Roj: **SAN 2639/2016** - ECLI: **ES:AN:2016:2639**

Id Cendoj: **28079220042016100026**
Órgano: **Audiencia Nacional. Sala de lo Penal**
Sede: **Madrid**
Sección: **4**
Fecha: **04/07/2016**
Nº de Recurso: **2/2016**
Nº de Resolución: **28/2016**
Procedimiento: **PENAL - PROCEDIMIENTO ABREVIADO/SUMARIO**
Ponente: **CARMEN PALOMA GONZALEZ PASTOR**
Tipo de Resolución: **Sentencia**

AUDIENCIA NACIONAL SALA DE LO PENAL SECCIÓN CUARTA ROLLO 2/16

PROCEDIMIENTO ABREVIADO 70/2012 JUZGADO CENTRAL DE INSTRUCCIÓN Nº3

ILMOS SRES:

Dª TERESA PALACIOS CRIADO

Dª CARMEN PALOMA GONZALEZ PASTOR

D. JUAN FRANCISCO MARTEL RIVERO

SENTENCIA 28/16

En Madrid, a cuatro de julio de dos mil dieciséis.

VISTAS por la Sección Cuarta de la Sala de lo Penal de la Audiencia Nacional, en juicio oral y público, las presentes actuaciones registradas en esta Sala con el número de Rollo 2/2016, previa su incoación por el Juzgado Central de Instrucción nº 3, por los tramites deL Procedimiento Abreviado con el número 70/2012, con respecto a:

Purificacion , con NIE NUM000 , nacida en Georgia el NUM001 /1976, hija de Carlos Antonio y Carla , representada por la procuradora dª Amparo Ivana Rouanet Mota y defendida por el letrado D. Jaime Cros Cecilia.

La referida acusada fue declarada en busca y captura el 15/07/2015 y su rebeldía el 03/09/2015, expidiéndose orden internacional de detención el 16/07/2015, lo que motivó fuera detenida en Georgia, solicitándose a dicho país su extradición. Una vez fue concedida y entregada la reclamada, se celebró el 04/05/2016 la pertinente comparecencia del artículo 505 de la L.E.Crim ., tras la que se dictó auto acordando su prisión, situación en la que ha permanecido hasta el día de la fecha.

Realizado lo anterior, se remitieron las actuaciones a esta sección para la celebración del juicio con respecto de la indicada, lo que tuvo lugar el 04/07/2016.

Han sido partes, además de la citada y del Ministerio Fiscal, representado por el Ilmo. Sr. D. Daniel Campos Navas, la acusación popular personada en nombre de la "Asociación Nacional de Afectados por Internet y las Nuevas Tecnologías" (ANFITEC), representada por el procurador D. Miguel Torres Álvarez y defendida por el letrado D. Manuel Merino Maestre.

Actúa como ponente la Ilma. Sra. Dª CARMEN PALOMA GONZALEZ PASTOR, que expresa el parecer de la Sala.

ANTECEDENTES DE HECHO

PRIMERO.- Por el Juzgado Central de Instrucción nº 3 se incoaron las Diligencias Previas 70/12, a raíz de las investigaciones llevadas a cabo por la Brigada de Investigación Tecnológica, dependiente de la U.D.E.F., como consecuencia de la investigación realizada a nivel internacional contra el virus troyano conocido como

"Ransomware" que ha afectado a usuarios de varios países, entre ellos, España, donde más de 300 afectados, repartidos por la geografía española, han recibido mensajes en los que aparece el membrete falsificado de la policía española en sus ordenadores solicitándoles el pago de una cantidad de 100 euros por la presunta comisión de determinados ilícitos, dando lugar a la presentación de las correspondientes denuncias en las que se ha acordado su acumulación y unión a las presentes actuaciones. Practicadas las diligencias de instrucción que se estimaron pertinentes, el 03/07/2015 se dictó el auto de transformación de las referidas diligencias en el Procedimiento Abreviado, registrado con el número 70/12 que, tras ser recurrido en apelación por varios de los imputados fue confirmado en auto de 20/10/2015 por la sección tercera de la Sala de lo Penal de la Audiencia Nacional , de modo que tras presentarse los escritos de acusación del Ministerio Fiscal y de la acusación popular personada en nombre de la "AsociaciÓn Nacional de Afectados por Internet y las Nuevas Tecnologías" (ANFITEC), se dictó auto de apertura del juicio oral el 26/10/2015, al que fueron seguidos los respectivos escritos de defensa de cada uno de los acusados, incluidos el de la ahora enjuiciada que fue presentado al juzgado el 20/05/2016.

