso no autorizado a cuentas y sistemas informáticos de la Compañía-1, Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, robaron y desviaron fraudulentamente criptomonedas de varios tipos (las "criptomonedas robadas") de monederos de criptomonedas mantenidos por la Compañí-1 en nombre de dos de sus clientes. Las criptomonedas robadas tenían un valor aproximado de $784,000 en moneda de los Estados Unidos en el momento del robo e incluían aproximadamente 770,784869 Bitcoin en efectivo, aproximadamente 6,363.490509 Litecoin, aproximadamente 407,3960974 Ethereum y aproximadamente 7.456728 Bitcoin.

6. Después de robar y desviar de manera fraudulenta las criptomonedas robadas, Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y 2 desconocidos, las lavaron por medio de docenas de transferencias y transacciones, y las intercambiaron por Bitcoin usando servicios de intercambio de criptomonedas. Por último, una parte de las criptomonedas robadas fueron depositadas en una cuenta de intercambio de criptomonedas controlada por Nicanor .

Alegaciones legales

7. Al menos desde aproximadamente marzo de 2019, hasta al menos mayo de 2019 inclusive, en el Distrito Sur de Nueva DIRECCION025 en otros lugares, Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, voluntariamente y a sabiendas combinaron, se unieron en una asociación delictuosa, se confederaron y acordaron juntas y entre sí cometer delitos contra los Estados Unidos, a saber, intrusión informática, en contravención de las secciones 1030 (a) (2) (c), 1030 (c) (2) (B) (i) y (iii), 1030 (a) (4), 1030 (c) (3) (A), 1030 (a) (5) (A), 1030 (a) (5) (B), 1030 (c) (4) (A) (i) (I) y 1030 (c) (4) (13) (i) del Título 18 del Código de los Estados Unidos.

8. Era una parte y un objeto de la asociación delictuosa el que Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, accederían y accedieron intencionadamente a ordenadores sin autorización, y excedieron el acceso autorizado y por lo tanto obtuvieron información de ordenadores protegidos, con el fin de lograr ventajas comerciales y ganancias financieras privadas, y el valor de la información obtenida excedería y excedió los $5,000 en moneda de los Estados Unidos en contravención de la sección 1030 (a) (2) (C) y 1030 (c) (2) (B) (i) y (iii) del Título 18 del Código de los Estados Unidos.

9. Fue además una parte y un objeto de la asociación delictuosa el que Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, los que a sabiendas y de forma intencionada defraudarían, accederían y tratarían de acceder a ordenadores protegidos sin autorización, y excedieron el acceso autorizado, y por medio de dicha conducta cometerían y cometieron el fraude intencionado y obtuvieron algo de valor que excedió los $5,000 en moneda de los Estados Unidos en un período de un año, en contravención de la sección 1030 (a) (4) y (c) (3) (A) del Titulo 18 del Código de los Estados Unidos.

10,Fue además una parte y un objeto de la asociación delictuosa el que Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, a sabiendas efectuarían y efectuaron la transmisión de un programa, información, código y comando y, como consecuencia de dicha conducta, causarían y causaron intencionadamente daños sin autorización a ordenadores protegidos, que causarían y causaron pérdidas (incluidas las perdidas resultantes de un curso de conducta relacionado que afecta a uno y otros mas ordenadores protegidos) agregando al menos un valor de $5,000 en moneda de los Estados Unidos a una o más personas durante cualquier periodo de un año, en contravención de las secciones 1030 (a) (5) (A), 1030 (c) (4) (A) (i) (I) y 1030 (c) (4) (B) (i).

11,Fue además una parte y un objeto de la asociación delictuosa el que Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, a sabiendas y de forma intencionada tuvieron acceso a un ordenador protegido sin autorización, y como consecuencia de dicha conducta, causaron daños temerariamente, y ocasionaron perdidas a una o más personas durante cualquier periodo de 1 año agregando un valor de al menos $5,000 en moneda de los Estados Unidos, en contravención de la sección 1030 (a) (5) (B) y 1030(c) (4) (A) (i) (I) del Título 18 del Código de los Estados Unidos.

Actos manifiestos

12. Para fomentar la asociación delictuosa y afectar a los objetos ilegales de esta, se efectuaron los siguientes actos manifiestos, entre otros, en el Distrito Sur de DIRECCION026 otros lugares:

a. El 30 de abril de 2019 o alrededor de esa fecha, Nicanor , alias " DIRECCION001 ", el acusado, y altos conocidos y desconocidos, perpetraron un intercambio de SIM del número de teléfono móvil usado por el Ejecutivo-1. A las pocas horas del ataque de intercambio de SIM, Nicanor y sus coconspiradores hicieron uso del control del número de teléfono del Ejecutivo-1 para obtener un acceso no autorizado a las cuentas y sistemas informáticos de la Campania-1.

b. El 30 de abril de 2019 y el 1 de mayo de 2019 o alrededor de esas fechas, como parte de su acceso no autorizado a las cuentas y sistemas informativos de la Compailia-1, Nicanor y sus coconspiradores cambiaron las contraseñas de las cuentas de G Suite para varios empleados de la Companfa-1. Como consecuencia, los empleados de la Compania-1, incluidos los empleados en el Distrito Sur de Nueva York, no fueron capaces de acceder a sus cuentas corporativas de G Suite.

c. El 1 de mayo de 2019 o alrededor de esa fecha, haciendo uso de su acceso no autorizado a las cuentas y sistemas informáticos de la Compailla-1, Nicanor y sus coconspiradores desviaron las criptomonedas robadas de los monederos de criptomonedas mantenidos por la Compaffla-1 en nombre de dos de sus clientes a las direcciones de criptomonedas y monederos controlados por Nicanor y sus coconspiradores.

d. El 4 de mayo de 2021 o alrededor de esa fecha, después de unos ataques de intercambio de SIM cuyos objetivos eran el Ejecutivo-2 y el Ejecutivo-3, Nicanor o uno de sus coconspiradores (el "Miembro de la asociación delictuosa") tuvieron acceso a la cuenta Skype del Ejecutivo-3 sin autorización y usaron dicha cuenta para enviar numerosos mensajes por medio de una conversación grupal a empleados de la Comparila-1, incluidos uno o más empleados en el Distrito Sur de Nueva York. Durante la conversación grupal de Skype, el Miembro de la asociación delictuosa describió, en esencia y en parte, el intercambio de SIM cuyo objetivo era el Ejecutivo-1, el acceso no autorizado a las cuentas y sistemas informáticos de la Compailia-1 y el robo resultante de criptomonedas. El Miembro de la asociación delictuosa también planteó preguntas a los empleados de la Compañía-1, en esencia y en parte, sobre la infraestructura informática de la Compania-1 y sus posesiones de criptomonedas de empleados.

(Sección 371 del Título 18 del Código de los Estados Unidos).

La pena máxima por una contravención del delito del que se le acusa en el Cargo Uno es una pena de prisión de 5 años; una sanción de la cantidad que sea mayor entre $250,000 en moneda de los Estados Unidos, el doble de la ganancia pecuniaria bruta derivada del delito o el doble de la perdida pecuniaria bruta a personas que no sean el acusado consecuencia del delito; libertad supervisada de tres años; restitución; y una evaluación especial obligatoria de $100 en moneda de los Estados Unidos

CARGO DOS

(Asociación delictuosa para cometer fraude electrónico)

El gran jurado además imputa que:

13.Las alegaciones establecidas en los párrafos 1 a 6 se incorporan como referencia como si se hubieran establecido completamente aquí.

