

**JDO. DE LO PENAL N. 3
GIJON**

SENTENCIA: 00224/2016

PROCEDIMIENTO ABREVIADO N° 385/15.

En Gijón, a seis de julio de 2016.

Vistos por Doña Asunción Domínguez Luelmo, Magistrada titular del juzgado de lo Penal n° 3 de esta ciudad, en juicio oral y público, los presentes autos procedentes de diligencias previas n° 1867/11 del Juzgado de instrucción n° 4 de Gijón y seguidos por un delito de grupo criminal y un delito continuado de daños, contra _____, nacido en _____,

_____ ón conocida, sin antecedentes penales, del que no consta solvencia y en situación de libertad provisional por esta causa, de la que estuvo privado el día 20-5-11, representado por el Procurador D. MANUEL FOLE LOPEZ y defendido por el Letrado D. DAVID MAEZTU LACALLE, contra _____,

_____ DNI n° _____ micilio en _____ o, sin profesión conocida, sin antecedentes penales, del que no consta solvencia y en situación de libertad provisional por esta causa de la que estuvo privado del día 31-5-11 al 2-6-11, representado por la Procuradora DÑA NOELIA MENENDEZ TAMARGO y defendido por el Letrado D. MIGUEL CAPUZ SOLER y contra _____,

_____ e Alicante es penales, del que no consta solvencia y en situación de libertad provisional por esta causa de la que estuvo privado del día 3 al 6-6-11, representado por la Procuradora DÑA VICTORIA ESTRADA GARCIA y defendido por el Letrado D. CARLOS SANCHEZ ALMEIDA y siendo parte acusadora el Ministerio Fiscal.

ANTECEDENTES DE HECHO

PRIMERO. Las presente causa seguida por delito de pertenencia a grupo criminal y delito continuado de daños contr _____,

tiene su origen en diligencias previas n° 1867/11 del juzgado de instrucción n° 4 de Gijón y una vez recibidas las mismas se señaló día para el juicio y se procedió a su celebración, planteándose por las defensas diversas cuestiones en el turno de intervenciones parte de las cuales se resolvieron en el acto y practicándose las pruebas propuestas que fueron admitidas, con el resultado que obra en autos.



SEGUNDO. El Ministerio Fiscal, en sus conclusiones provisionales calificó los hechos enjuiciados como constitutivos de un delito de grupo criminal previsto y penado en los artículos 15-1 y 570 ter 1 c) y 2 a) del C.P. y un delito continuado de daños previsto y penado en los arts 15-1, 74 y 264-2 y 3-2º del C.P. estimando responsables en concepto de coautores a los acusados

concurrancia de la circunstancia atenuante analógica del art. 21-7º en relación con el art. 21-4º del C.P. en el acusado y sin la concurrancia de circunstancias modificativas de responsabilidad en los otros dos acusados y pidió que se les impusieran a cada uno de los

primer delito la pena de once meses de prisión con inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena, y por el segundo delito la de cuatro años y cinco meses de prisión con igual inhabilitación durante el tiempo de la condena, y 5.600 euros de multa y a por el primer delito la pena de ocho meses de prisión con inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena, y por el segundo delito la de cuatro años y cuatro meses de prisión con igual inhabilitación durante el tiempo de la condena, y 4.200 euros de multa, así como a todos ellos el pago de las costas procesales y que se procediera al comiso del material informático intervenido, de conformidad con el art. 127 del C.P. y 2-4º A) del RD 2783/76 el cual con arreglo a lo dispuesto en los arts 781 y 367 quinquies 1.1.a) de la L.E.Cr. se entregara previamente formateadas sus unidades de almacenamiento lógicas y físicas a la Unidad de Policía Judicial actuante en esta causa. Igualmente solicitó que los acusados indemnizaran conjunta y solidariamente al Congreso de los Diputados en cuanto órgano que provee de los medios materiales de la Junta Electoral Central en 700 euros con aplicación de los intereses legales.

TERCERO. El Ministerio Fiscal en sus conclusiones definitivas realizó las siguientes modificaciones: retiró la circunstancia atenuante analógica solicitada inicialmente para el acusado y solicitó para cada uno de los acusados por el delito de grupo criminal la pena de siete meses y dieciséis días de prisión y por el delito continuado de daños la de tres años, ocho meses y un día de prisión, multa de 1.400 euros y responsabilidad personal subsidiaria de treinta días en caso de impago, elevando el resto a definitivas.

CUARTO. La defensa de solicitó su libre absolución, alegando con carácter previo cuestiones relativas a la vulneración de derechos fundamentales y a la irregularidad de las pruebas practicadas.





QUINTO. La defensa de solicitó su libre absolución, alegando con carácter previo cuestiones relativas a la vulneración de derechos fundamentales y a la irregularidad de las pruebas practicadas.

SEXTO. La defensa de solicitó su libre absolución, alegando con carácter previo cuestiones relativas a la vulneración de derechos fundamentales y a la irregularidad de las pruebas practicadas.

HECHOS PROBADOS.

No consta que los acusados y pertenecieran a grupo criminal con el objeto de cometer de forma concertada uno o varios delitos menos graves o de la perpetración reiterada de faltas.