Remitidas, de nuevo las actuaciones a esta Sección el 03/06/2016, donde ya se había celebrado el juicio con respecto de los otros acusados, a los efectos de proceder al enjuiciamiento de la citada, se dictó auto de admisión de las pruebas y mediante Decreto se señaló para la celebración del juicio para el día 04/07/2016, fecha en la que el Ministerio Fiscal y la acusación popular manifestaron al tribunal haber llegado a un acuerdo con la defensa de la acusada así como ésta última.

SEGUNDO.- El Ministerio Fiscal calificó definitivamente los hechos para la acusada Purificacion , como constitutivos de un delito de blanqueo de capitales, del artículo 301 del Código Penal , con la concurrencia de la circunstancia modificativa de la responsabilidad criminal analógica de confesión tardía (artículo 21.7º en relación con la 4ª del Código Penal), por lo que solicitó la pena de un año de prisión y multa de 30.000 euros con responsabilidad personal subsidiaria de 16 días en caso de impago, inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena y pago proporcional de las costas.

CUARTO.- La acusación popular calificó los hechos de conformidad con la acusación pública, solicitando la imposición de las mismas penas.

QUINTO.- La defensa de la acusada, en idéntico trámite, calificó los hechos de conformidad con la acusación pública, solicitando la imposición de la misma pena.

HECHOS PROBADOS

Y así expresamente se declara

1.- Al menos desde mayo de 2011, centenares de miles de ordenadores de todo el mundo comenzaron a verse afectados por un virus-troyano conocido como policialmente como "RANSOMWARE" o "BLOKER" como era llamado en los ámbitos delincuenciales, habiéndose producido tales infecciones en países como Canadá, Estados Unidos, Emiratos Árabes, Irán, Rusia, Austria, Bélgica, Suiza, Alemania, Dinamarca, Finlandia, Francia, Grecia, Irlanda, Italia, Luxemburgo, Holanda, Malta, Portugal, Rumania, Suecia o Reino Unido.

El RANSOMWARE actuaba a en función de parámetros pre- fijados de navegación web, relacionados con la actividad de la víctima a través de la Red, se activaba y ejecutaba bloqueando el equipo informático de las víctimas solicitando el pago de una multa para su desbloqueo. Bajo la apariencia de un comunicado en nombre de diferentes Cuerpos Policiales de los países arriba referenciados, alertaba al usuario que en su ordenador se había constatado un tráfico de datos y de navegación vinculados directamente con diferentes ilícitos penales (pornografía infantil o actividades de terrorismo), induciéndole, a efectuar el pago de la cantidad de 100 euros a través de pasarelas de pago virtuales y anónimas (PAYSAFECARD y UKASH para Europa o MONEYPAK para EEUU), a modo de multa por el ilícito penal presuntamente detectado para con ello conseguir el desbloqueo y el acceso de los datos del equipo informático infectado.

En el caso español, en una de sus variantes, al bloquearse el ordenador la pantalla del mismo era ocupada por un mensaje con el escudo y formato que imitaba los oficiales del Cuerpo Nacional de Policía con el siguiente texto:

" *La POLICIA ESPAÑOLA.*

Atención!!! Ha sido detectada actividad ilegal!! Su sistema operativo ha sido bloqueado debido a una infracción de la legislación española!

Han sido detectadas las siguientes infracciones: Su dirección IP ha sido registrada en las webs ilegales con contenido pornográfico orientadas a la difusión de la pornografía infantil, zoofilia e imágenes de violencia contra menores! En su ordenador han sido detectados los archivos de video de contenido pornográfico con elementos

de violencia y pornografía infantil! Además, desde su ordenador se realiza un envío ilegal (SPAM) de orientación pro terrorista. El presente bloqueo ha sido realizado para prevenir la posibilidad de difusión de dichos materiales desde su ordenador en Internet.

Sus datos IP

Browser OS

Country City

ISP

Para desbloquear su ordenador, Usted debe pagar una multa de 100 euros! La multa tiene que ser pagada antes de 24 horas desde el momento del bloqueo de su ordenador! En el caso de impago, todos los datos de su ordenador serán eliminados!

Usted tiene dos formas de pagar la multa:

Usted puede adquirir un cupón UKASH por el importe de 100 euros. El número de ese cupón UKASH, usted ha de introducir en el campo del pago y apretar el botón "OK".