14.Desde al menos aproximadamente marzo de 2019, hasta at menos mayo de 2019 inclusive, en el Distrito Sur de DIRECCION026 en otros lugares, Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, voluntariamente y a sabiendas combinaron, se unieron en una asociación delictuosa, se confederaron y acordaron juntos y entre sí cometer fraude electrónico, en contravención de la Sección 1343 del Título 18 del C6digo de los Estados Unidos.

15.Fue una parte y un objeto de la asociación delictuosa el que Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, voluntariamente y a sabiendas, habiendo concebido e intentando concebir una estratagema y artificio para defraudar, y obtener dinero y bienes por medio de pretextos, manifiestos y promesas fraudulentos, transmitiría y transmitió e hiciera que se transmitiera por medio de comunicaciones electrónicas y de radio en comercio interestatal e internacional, escritos, anuncios, señales, imágenes y sonidos con el fin de ejecutar dicha estratagema y artificio, en contravención de la sección 1343 del Título 18 del Código de los Estados Unidos, a saber, Nicanor y otros participaron en una estratagema de intercambio de SIM y obtuvieron acceso no autorizado a cuentas en línea y sistemas informáticos para obtener de manera fraudulenta criptomonedas, cuya estratagema comprendía el uso de comunicaciones electrónicas interestatales e internacionales.

(Sección 1349 del Título 18 del Código de los Estados Unidos).

La pena máxima por una contravención del delito del que se le acusa en el Cargo Dos es prisión por 20 dos; una sanción igual a la cantidad que sea mayor entre $250,000 en moneda de los Estados Unidos, el doble de la ganancia pecuniaria bruta derivada del delito o el doble de la perdida pecuniaria bruta a personas distintas del acusado que sea consecuencia del delito; libertad supervisada de tres años; y una cuota especial obligatoria de $100 en moneda de los Estados Unidos.

CARGO TRES

(Robo de identidad con agravante)

El gran jurado además imputa que:

16. Las alegaciones establecidas en los párrafos 1 a 6 se incorporan coma referencia como si se hubieran establecido completamente aquí.

17. Desde al menos marzo de 2019 hasta mayo de 2019 inclusive, en el Distrito Sur de DIRECCION026 en otros lugares, Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, a sabiendas transfirieron, poseyeron y usaron, sin autoridad legal, un medio de identificación de otra persona, durante y en relación con un delito grave por contravención de la sección 1028 A (c) del Titulo 18 del Código de los Estados Unidos, a saber, Nicanor transfirió, poseyó y uso, y ayudo e instigo en la transferencia, posesión y uso de números de teléfono móvil y credenciales de cuentas electrónicas de otras personas durante y en relación con el delito de asociación delictuosa de fraude electrónico del que se le acusa en el Cargo Dos de esta acusación formal.

(Secciones 1028 A (a) (1), 1028 A (b) (2) del Titulo 18 del Código de los Estados Unidos).

La pena máxima por una contravención del delito del que se le acusa en el Cargo Tres es una pena obligatoria de prisión de dos años, quo debe cumplirse de forma consecutiva después de cualquier otra pena de prisión impuesta por los otros cargos de la acusación formal; una sanción igual a la cantidad que sea mayor entre $250,000 en moneda de los Estados Unidos, el doble de la ganancia pecuniaria bruta derivada del delito o el doble de la perdida pecuniaria bruta a personas distintas del acusado que sea consecuencia del delito; libertad supervisada de un año; y una cuota especial obligatoria de $100 en moneda de los Estados Unidos.

CARGO CUATRO

(Asociación delictuosa para cometer lavado de dinero)

El gran jurado además imputa que:

18.Las alegaciones establecidas en los párrafos 1 a 6 se incorporan como referencia como si se hubieran establecido completamente aquí.

19.Alrededor de mayo de 2019, en el Distrito Sur de DIRECCION026 en otros lugares, Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, a sabiendas combinaron, se unieron en una asociación delictuosa, se confederaron y acordaron juntos y entre si contravenir las leyes de lavado de dinero de los Estados Unidos.

20.Fue una parte y un objeto de la asociación delictuosa el que Nicanor , alias " DIRECCION001 ", el acusado, y otros conocidos y desconocidos, sabiendo que los bienes implicados en ciertas transacciones financieras representaban los ingresos de cierta forma de actividad ilegal, llevaría a cabo y llevó a cabo y trato de llevar a cabo dichas transacciones financieras especificadas, que de hecho comprendían los ingresos de actividades ilegales especificadas, a saber, la intrusión informática y la estratagema de fraude electrónico cuyo objetivo era la Compafifa-1, en contravención de las secciones 1030 (a) (2) (C), 1030 (c) (2) (13) (1) y (iii), 1030 (a) (4), 1030 (c) (3) (A), 1030 (a) (5) (A), 1030 (a) (5) (13), 1030 (c) (4) (A) (i) (1), 1030 (c) (4) (B) (i) y 1343 del Título 18 del Código de los Estados Unidos, sabiendo que las transacciones fueron diseñadas en total y en parte para ocultar y camuflar la naturaleza, el lugar, el origen, la propiedad y el control de los ingresos de actividades ilegales especificadas en contravención de la sección 1956(a) (1) (B) (1) del Titulo 18 del Código de los Estados Unidos, a saber, Nicanor y sus coconspiradores hicieron que los ingresos de la intrusión informática y la estratagema de fraude electrónico contra la Compañía-1 se distribuyera entre ellos y otros coconspiradores, entre otras cosas, haciendo que las criptomonedas robadas se transfirieran por medio de docenas de transferencias y transacciones y se intercambiaran parcialmente por Bitcoin usando servicios de intercambio de criptomonedas, para ocultar la naturaleza, el lugar, la propiedad y el control de las criptomonedas robadas.

(Sección 1956(h) del Título 18 del Código de los Estados Unidos).

La pena máxima por una contravención del delito del que se le acusa en el Cargo Cuatro es de 20 años de prisión; una sanción de $500,000 en moneda de los Estados Unidos o el doble del valor de la propiedad implicada en la transacción, la que sea mayor; libertad supervisada de tres y una cuota especial obligatoria de $100 en moneda de los Estados Unidos.

ALEGACION DE DECOMISO EN CUANTO AL CARGO UNO

21. Como consecuencia de cometer el presunto delito del Cargo Uno de esta acusación formal, Nicanor , alias " DIRECCION001 ", el acusado, cederá en decomiso a favor de los Estados Unidos, según la sección 1030(i) del Título 18 del Código de los Estados Unidos todo bien, inmueble o personal, que constituya o se derive de cualquier ingreso obtenido directa o indirectamente, como consecuencia de dicho delito, y de todo bien personal usado o con la intención de ser usado para cometer o facilitar la comisión de dicho delito, incluida, entre otros, una suma de dinero en moneda de los Estados Unidos que represente la cantidad de ingresos rastreable con la comisión de dicho delito.

ALEGACION DE DECOMISO CON RESPECTO AL CARGO DOS

22. Como consecuencia de cometer el presunto delito del Cargo Dos de esta acusación formal, Nicanor , alias " DIRECCION001 ", el acusado, cederá en decomiso a favor de los Estados Unidos según la sección 981 (a) (1) (C) del Título 18 del Código de los Estados Unidos y la sección 2461 (c) del Título 28 del Código de los Estados Unidos, todo bien, inmueble o personal, que constituya o se derive de ingresos rastreables a la comisión de dicho delito, incluida, entre otros, una suma de dinero en moneda de los Estados Unidos que represente la cantidad de ingresos rastreable con la comisión de dicho delito.