Usted puede pagar la multa mediante paysafecard.

Usted ha de pagar paysafecard por importe de 100 euros. Usted ha de introducir el código PIN delcheque en el campo del pago y apretar el botón "OK". "

El citado texto era mostrado en diversos idiomas dependiendo de la localización geográfica de la víctima proporcionando en este mensaje diversas cuentas de correo electrónico donde supuestamente se contactaba con el cuerpo policial que aparecía en el mensaje.

2. La puesta en marcha y explotación del "RANSOMWARE" era obra de una grupo de personas ruso parlantes y ubicadas principalmente en Rusia, que mantenían sus contactos a través de Internet, utilizando foros de acceso restringido, chats y servicios de comunicación, en los que siempre se identificaban mediante un apodo o nickname, que conservaban en el tiempo y que era su principal credencial para acceder a dichos ámbitos virtuales de ciberdelincuentes y relacionarse entre ellos. Dentro de esa estructura delincuencial, los distintos miembros del grupo se hacían cargo de las distintas funciones que abarcaban desde la creación de virus hasta el circuito económico del producto de su actividad. Entre las distintas etapas o tareas de la citada estructura se pueden distinguir las siguientes:

A.- Creación y distribución del código malicioso. El "ransomware coder" era la persona encargada de programar el ransomware y de ponerlo a disposición de otros miembros del grupo en foros underground de hacking. Se elaboraba de forma expresa, ya sea para un individuo o para un grupo de afiliados, todo ello por una suma concreta de dinero o bien por un porcentaje de las ganancias ilícitas, tomando como base el número de ordenadores infectados. El "coder" aparte de ofrecer el código, ofrecía también un servicio de actualizaciones diarias de dicho código, para que no pudiera ser detectado por los antivirus o bien dificultar así, su estudio mediante técnicas de reversing, las cuales permiten analizar las acciones que genera el ransomware dentro del ordenador y acceder a las estadísticas generadas por los servidores de control "C&C".

B- En otro plano de la actividad, aparecía el grupo de usuarios denominados "ransomware exploiters", que se dedicaban a explotarlo, estableciendo la infraestructura de dominios y servidores para su propagación e infección, Dichos dominios y servidores eran contratados con datos falsos por los denominados "exploiters", a través de resellers o revendedores de dominios de Internet *(empresas de hosting rusas que a su vez subcontratan dominios por todo el mundo)* que suelen ofrecer precios económicos o servicios de bulletproof hosting *(servicios de hosting que entre las clausulas del contrato que firman con los clientes está la de avisarles en caso de que cualquier autoridad pregunte por los servicios que tiene contratados)* .

C.- La infraestructura se caracterizaba por el anonimato tanto en la contratación de los dominios y servidores, como en los accesos a los servidores de control "C&C" y como por su corto periodo de uso de dichos servidores. Los servidores de control "C&C" eran los que llevaban el control estadístico del número de usuarios infectados, albergaban las imágenes del bloqueo del ordenador simulando las respectivas Policías de cada país afectado. Estos servidores "C&C" eran de vital importancia para la investigación ya que si se logran intervenir a tiempo, mediante la realización de técnicas forenses se podrían ver las conexiones realizadas por los usuarios maliciosos que tienen el control del mismo. Los pagos de los servicios y servidores "C&C" se hacían a través de paypal o medios de pago de moneda electrónica/virtual.

D.- La infección del ordenador de la víctima se producía navegando por internet, generalmente a través de páginas muy visitadas. Dado que la víctima desconocía el momento en concreto se ha infectado, resultaba imposible hacer el seguimiento y análisis de los sitios comprometidos.

E.- Otro aspecto de la organización era el relativo al movimiento económico del dinero obtenido. Otros miembros de la organización, se encargaban de convertir los códigos UKASH, PaysafeCard o Moneypak pagados por las víctimas, en dinero físico o virtual, y ponerlo a disposición de los exploiters. Este sistema carecía de mulas físicas que se encarguen de convertir los códigos de Ukash, Moneypak y Paysafecard en dinero real, sin embargo había miembro de la organización que realizaban esa gestión y contactaban directamente o mediante intermediarios con los "exploiters", cobrando por ello una retribución.

3.- En el caso de usuarios españoles infectados el mensaje utilizado para el bloqueo de sus equipos facilitaba el dominio concreto de "lapoliciaespanola.org", como modo alternativo a efectuar el pago en caso de que el sistema no lo pudiera confirmar. Dicho dominio había sido registrado a nombre de un tal " Jose Ángel ", facilitando la cuenta de correo electrónico DIRECCION000 . Este mismo e-mail fue utilizado para el registro de los dominios landes-kriminalt.net, landes- kriminalt.org, bundeskriminalamt.net (Alemania), it-polizia.org (Italia), policemetropolitan.org (afectando a Reino Unido), n- p-f.org (afectando a Francia) que constaban en las imágenes del virus en dichos países, lo que evidenciaba un origen común en los fraudes asociados a todos ellos.

En los datos del registro de bundeskriminalamt.net, la citada cuenta de correo DIRECCION000 estaba vinculada con el apodo o nickname " Canoso ". " Canoso " fue localizado en el foro ruso "gofuckbiz.com" en el que realizaba una serie de publicaciones relacionadas con la distribución de malware y buscando formas de traficar con códigos Ukash y Paysafecard, facilitando para sus contactos la cuenta de NUM002 y la cuenta de mensajería instantánea Jabber identificada como DIRECCION001

De esta forma se pudo conocer que el usuario de la cuenta DIRECCION000 , DIRECCION001 , e NUM002 , era la persona conocida en los foros delincuenciales como " Canoso " o " Flequi ", que era el máximo responsable de la creación y difusión a nivel mundial del virus-troyano "RANSOMWARE" o "BLOKER".

Tras una exhaustiva y minuciosa investigación policial, se ha podido determinar que la identidad real de " Canoso " o " Flequi ", es la de uno de los acusados ya enjuiciados Florentino .

4.- En las presentes diligencias previas constan 933 denuncias de personas cuyos ordenadores fueron afectados por el "Ransomware", de las cuales 390 pagaron la cantidad exigida (se adjunta anexo con el listado con las identidades de dichas personas que efectuaron el pago), si bien el número de ordenadores puede estimarse mucho mayor ya que en el Instituto Nacional de Tecnologías de la Comunicación (INTECO) -ahora Instituto Nacional de Ciberseguridad (INCIBE)- se recibieron

784.415 consultas relacionados con el citado virus y 26.028 llamadas telefónicas.

5.- Una vez las víctimas habían pagado lo que pensaban era una multa, los distribuidores del "Ransomware" se hacían con los códigos de Paysafecard, Ukash o Moneypak, e iniciaban una nueva etapa para reciclarlos ocultando el ilícito origen de los mismos y obtener su importe ya fuera en efectivo, ya en cuentas seguras de los miembros de la organización.

La investigación permitió conocer que en España se estaban llevando a cabo simultáneamente dos modalidades de conversión de los códigos UKASH, Moneypak y Paysafecard en dinero o en cuentas de los miembros de la organización, incluido Florentino .

6.- En la primera de las variantes de reciclado de los códigos de las plataformas de pago virtual, la organización asentada en Rusia a través de Internet enviaba a los miembros de la organización que operaba en España, más concretamente en la provincia de Málaga, las numeraciones de los códigos Ukash, Paysafecard y Moneypak procedentes del "ransomware" con los que realizaban los siguientes pasos:

a/ Solicitaban la emisión de tarjetas de crédito y débito mediante páginas de Internet a nombres supuestos y domiciliados supuestamente en los Estados Unidos de América. Una vez emitidas esas tarjetas, eran remitidas por otro miembro de la organización a España a través de envíos de paquetería postal (FEDEX).

b/ El mismo día que la organización disponía físicamente de las tarjetas, eran activadas y cargadas el dinero "virtual" procedente de los códigos Moneypak en las mismas. Pare ello los acusados utilizaban un acceso por escritorio remoto a un servidor situado en Estados Unidos con dirección IP NUM003 , al objeto de burlar la medida de seguridad de la propia web www.moneypak.com que exige que los códigos Moneypak sean cargados desde una conexión IP geolocalizada en Estados Unidos.