ALEGACION DE DECOMISO CON RESPECTO AL CARGO CUATRO

23.Como consecuencia de cometer el presunto delito del Cargo Cuatro de esta acusación formal, Nicanor , alias " DIRECCION001 ", el acusado, cederá en decomiso a favor de los Estados Unidos según la sección 982(a) (1) del Título 18 del Código de los Estados Unidos, todo bien, inmueble o personal, involucrado en dicho delito, o de todo bien rastreable a dicho bien, incluido, entre otros, una suma de dinero en moneda de los Estados Unidos que represente la cantidad de los bienes involucrados en dicho delito.

Disposición de bienes sustitutos

24. Si cualquiera de los bienes sujetos a decomiso descritos arriba coma consecuencia de cualquier acto u omisión del acusado:

a. no puede ser localizada después del ejercicio de debida diligencia;

b. no se ha transferido ni vendido ni cedido en deposito a una tercera persona;

c. se ha puesto más allá de la jurisdicción del tribunal;

d. ha disminuido sustancialmente de valor; o

e. se ha combinado con otra propiedad, que no puede subdividirse sin dificultad;

es la intención de los Estados Unidos, según la sección 853 (p) del Título 21 del Código de los Estados Unidos y la sección 2461(c) del Título 28 del Código de los Estados Unidos, buscar el decomiso de cualquier otro bien del acusado con un valor de hasta el valor del bien sujeto a decomiso mencionado arriba. (Secciones 981, 982, 1030 del Título 18 del Código de los Estados Unidos; Sección 853 del Título 21 del Código de los Estados Unidos; y Sección 2461 del Título 28 del Código de los Estados Unidos).

SÉPTIMO. - Los hechos en que se fundamenta la ampliación de la solicitud de extradición son los siguientes:

" 6. Desde marzo de 2019 a mayo de 2019 aproximadamente, Nicanor , en colaboración con otros coconspiradores, perpetro una estratagema de intercambio de SIM, que incluía el robo de aproximadamente $784,000 en moneda de los Estados Unidos en criptomonedas pertenecientes a clientes de la compañía de la victima ("Compañía-1"), una compañía tecnológica con sede en Manhattan, Nueva York, que proporciona infraestructura de monederos y software relacionado con intercambios de criptomonedas por todo el mundo. Esta conducta forma la base de los Cargos Uno y Dos de la acusación formal. Para fomentar la estratagema delictiva, Nicanor y sus coconspiradores usaron medios de identificación de empleados de la Compañía-1 (a saber, sus números de teléfono y credenciales de conexión de la cuenta electrónica) sin autorización. Esta conducta forma la base del Cargo Tres de la acusación formal. Según se describe abajo con detalle, después de robar las criptomonedas, Nicanor y sus cómplices las lavaron por medio de decenas de transferencias y transacciones, y algunas de ellas se transfirieron a una cuenta de intercambio de criptomonedas controlado por Nicanor . Esta conducta es la base del Cargo Cuatro de la acusación formal.

A. Antecedentes

7. Una "tarjeta SIM" es un módulo de identidad de suscritor o módulo de identificación de suscritor. Un teléfono móvil requiere una tarjeta SIM para conectar el móvil a la red de teléfonos móviles. La tarjeta SIM de un móvil en particular esta vinculada generalmente al número de teléfono de este móvil. En términos generales, una estratagema de intercambio de SIM, como el de la acusación de este caso, se produce cuando un participante de la estratagema hace que una compañía telefónica cambie un numero de teléfono de la victima a una tarjeta SIM que controla el participante de la estratagema o un coconspirador. Al hacer esto, el participante de la estratagema puede recibir mensajes destinados para la victima, que el participante de la estratagema puede usar después para, entre otras cosas, reajustar contraseñas y acceder cuentas de la victima, como cuentas

de correos electrónicos y bancarias.

B. Los ataques de intercambio de SIM contra el Eiecutivo-1

8. El cofundador de la Compañía-1 y vicepresidente de desarrollo ("Ejecutivo 1") fue víctima de ataques de intercambio de SIM en marzo y finales de abril de 2019. Según se describe abajo, el ataque de intercambio de SIM contra el Ejecutivo- 1 a finales de abril de 2019 resulto en el robo con éxito de una gran cantidad de criptomonedas de la Compafifa-1.

9. Los registros de AT&T para la cuenta móvil del Ejecutivo-1 confirman que dos dispositivos maliciosos no autorizados, identificados por los números de IMEI NUM006 ("Dispositivo malicioso-1") y NUM007 ("Dispositivo malicioso-2"), estaban asociados con la cuenta del móvil del Ejecutivo-1 el 30 de abril de 2019. Según los registros de AT&T, los dispositivos maliciosos sospechosos siguieron asociados con la cuenta móvil del Ejecutivo-1 durante unas tres horas.

10. Dos coconspiradores diferentes basados en los Estados Unidos ("CC-1" y "CC-2") tenían los dispositivos maliciosos (Dispositivo malicioso-1 y Dispositivo malicioso-2) que estaban vinculados fraudulentamente con la cuenta móvil del Ejecutivo-1 como parte del ataque de intercambio de SIM. Ambos cómplices admitieron perpetrar los ataques de intercambio de SIM con Nicanor :

a. En junio de 2019, la policía de Texas ejecut6 un registro consentido en una residencia de CC-1, un menor, y recuperó el Dispositivo malicioso-1, un iPhone de color gris con IMEI NUM006 . Después de recuperar el Dispositivo malicioso-1, CC-1 participo en una entrevista video grabada con la policía. Durante la entrevista, CC-1 declaro, en sustancia y en parte, que, en abril/mayo de 2019, participo en intercambios de SIM con " DIRECCION001 ", cuyo nombre real es Nicanor , y que se pagó a CC-1 un 10% de los ingresos de cada intercambio de SIM satisfactorio, que ascendía a un total de unos $5,000.

b. En febrero de 2020, la policía de Arkansas ejecuto una orden de registro en la residencia de CC-2, entonces un menor, y recupero el Dispositivo malicioso-2, un iPhone 5 con IMEI NUM007 , del cajón de una cómoda en el dormitorio de CC-2. Después de recuperar el Dispositivo malicioso-2, CC-2 se entrevist6 con la policía. Durante la entrevista, CC-2 declaro, en esencia y en parte, que, entre aproximadamente finales de abril o principios de mayo de 2019 y junio de 2019, CC-2 participo en intercambios de SIM con " DIRECCION001 ", cuyo nombre real es Nicanor y que es del Reino Unido. CC-2 informó que fue pagado periódicamente por Nicanor por su papel en los intercambios de SIM.

11. El análisis policial del Dispositivo malicioso -2 reveló que estaba asociado con múltiples números de teléfono, incluidos el numero de teléfono del Ejecutivo-1. El 1 de mayo de 2019, el Dispositivo malicioso -2 recibió) un mensaje de texto, enviado al número de teléfono del Ejecutivo-1, indicando lo siguiente: "111999 Use este código para la verificación de la [Compañía- 1]". Se cree que este mensaje de texto fue recibido por los coconspiradores durante el ataque de intercambio de SIM contra el Ejecutivo-1.

C. Las intrusiones en los sistemas informáticos de la Compañía -1 y robo de criptomonedas.

12. Aproximadamente una hora después del ataque de intercambio de SIM de abril de 2019 delEjecutivo-1, varias cuentas de la Suite G en la Comparifa-1, incluida la cuenta del administrador, estuvieron sujetas a un acceso no autorizado. Los registros del protocolo de Internet ("IP") para las cuentas de la Suite G de la Compafifa-1 reflejan esa dirección de IP3 NUM008 (la Dirección de IP maliciosa") fue utilizada para conectarse con la cuenta G Suite del Ejecutivo-1, la cuenta G Suite del administrador, y la cuenta G Suite de otro empleado de la Comparifa-1 el 30 de abril y 1 de mayo de 2019 como parte del ataque.

13. Los registros de la Compañía-1 y los registros de IP reflejan que, durante aproximadamente los tres días siguientes, múltiples servidores de la Compañía-1 y su entorno Microsoft Azure estaban sujetos a un acceso no autorizado. Como parte del ataque, los miembros de la asociación delictuosa cambiaron las contraseñas, y usaron las credenciales de conexión de la cuenta de los empleados sin autorización para conectarse a las cuentas de G Suite usadas por varios empleados de la Compañía-1, incluidos los empleados de la Oficina de

Manhattan de la Compañía- 1. Según los registros IP, al menos un empleado trató de acceder a su cuenta de correo electrónico y corporativa de G Suite de la oficina de Manhattan de la Compafila-1 durante la intrusión y no pudo hacerlo.

14. Los registros de la Compañia-1 también reflejan que, el 1 de mayo de 2019, se robaron criptomonedas de varios tipos, que pertenecían a clientes de la Compañía-1, y se retiraron de monederos de criptomonedas de los servidores comprometidos. Se robo un total de aproximadamente $784,000 en moneda de los Estados Unidos en criptomonedas mediante el ataque de la forma siguiente (la "Criptomoneda robada"):

Tipo de moneda Cantidad Hora Cliente Equival. en dolares

Bitcoin Cash 770.784869 1/MAY/19 01:17:00 1 $209,512,04

Litecoin 6363.490509 1/MAY/19 01:18:39 1 $468.720.51

Ethereum 407.396074 1/MAY/19 01:19:36 2 $65,516.76

Bitcoin 7.456728 1/MAY/19 01:23:18 1 $40,286.44

D. Otros ataques de intercambio de SIM que tenían como objetivo a ejecutivos de la Compañía-1

15. El 3 de mayo de 2019, aproximadamente dos días después el robo, otros dos ejecutivos de la Compañía-1 ("Ejecutivo-2" y "Ejecutivo-3") fueron víctimas de ataques de intercambio de SIM. El 4 de mayo de 2019, después de estos ataques, uno de los miembros de la asociación delictuosa tuvo acceso a la cuenta de Skype del Ejecutivo-2 sin autorización y la usó para iniciar una conversación grupal en línea con empleados de la Compañía-1, que continuó durante unas dos horas. Durante esta conversación por Skype, el atacante consultó el ataque de intercambio de SIM con el Ejecutivo-1, el acceso no autorizado a los sistemas informáticos de la Compañía-1 y el robo de criptomonedas de los monederos de la Compalifa-1. Los mensajes del atacante incluían lo siguiente, entre otras cosas:

- 4 RIP 800k

- También accedimos / a su azure / porque a alguien le gusta tenor las contraseñas guardadas

- Puedes dar al [Ejecutivo-1] una palmadita en el hombro por esto

- Si no fuera por 61 no tendría 16 años ni tendría 800k rn

- Ser hackeado por un grupo de jóvenes, no está bien visto en el historial

- Te lo dije . . . Intercambié sim [Ejecutivo-1] / reajusté su correo electrónico / obtuve las conexiones

16. Durante la conversación de Skype, el atacante también hizo ciertas preguntas sobre la infraestructura informática de la Compañía-1 y las propias posesiones de criptomonedas de los empleados de la Compañía-1. Los mensajes del atacante de la cuenta Skype del Ejecutivo-2 fueron recibidos en tiempo real por al menos un empleado de la oficina de Manhattan de la Compañía-1.

E. Lavado de los ingresos delictivos.

16. Después de robar las criptomonedas de la Compañí-1, los miembros de la asociación delictuosa las lavaron por media de decenas de transferencias y transacciones, y algunas de ellas fueron intercambiadas por Bitcoin ("BTC") usando servicias de intercambio de criptomonedas. Según se describe con mas detalle mas abajo parte de las criptomonedas robadas se pueden identificar con una cuenta de criptomonedas controlada por Nicanor .

17. Según el análisis de las cadenas de bloques de criptomonedas relevantes (que son libros mayores públicos descentralizados que registran todas las transacciones de una criptomoneda en particular), el FBI identifico las criptomonedas robadas en parte de la forma siguiente:

a. Aproximadamente 7.46 BTC de las criptomonedas robadas, valoradas en aproximadamente $40,286,44 en moneda de los Estados Unidos y mantenidas en nombre del Cliente-1, fueron depositadas directamente en una dirección de Bitcoin particular (la "Dirección de BTC robada") el 1 de mayo de 2019 a las 5:23 AM UTC.

b. Aproximadamente 770.78 Bitcoin Cash (BCH) de las criptomonedas robadas, valoradas en aproximadamente $209,512.04 en moneda de los Estados Unidos y mantenidas en nombre del Cliente-1, fueron robadas de monederos de la Compañía- 1 el 1 de mayo de 2019 a las 1:17 AM UTC. Estas BCH fueron depositadas sistemáticamente usando una cadena de pelados de 44 transacciones a un servicio de intercambio de criptomonedas, Switchain. Los registros recibidos de Switchain muestran que las BCH transferidas mediante 42 de estas transacciones (aproximadamente 748.65 BCH) fueron intercambiadas por BTC y depositadas en la dirección de las BTC robadas unas dos horas después del robo como máximo. Al final, al menos

aproximadamente $243,000 en moneda de los Estados Unidos de Bitcoin identificables directamente con las criptomonedas robadas ("BTC robadas") fueron depositadas en la dirección de BTC robadas.

Después de ser transferidas a la dirección de BTC robadas, las BTC robadas se transfirieron a través de dos cadenas de pelado y pudieron identificarse en parte al menos seis direcciones de Bitcoin ("Grupo de direcciones de arc-1"). La primera cadena de pelado se inicio el 1 de mayo de 2019 a las 6:01 AM UTC con una retirada de aproximadamente 7.46 BTC de la dirección de BTC robadas. La segunda cadena de pelado fue iniciada el 1 de mayo de 2019 a las 8:02 AM UTC con la retirada de aproximadamente 36.92 BTC de la dirección de BTC robadas.6 Debido a estas técnicas de lavado, solo una fracción de las BTC robadas podría identificarse definitivamente con el Grupo de direcciones de BTC-1.

F. Las tres cuentas de Binance.

18. Segall se describe con más detalle abajo, las autoridades de los Estados Unidos determinaron que Nicanor controlaba tres cuentas de intercambio de criptomonedas Binance, que estaban estrechamente conectadas a la estratagema delictiva contra la Compañía-1, una de las cuales recibió una parte de las criptomonedas robadas lavadas. Las tres cuentas de Binance son: (1) la cuenta de Binance registrada en la dirección de correo electrónico DIRECCION027 (la "cuenta DIRECCION028 "); (2) la cuenta Binance registrada en la dirección de correo electrónico DIRECCION029 (la cuenta " DIRECCION030 "); y (3) la cuenta Binance registrada en la dirección de correo electrónico DIRECCION031 (la cuenta " DIRECCION032 ").