Una vez cargadas de saldo con cargo a los códigos Moneypak, a continuación y preferiblemente en horario nocturno, varios de los miembros de la organización hacían sucesivas rondas de cajeros para extraer dinero en efectivo.

c/ Una vez tenían en su poder el efectivo extraído de los cajeros, los acusados lo enviaban a los miembros de la organización en Rusia mediante envíos a través de Agencias de Envío de Dinero, como Western Union o Money Gram fundamentalmente, en los que los miembros de la organización asentada en España iban rotando sus identidades con el fin de no sobrepasar las cuantías que determinaran las comunicaciones de las entidad al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC).

d/ Otra de las formas de enviar el dinero al exterior era mediante transferencias a cuentas electrónicas con las que la organización opera en Rusia siendo el sistema elegido "Webmoney", esta divisa electrónica ofrecía como a la organización la posibilidad de depositar una gran variedad de monedas físicas en las cuentas pertinentes a cambio de denominaciones Webmoney equivalentes. Así por ejemplo, las cuentas de Webmoney con la denominación "Z", que la organización utiliza, quiere decir que todos los ingresos realizados en este tipo de cuenta son convertidos automáticamente en Dólares Americanos. Para ello emplearon el locutorio CALL BOX INTERNET regentado por Purificacion - con NIE NUM000 , nacida el NUM001 /1976 en Georgia y sin antecedentes penales- sito en la Avenida Isabel Manoja 22 de Torremolinos, tratándose de una casa de cambio autorizada para el envío de dinero a través de Webmoney hacia Rusia. Los acusados ingresaban a través de cajeros automáticos en la cuenta del locutorio o de la propia Purificacion las cantidades a enviar, y para identificar el destino se hacía constar en las referencias de los ingresos los números de la cuenta de Webmoney a la que había que transferir las cantidades. El importe y las numeraciones las habían recibido previamente Jesús María o Camilo de los ciberdelincuentes a través de las comunicaciones mantenidas a través de jabberes.org.

FUNDAMENTOS DE DERECHO

PRIMERO.- Los hechos así relatados constituyen, a juicio del tribunal, para la acusada Purificacion , un delito de blanqueo de capitales, del artículo 301 del Código Penal , en el que han resultado debidamente acreditada su participación a través del reconocimiento de su participación objeto de acusación tanto en el escrito del Ministerio Fiscal, como en el de la acusación popular.

Así las cosas, entendiendo el tribunal que los hechos objeto de acusación y reconocidos por la acusada se corresponden con las calificaciones efectuadas, procede, de conformidad con lo dispuesto en el artículo 787.2 de la L.E.Crim . dictar sentencia en los términos aceptados, toda vez que los hechos declarados probados han sido realizados por cada uno de los acusados en los términos expuestos y se corresponden con las calificaciones realizadas.

Habiéndose interesado por el Ministerio Fiscal, la acusación popular y la propia defensa en el acto del plenario la solicitud de la declaración de firmeza de la presente resolución, comprobada la asunción de los hechos y responsabilidad penal por parte de la acusada y su defensa, procede, de conformidad con lo dispuesto en el artículo 695 de la L.E.crim ., declarar firme la presente resolución al plasmarse en ella los hechos objeto de acusación y la conformidad debidamente prestada por la acusada y su defensa.

SEGUNDO.- Concurre la circunstancia modificativa de la responsabilidad criminal analógica de confesión tardía, al haber reconocido en juicio su participación (artículo 21.7º en relación con la 4ª del Código Penal). Lo anterior, motiva la imposición de la pena interesada en los términos que se exponen en la Parte Dispositiva de la presente resolución.

TERCERO.- En materia de costas, procede imponer a la acusada la parte proporcional de conformidad con lo dispuesto en los artículos 123 del código Penal y 240 de la L.E.Crim .

VISTOS los citados preceptos y demás de general y pertinente aplicación

F A L L A M O S

QUE DEBEMOS CONDENAR Y CONDENAMOS a la acusada **Purificacion ,** como autora de un delito de blanqueo de capitales, con la concurrencia de la circunstancia modificativa de la responsabilidad criminal analógica de confesión tardía, a la pena de **un año de prisión,** multa de 30.000 euros, con responsabilidad subsidiaria de 16 días en caso de impago, inhabilitación especial para el derecho de sufragio pasivo durante la condena y pago de las costas.

Será de abono a la acusada el tiempo que ha estado privada de libertad.

Se acuerda el comiso de todos los efectos informáticos y efectos incautados.

Se declara la firmeza de la presente resolución.

Así, por esta nuestra sentencia definitivamente juzgando en esta instancia, lo pronunciamos, mandamos y firmamos.

PUBLICACIÓN.- Leída y publicada ha sido la anterior Sentencia por la Magistrado Ponente Ilma. Sra. Dª CARMEN PALOMA GONZALEZ PASTOR, estando celebrando audiencia pública el día de su fecha. Doy fe.