19. Binance proporcionó información de dispositivos detallada para los dispositivos electrónicos que se usaron para acceder a las tres cuentas de Binance. La información de los dispositivos consistía en 20 campos separados que describen atributos diferentes del dispositivo electrónico en particular. Según la información del dispositivo, las tres cuentas de Binance estaban sometidas a un control común. En particular, el mismo dispositivo electrónico (con los 20 campos coincidentes) se usó para acceder a la cuenta DIRECCION028 y la cuenta DIRECCION032 entre el 3 de mayo de 2019 y el 4 de mayo de 2019. Además, el mismo (segundo) dispositivo electrónico (nuevamente, con los 20 ampos coincidentes) se uso para acceder a la cuenta DIRECCION032 y a la cuenta DIRECCION030 el 12 de junio de 2019.

20. Las cuentas de Binance están estrechamente relacionadas con el Grupo de direcciones de BTC-1, que, según se describe arriba, recibieron una parte de las criptomonedas robadas lavadas como parte de la estratagema delictiva, En particular, según los registros de Binance:

a. El 30 de abril de 2019, la cuenta DIRECCION028 envió aproximadamente 2 BTC a una dirección en el Grupo de direcciones de BTC-1, Al día siguiente, el 1 de mayo de 2019, esta dirección del Grupo de direcciones de BTC-1 recibio fondos identificables con las BTC robadas.

b. El 3 de mayo de 2019, la cuenta DIRECCION032 recibió un depósito (el único) de aproximadamente 35 BTC, de los que aproximadamente 31 BTC llegaron del Grupo de direcciones BTC-1. El depósito constaba de BTC de cinco direcciones del Grupo de direcciones BTC-1, todas las cuales habían recibido fondos el 1 de mayo de 2019 identificable a las BTC robadas, Notablemente, algunas de las BTC en el depósito de la cuenta DIRECCION032 eran directamente identificables con las BTC robadas.

Las cuentas de Binance también estaban estrechamente ligadas a la estratagema delictiva mediante pruebas de la dirección IP. según se describe arriba, la Dirección IP maliciosa se usó para conectarse con la cuenta de G Suite del administrador y la cuenta de G Suite de otro empleado de la Compañía-1 el 30 de abril de 2019 y el 1 de mayo de 2019 con o parte de la intrusión cibernética en la Compañía-1. Según los registros proporcionados por Binance, en el mismo día, aproximadamente tres horas antes de que se usaran para acceder a las cuentas G Suite de la Compañía-1, la Dirección maliciosa IP se usaba para acceder a la cuenta DIRECCION028 . Además, la Dirección maliciosa IP también se usaba para tener acceso a cuentas relevantes a la investigación días y semanas después de las intrusiones cibernéticas según la investigación, incluidas las siguientes:

a. El 11, 16 y 18 de mayo de 2019: la Dirección de IP maliciosa se usó para acceder a la cuenta DIRECCION028 y a la cuenta DIRECCION032 en cada uno de esos días.

b. El 6 de junio de 2019: la Dirección de IP maliciosa se usó para acceder a la cuenta DIRECCION032 y a la cuenta DIRECCION030 .

21. Por último, hay otras conexiones de IP entre las tres cuentas de Binance. Por ejemplo, la dirección de IP NUM009 se usó para acceder a la cuenta DIRECCION028 y la cuenta DIRECCION032 en coda uno de los días 10 de mayo de 2019 y 17 de mayo de 2019, indicando además que estas cuentas están controladas por el mismo individuo.

G. Nicanor

22. Nicanor controla una cuenta en el intercambio de criptomonedas Coinbase (la "cuenta Coinbase de Nicanor "). Según los registros de Coinbase, la cuenta de Coinbase de Nicanor se registró el 11 de julo de 2017, bajo el nombre de Rubén y la dirección de correo electrónico DIRECCION033 . La información de registro asociada con la cuenta de Coinbase Nicanor incluía la información para pasaportes del RU a nombre de Nicanor , así como la imagen de debajo del carné de conducir de Nicanor .

23. Las autoridades de los Estados Unidos han obtenido una orden de registro judicial de la cuenta de correo electrónico DIRECCION033 , que se usó para registrar la cuenta Coinbase de Nicanor . El contenido de la cuenta de correo electrónico confirme además que está controlada por Nicanor . Entre otras cosas, la cuenta de correo electrónico contenía un formulario del Servicio de Rentas Internas (Internal Revenue Service) de los Estados Unidos a nombre de Nicanor ; una fotografía del carné de conducir de Nicanor (la misma que arriba); una fotografía de un pasaporte del RU a nombre de Nicanor (fecha de nacimiento del NUM000 de 1999); una declaración de cuenta financiera dirigida a " DIRECCION034 "; una factura de 2018 dirigida a " Rubén " por la compra de un monedero de hardware de criptomonedas Trezor Model T (compatible con mas de 1200 tipos de monedas); y un informe de julio de 2019 del Centro Medico "Triay Medical Centre" en España que citaba a Nicanor cam° el paciente.

24. La cuenta de Coinbase de Nicanor participo en transacciones de criptomonedas con una de las tres cuentas de Binance tratadas arriba. En particular, el 15 de noviembre de 2018, la cuenta DIRECCION028 recibió un depósito de unos 0.04 BTC (con un valor aproximado de $226 en moneda de los Estados Unidos) de la cuenta de Coinbase de Nicanor . Además, el 6 de abril de 2019, la cuenta DIRECCION028 recibió un depósito de aproximadamente 9 BTC (con un valor aproximado de $45,538 en moneda de los Estados Unidos) de la cuenta de Coinbase de Nicanor .

25. Además, hay conexiones de IP entre la cuenta de Coinbase de Nicanor y las tres cuentas Binance según se indica a continuación:

a. La dirección de IP NUM010 se usó para conectarse con la cuenta DIRECCION028 el 6 de abril de 2019, a las 19:04 UTC. Aproximadamente siete minutos después, se usó la misma dirección IP para conectarse con la cuenta de Coinbase de Nicanor . Según se describió arriba, este es el mismo día en el que se enviaron aproximadamente 9 BTC de la cuenta de Coinbase de Nicanor a la cuenta de DIRECCION028 .

b. La dirección IP NUM011 se usó para conectarse con la cuenta de Coinbase de Nicanor y las tres cuentas de Binance en las fechas siguientes:

· *Cuenta de Coinbase de Nicanor : 6 de abril de 2019*

· *Cuenta DIRECCION028 : 7 de diciembre de 2018,24 de diciembre de 2018 y 28 de febrero de 2019*

· cuenta DIRECCION032 : 16 de junio de 2019

· cuenta DIRECCION030 : 16 de junio de 2019

Según lo anterior, Nicanor controla las tres cuentas de Binance, incluida la cuenta que recibió los ingresos de la estratagema delictiva contra la Compañía-1. Según se describe arriba, la Dirección maliciosa IP, que se usaba para obtener un acceso no autorizado a las cuentas de la Compañía-1 durante el ataque, también se usó para tener acceso a una de las cuentas de Binance aproximadamente tres horas antes (y se usó para tener acceso a las tres cuentas de Binance otros días), implicando aún más a Nicanor en la estratagema delictiva.

OCTAVO. - Celebrada por el Juzgado Central de Instrucción nº 5 la comparecencia prevista en el artículo 12 de la Ley de Extradición Pasiva en fecha de 19 de enero de 2022, el reclamado manifestó que no consentía a la entrega a las autoridades reclamantes y que no renunciaba al principio de especialidad extradicional.

Mediante resolución de fecha 19 de enero de 2022, se acordó elevar el procedimiento de extradición a la Sección Segunda de la Sala de lo Penal de la Audiencia Nacional.

En fecha 10 de marzo de 2022 tuvo lugar la correspondiente vista, en la que la defensa del reclamado interesó al Tribunal el planteamiento de una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea, habiéndose acordado, mediante auto de fecha 28 de marzo de 2022, con suspensión de la tramitación del presente procedimiento, el planteamiento de la cuestión prejudicial en los siguientes términos:

1ª. - ¿Deben los artículos 126 y 127 del Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica [Acuerdo de retirada] y los artículos 18.1 y 21.1 del Tratado de Funcionamiento de la Unión Europea interpretarse en el sentido de que se aplican a una solicitud de extradición de un tercer estado cursada con posterioridad a la finalización del periodo transitorio previsto en el Acuerdo de retirada sobre un ciudadano del Reino Unido que era residente en

un Estado Miembro durante y después del fin del Acuerdo de retirada por hechos cometidos antes y durante la vigencia del Acuerdo de retirada?

En caso negativo,

2ª. - ¿Deben interpretarse los artículos 10, 12, 13, 14, 15, 126 y 127 del Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica [Acuerdo de retirada] y el artículo 21 del Tratado de Funcionamiento de la Unión Europea en el sentido de que es de aplicación la doctrina de las Sentencias del TJUE en los asuntos C-182/15 (Petruhhin), Pisciotti (C-191/16) y C-897/19 PPU (I.N.)a una solicitud de extradición de un tercer país relativa a un nacional británico que era ciudadano de la Unión Europea en el momento de los hechos que motivan la solicitud de extradición y que ha residido ininterrumpidamente en el territorio de otro Estado Miembro antes y durante la vigencia del Acuerdo de retirada?

En caso negativo,

3ª.- ¿Es aplicable la doctrina de las Sentencias del TJUE en los asuntos C-182/15 (Petruhhin), Pisciotti (C-191/16) y C-897/19 PPU (I.N.)a la vista del mecanismo de cooperación judicial en materia penal previsto en los arts. 62 a 65 del Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica y el Título VII de la Tercera Parte del Acuerdo de Comercio y Cooperación entre la Unión Europea y la Comunidad Europea de la Energía Atómica, por una parte, y el Reino Unido de Gran Bretaña e Irlanda del Norte, por otra a una solicitud de extradición de un tercer país relativa a un nacional británico que era ciudadano de la Unión Europea en el momento de los hechos que motivan la solicitud de extradición y que ha residido ininterrumpidamente en el territorio de otro Estado Miembro antes y durante la vigencia del Acuerdo de retirada?

En la citada resolución se solicitaba se aplicase a la cuestión prejudicial planteada el procedimiento de urgencia previsto en el artículo 107 del Reglamento de Procedimiento, en relación con el artículo 23 bis del Estatuto del TJUE, no habiéndose aceptado dicha solicitud, estado al día de la fecha pendiente de resolución, por lo que, mediante providencia de fecha 10 de enero de 2023, y a la vista del tiempo transcurrido desde la iniciación del procedimiento, y dada la situación de prisión provisional en que se encuentra el reclamado, se alzó la suspensión que venía acordada, señalándose el día 16 de enero del presente para la celebración de nueva vista, dado el tiempo transcurrido desde la anterior.

NOVENO. - En el acto de la vista, el Ministerio Fiscal reiteró su informe en el sentido de que procedía acceder, en esta vía jurisdiccional a la extradición de Nicanor a los Estado Unidos de América.

La defensa de Nicanor interesó, nuevamente, se ofreciese a las autoridades del Reino Unido de Gran Bretaña, de donde es nacional su defendido, la posibilidad de su enjuiciamiento por las mismas, en aplicación de la conocida como doctrina Petruhhin

DÉCIMO. - Mediante resolución de fecha 18 de enero de 2023 se acordó, con suspensión del plazo para dictar la resolución que proceda, remitir comunicación a las autoridades del Reino Unido de Gran Bretaña e Irlanda del Norte, a través del Magistrado de enlace del mismo en España, a fin de que en el improrrogable plazo de quince días comunicasen si es de su interés remitir a España solicitud de extradición sobre Nicanor a fin de su enjuiciamiento por los hechos que motivan la solicitud de extradición formulada por los Estado Unidos de América.

UNDÉCIMO. - En fecha 7 de febrero del actual se recibe comunicación de la Nacional Crime Agenci, Interpol Manchester, Reino Unido, por la que se comunica que la Autoridad Central del Reino Unido del Ministerio del Interior ha resuelto que en el presente caso no es de aplicación el mecanismo Petruhhin.

DÉCIMO. - Quedando el procedimiento concluso para el dictado de la presente resolución, la cual una vez deliberada, el Ilmo. Sr. Magistrado D. Fernando Andreu Merelles, ponente de la misma, expresa el parecer de la Sala.

RAZONAMIENTOS JURIDICOS.

PRIMERO. - El procedimiento de extradición entre el Reino de España y los Estado Unidos de América se encuentra regulado:

a) Tratado de extradición entre España y los EE. UU. de 29 de mayo de 1970, que entró en vigor el 16 de junio de 1971.

b) Primer Tratado suplementario de extradición entre España y los EE. UU., de 25 de enero de 1975.

c) Segundo Tratado suplementario de extradición entre España y los EE. UU. de19 de febrero de 1988.

d) Tercer Tratado suplementario de extradición entre España y los EE. UU., de 12 de marzo de 1996.

e) Acuerdo de extradición entre los EE. UU. y la UNION EUROPEA de 25 de junio de 2003 (en vigor desde el 1 de febrero de 2010, según Decisión 2009/933, de 30 de noviembre, del Consejo y Decisión 2009/820, de 23 de octubre, del Consejo).

f) Instrumento previsto en el art 3 del Acuerdo de Extradición entre la Unión Europea y los Estados Unidos de América de 25 de Junio de 2003, para la aplicación del Tratado de Extradición entre España y EE. UU. de 29 de mayo de 1979 y Tratado Suplementario de Extradición de 25 de enero de 1975, 9 de febrero de 1988 y 12 de marzo de 1996, hecho ad-referéndum en Madrid el 17 de diciembre de 2004, de fecha 18 de enero de 2010 (BOE de 26 de enero de 2010).

g) Con carácter supletorio, por la ley de extradición pasiva de 21 de marzo de 1985.

SEGUNDO. - No existe debate acerca de la identidad de la persona objeto de reclamación extradicional, tratándose de D. Nicanor , nacido en DIRECCION024 , Inglaterra, el día NUM000 de 1.99, con pasaporte del Reino Unido nº NUM001 .

TERCERO. - Se cumplen los presupuestos documentales a que se refiere el artículo X del citado Instrumento pata la aplicación del Tratado de Extradición entre España y los EE.UU., al haberse acompañado a la solicitud de extradición:

1. Una descripción de la persona reclamada;

2. Una declaración sobre los hechos relativos al caso;

3. Los textos legales de la Parte Requirente que sean aplicables incluyendo los preceptos que establecen el delito y la pena;

4. Una declaración de que la acción penal o la pena no han prescrito según la legislación de la Parte Requirente.

CUARTO. - Concurren los principios de doble incriminación y mínimo punitivo exigidos en el artículo II del citado Instrumento, y así los hechos serían constitutivos, conforme a la legislación del Estado requirente, de los delitos de:

- Cargos uno, tres y cinco: Conspiración para cometer un delito contra los Estados Unidos, es decir, accesar una computadora sin autorización y así obtener información de una computadora protegida, en infracción de la sección 1030(a)(2) (C) del Título 18 del Código de los Estados Unidos, todo en infracción de la Sección 371 del Título 18 del Código de los Estados Unidos.

Penas: Cinco años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

- Cargos dos y cuatro: Intrusión en computadora, es decir, accesar intencionalmente una computadora sin autorización y así obtener información de una computadora protegida, en infracción de la sección 1030(a)(2) (C) del Título 18 del Código de los Estados Unidos, y ayudar e instigar, en infracción de la sección 2 del Título 18 del Código de los Estados Unidos

Penas: Cinco años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

- Cargo seis: Conspiración para cometer un delito contra los Estados Unidos, es decir, accesar intencionalmente una computadora sin autorización y con la intención de extorsionar a una persona para obtener algo de valor, y transmitir una comunicación que contiene una amenaza para que se revele información confidencial, o transmitir una comunicación que contiene una demanda o solicitud de algo de valor en relación con daño a una computadora protegida cuando ese daño ha sido causado para facilitar la extorsión, en infracción de la sección 1030(a)(7) del Título 18 del Código de los Estados Unidos, todo en infracción de la sección 371 del Título 18 del Código de los Estados Unidos

Penas: Cinco años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso

- Cargo siete: Comunicaciones extorsivas, es decir, transmitir a sabiendas en el comercio interestatal y extranjero, con intención de extorsionar a una persona para obtener algo de valor, una comunicación que

contenía una amenaza de daño a la reputación de otra persona, en infracción de la sección 875(d) del Título 18 del Código de los Estados Unidos.

Penas: Dos años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

- Cargos ocho y diez: acoso, es decir, con intención de hacer daño, hostigar y causar una angustia emocional significativa a una persona en otro estado, usando instalaciones de comercio interestatal y extranjero, entre ellos un servicio interactivo de computadora y un servicio de comunicación electrónica, para participar en una conducta que causa una angustia emocional significativa a la víctima y la coloca en un estado de temor razonable de muerte o grave lesión corporal, en infracción de la sección 2261A(2) del Título 18 del Código de los Estados Unidos.

Penas: Cinco años de prisión, tres años de libertad supervisada; una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

- Cargo nueve: Comunicaciones amenazantes, es decir, enviar a sabiendas un mensaje en el comercio interestatal y extranjero que contenía una verdadera amenaza de hacer daño a otra persona, en infracción de la sección 875(c) del Título 18 del Código de los Estados Unidos.

Penas: Cinco años de prisión, tres años de libertad supervisada: una multa de $250,000 en moneda de los Estados Unidos; una cuota especial por cargo de $100 en moneda de los Estados Unidos; restitución; decomiso.

Tales hechos están tipificados en nuestro Código Penal en los artículos 197 y 197 bis, que castigan el delito de descubrimiento y revelación de secretos, en el artículo 570 bis, que castiga la pertenencia o integración a organización criminal y en el artículo 243 del mismo texto legal, que castiga el delito de extorsión.

Y con respecto de la extradición acumulada:

- Cargo Uno: Asociación delictuosa para cometer intrusiones informáticas, en contravención de las secciones 1030 (a) (2) (c), 1030 (c) (2) (B) (i) y (iii), 1030 (a) (4), 1030 (c) (3) (A), 1030 (a) (5) (A), 1030 (a) (5) (B), 1030 (c) (4) (A) (i) (I) y 1030 (c) (4) (13) (i) del Título 18 del Código de los Estados Unidos.

La pena máxima por una contravención del delito del que se le acusa en el Cargo Uno es una pena de prisión de 5 años; una sanción de la cantidad que sea mayor entre $250,000 en moneda de los Estados Unidos, el doble de la ganancia pecuniaria bruta derivada del delito o el doble de la perdida pecuniaria bruta a personas que no sean el acusado consecuencia del delito; libertad supervisada de tres años; restitución; y una evaluación especial obligatoria de $100 en moneda de los Estados Unidos.

- Cargo Dos: Asociación delictuosa para cometer fraude electrónico, en contravención con (Sección 1349 del Título 18 del Código de los Estados Unidos).

La pena máxima por una contravención del delito del que se le acusa en el Cargo Dos es prisión por 2 dos; una sanción igual a la cantidad que sea mayor entre $250,000 en moneda de los Estados Unidos, el doble de la ganancia pecuniaria bruta derivada del delito o el doble de la perdida pecuniaria bruta a personas distintas del acusado que sea consecuencia del delito; libertad supervisada de tres años; y una cuota especial obligatoria de $100 en moneda de los Estados Unidos.

- Cargo Tres: Robo de identidad con agravante, en contravención con las Secciones 1028 A (a) (1), 1028 A (b) (2) del Título 18 del Código de los Estados Unidos.

La pena máxima por una contravención del delito del que se le acusa en el Cargo Tres es una pena obligatoria de prisión de dos años, quo debe cumplirse de forma consecutiva después de cualquier otra pena de prisión impuesta por los otros cargos de la acusación formal; una sanción igual a la cantidad que sea mayor entre $250,000 en moneda de los Estados Unidos, el doble de la ganancia pecuniaria bruta derivada del delito o el doble de la perdida pecuniaria bruta a personas distintas del acusado que sea consecuencia del delito; libertad supervisada de un año; y una cuota especial obligatoria de $100 en moneda de los Estados Unidos.

- Cargo Cuatro: Asociación delictuosa para cometer lavado de dinero, en contravención de las secciones 1030 (a) (2) (C), 1030 (c) (2) (13) (1) y (iii), 1030 (a) (4), 1030 (c) (3) (A), 1030 (a) (5) (A), 1030 (a) (5) (13), 1030 (c) (4) (A) (i) (1), 1030 (c) (4) (B) (i) y 1343 del Título 18 del Código de los Estados Unidos, sabiendo que las transacciones fueron diseñadas en total y en parte para ocultar y camuflar la naturaleza, el lugar, el origen, la propiedad y el control de los ingresos de actividades ilegales especificadas en contravención de la sección 1956(a) (1) (B) (1) del Título 18 del Código de los Estados Unidos.

La pena máxima por una contravención del delito del que se le acusa en el Cargo Cuatro es de 20 años de prisión; una sanción de $500,000 en moneda de los Estados Unidos o el doble del valor de la propiedad implicada en la transacción, la que sea mayor; libertad supervisada de tres y una cuota especial obligatoria de $100 en moneda de los Estados Unidos.

Tales hechos serían constitutivos, conforme a nuestro Código Penal, de los delitos de acceso ilícito a sistemas informáticos, de estafa informática, de blanqueo de capitales y de pertenencia a organización criminal, previstos y penados en los arts. 197 y 197 bis, 248.2, 250.1.5, 301, 302 y 570 bis del Código Penal.

QUINTO. - En el presente procedimiento, y dado que este Tribunal accedió a la petición formulada por la defensa del reclamado en la celebración de vista de fecha 13 de marzo de 2021, en el sentido de plantear una cuestión prejudicial al TJUE, en los términos expresados en los antecedentes de esta resolución, la vista contemplada en el artículo 14 de la LEP tuvo su continuación en la celebrada en fecha 16 de enero de 2023, dada la falta de contestación del TJUE respecto de la cuestión prejudicial planteada, y la necesidad de dar respuesta a la solicitud de extradición instada por los Estados Unidos, dada la situación de prisión provisional en la que se encuentra el reclamado, situación que como es sabido tiene un carácter excepcional y exige que los procedimientos en los que se acuerde dicha medida cautelar se tramiten con la urgencia que dicha situación requiere. Ello no ha supuesto, en absoluto, merma alguna en los derechos del reclamado, y ello por cuanto, y atendiendo a la solicitud formulada por su defensa, este Tribunal acordó dirigirse a las autoridades del Reino Unido, nacionalidad del reclamado, a fin de que nos informasen si era de su interés instar la extradición de su nacional, en aplicación de la doctrina Petruhhin, habiendo sido dicha respuesta negativa, lo que supone que, para el caso que nos ocupa, sea irrelevante la respuesta que pueda ofrecer el TJUE a la cuestión prejudicial planteada que, sin duda, podrá tener relevancia y despejar las dudas habidas para futuros supuestos.

Esta circunstancia nos hace que debamos rechazar las alegaciones de indefensión se que denunciaron por la defensa del reclamado en el acto de la vista, alegando no haber podido entrevistarse con su defendido, y no haber podido tener acceso al procedimiento digitalizado, sino tan solo mediante copias, y a no haber tenido tiempo suficiente para preparar la defensa, y ello por cuanto desde que se denunciaren tales carencias hasta la continuación del acto de la vista, que tuvo lugar en fecha 16 de enero de 2023, la defensa ha tenido casi diez meses para poder tener acceso a todo el expediente, como así ha sido, y a entrevistarse con su defendido, y preparar con tiempo y detenidamente la continuación de la vista, en la que se ofreció a la defensa que realizase cuantas alegaciones tuviere por conveniente en defensa de los intereses de su cliente, y así lo hizo.

SEXTO. - Habiéndose no solo accedido por esta Sala al planteamiento de la cuestión prejudicial, sino que, y ante la tardanza en su resolución, se accedió a al Reino Unido la posibilidad de reclamar a su nacional, a lo que se ha renunciado, las alegaciones efectuadas por la defensa del reclamado han quedado plenamente satisfechas y avocan a que esta Sala se pronuncia sobre el fondo del asunto, lo que en esta resolución se hace.

SÉPTIMO. - La defensa del reclamado entiende que la competencia para el enjuiciamiento de los hechos corresponde a la jurisdicción española y no a la del Estado requirente, pues a su juicio la jurisdicción competente seria aquella en donde se encontrasen, físicamente, los servidores informáticos a través de los cuales se habrían cometido los hechos objeto de la reclamación.

Al respecto, debemos recordar que, conforme al principio de ubicuidad, consagrado por Acuerdo del Tribunal Supremo de 3 de febrero de 2005, cuando la acción y el resultado del delito no tengan lugar dentro de una misma jurisdicción, el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo, y así la Sentencia 456/2013, dispone que " *el delito se reputará cometido tanto en todos los lugares en los que se haya llevado a cabo la acción como en el que se haya producido el resultado*", y en el presente caso, no cae duda que los efectos del delito se han producido en los Estados Unidos, sin perjuicio de que sus autores se encontrasen fuera de dicho país, sin que conste, por otra parte, que el delito se hubiere cometido, ni siquiera en parte, en España.

A todo ello debemos añadir no solo que en España no se haya incoado proceso penal alguno por los hechos objeto del presente procedimiento de extradición, sino que es los Estados Unidos quien, sin duda, se encuentra en mejor situación para conocer de los mismos, dado que el mismo se enmarca en un procedimiento mucho más amplio que comprende las actividades delictivas de una organización criminal de la que se acusa pertenecer al reclamado, encontrarse en Estados Unidos las pruebas obtenidas durante la investigación, así como en donde se han ocasionado los perjuicios derivados de los hechos objeto de enjuiciamiento.

OCTAVO. - Se alegó, en el acto de la vista , y como motivo de denegación a ala entrega, la desproporcionalidad de las penas que pudieran imponerse al reclamado, que, caso de ser condenado por todos los delitos por los que es reclamado, supondría, de facto, la imposición de una condena de por vida.

Al respecto hemos de constatar que la diferencia de penalidad existente entre los tipos por los que es reclamado en los Estados Unidos y los contemplados en nuestra legislación penal, salvo en el caso de organización criminal para la comisión del delitos de blanqueo de dinero no en ni mucho menos distante, pues las penas contempladas en una y otra legislación son prácticamente similares; debiéndose reiterar que al Tribunal de extradición le corresponde comprobar la concurrencia de los principios extradicionales de doble incriminación y mínimo punitivo, pero no le corresponde hacer una crítica sobre la penalidad que atribuye el Estado reclamante al tipo delictivo aplicable a la conducta supuestamente protagonizada por el reclamado, pues ningún precepto legal o convencional lo impone. Por otro lado, la tesis de exasperación de penas esgrimida por la defensa del reclamado está sujeta a modulaciones, que han sido silenciadas por dicha defensa. Tales modulaciones, relacionadas con la continuidad delictiva de las concretas acciones ejecutadas y la concurr4encia de otras circunstancias que pudieran modular las penas a imponer definitivamente, deberán ser instadas y luego decididas, en su caso, en el pertinente juicio oral, en plenitud alegatoria y probatoria. Pues reiteramos que no corresponde al Tribunal de la extradición hacer declaraciones sobre la culpabilidad o inocencia del reclamado, ni acerca de la específica penalidad a que debe ser condenado, en la fase procesal en que sus acciones sean enjuiciadas.

NOVENO. - Por último, la defensa de Nicanor invocó el auto de esta misma Sección, núm. 26/2008, de 1 de agosto, a fin de interesar que, en caso de acordar la entrega extradicional de su defendido, se condicione dicha entrega a que el cumplimiento de la pena se debe realizar en el Reino Unido, de donde es nacional el reclamado, por cuanto carece del más mínimo arraigo en los Estados Unidos.

Dicha alegación debe ser igualmente rechazada, y ello por cuanto en el supuesto examinado en el auto al que se refiere la de defensa de Nicanor , el reclamado ostentaba la nacionalidad española, condición que no concurre en el caso que nos ocupa, debiéndose plantear dicha posibilidad en el marco de los convenios que sobre dicho particular pudieran haber suscrito los Estados Unidos y el Reino Unido.

En atención a lo expuesto, y vistos los artículos citados y demás de general y pertinente aplicación.

P A R T E D I S P O S I T I V A.

LA SALA ACUERDA. - DECLARAR PROCEDENTE en esta fase jurisdiccional, LA EXTRADICIÓN de Nicanor solicitada por las autoridades de los **ESTADOS UNIDOS DE AMÉRICA**, para su enjuiciamiento por los hechos por los que es acusado en el Caso núm. 3:21-mj-70812 MAG del Tribunal de Distrito de Estados Unidos para el Distrito Norte de DIRECCION035 el Caso núm. 21 Cr. 536 del Tribunal de Distrito de los Estados Unidos para el Distrito Sur de Nueva York.

Notifique se la presente resolución al Ministerio Fiscal y partes, haciéndoles saber que no es firme, pues contra la misma cabe interponer recurso de súplica ante el Pleno de la Sala de lo Penal de esta Audiencia Nacional, en el plazo de tres días siguientes a la fecha de la notificación.

Firme que sea esta resolución, remítase testimonio al Ministerio de Justicia (Subdirección de Cooperación Jurídica Internacional), al Ministerio del Interior (Dirección General de la Policía y Servicio de Interpol).

Así, por este nuestro Auto, lo dictamos, mandamos y firmamos.

DILIGENCIA. - Seguidamente se cumple lo acordado. Doy fe.