No consta que los acusados formaran parte del colectivo Anonymous y que con ocasión de la celebración en España de las elecciones locales y autonómicas de fecha 22 de mayo de 2011, con la finalidad de entorpecer el proceso electoral se hubieran puesto de acuerdo y hubieran dirigido, organizado y ejecutado un ataque de Denegación de Servicio Distribuido (DDoS), el día 18 de mayo de 2011 bajo el nombre de operación "Spanish Revolution" contra el entorno informático de la Junta Electoral Central residente en el Congreso de los Diputados, contra la página web de la Unión general de Trabajadores y contra la página web del Congreso, que hubiera afectado de forma importante al normal funcionamiento del correo electrónico obstaculizando los trámites previos al proceso electoral ni que remitiendo múltiples peticiones simultáneas hubieran ocasionado el bloqueo de la página web de la Junta electoral central, ni que hubieran acordado realizar otro ataque de Denegación de Servicio Distribuido DDoS sobre las 16,00 horas del día 20 de mayo de 2011 la llamada operación "V de Votaciones" contra las páginas web del PP, del PSOE y de CIU.

FUNDAMENTOS JURÍDICOS

PRIMERO. Se imputa a los tres acusados por el Ministerio Fiscal un delito de grupo criminal previsto y penado en los artículos 15-1 y 570 ter 1 c) y 2 a) del C.P. y un delito continuado de daños previsto y penado en los arts 15-1, 74 y 264-2 y 3-2º del C.P.

El delito previsto y penado en el art. 570 ter 1 c) sanciona la conducta de quienes constituyeren, financiaren o integraren un grupo criminal, cuando se trate de cometer uno o





varios delitos menos graves no incluidos en apartado a) (delitos contra la vida o integridad física de las personas, la libertad, la libertad e indemnidad sexuales o la trata de seres humanos), o de la perpetración reiterada de faltas, disponiendo que a los efectos de este código se entiende por grupo criminal la unión de más de dos personas, que sin reunir alguna o algunas de las características de la organización criminal definida en artículo anterior tenga por finalidad o por objeto la perpetración concertada de delitos o la comisión concertada y reiterada de faltas.

El subtipo agravado establecido en el apartado 2 a) del mismo precepto legal se refiere al supuesto de que el grupo estuviera formado por un elevado número de personas.

Dicho tipo fue introducido en el Código Penal por LO 5/10 de 22 de junio según se establece en su Exposición de Motivos para sancionar las formas de concertación criminal que no encajaban en el arquetipo de las organizaciones criminales pero que sí aportan un plus de peligrosidad criminal a las acciones de sus componentes, porque la jurisprudencia relativa al delito de asociación ilícita así como la que ha analizado las ocasionales menciones que el código penal vigente hace a las organizaciones criminales, como en materia de tráfico de drogas, requiere la comprobación de una estructura con vocación de permanencia, dejando fuera otros fenómenos análogos muy extendidos en la sociedad, a veces extremadamente peligrosos o violentos que no reúnen esos requisitos estructurales. La necesidad de responder a esa realidad conduce a la definición en paralelo con las organizaciones de los que esta ley denomina grupos criminales.

El precepto relativo a los grupos criminales, equipara las conductas de constitución de los mismos, con la financiación de su actividad o la integración en ellos, pero siempre distinguiendo la respuesta punitiva a partir de la gravedad de las infracciones criminales que tratan de cometer, en términos análogos a los que rigen para las organizaciones, y con similares agravaciones en razón de las características del grupo.

Se ha venido por ello declarando que el grupo criminal está constituido por un grupo de personas mínimamente coordinadas y puestas de acuerdo de forma estable y duradera durante un cierto período de tiempo, que han realizado actividad ilícita.

El delito previsto y penado en el art. 264-2 del C.P. sanciona la conducta del que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando suprimiendo o haciendo inaccesibles datos informáticos cuando el resultado producido fuera grave

El apartado tercero del mismo precepto en su apartado segundo establece un subtipo agravado cuando se hubieran ocasionado daños de especial gravedad o afectado a los intereses generales.



El tipo del art. 264-2º del C.P. fue introducido por la reforma de LO/95 en la que se pasó a configurar como un tipo agravado más del delito de daños, tratando de dar respuesta al problema introducido a raíz del desarrollo de las nuevas tecnologías por los conocidos como piratas o hackers a través de la difusión de virus informáticos, es decir programas cuya finalidad es producir un deterioro o destrucción del software de los terminales que infectan, o sencillamente una alteración de su sistema operativo, que determina un funcionamiento anómalo o deficiente, problema para el que no daba respuesta el tipo básico ordinario, pensando más en la afectación de un bien, de un objeto material tangible.

El delito de daños constituye una figura concretada en la destrucción o menoscabo material o funcional de la propiedad ajena, de manera que el objeto de ajeno dominio sobre el que se lleva a cabo la acción resulte destruido o menoscabado, sea en su entidad física sea en la funcionalidad que le es propia.

La acción de destruir, alterar, inutilizar, dañar de cualquier otro modo datos programas o documentos electrónicos contenidos en un soporte informático, venía a comportar un daño patrimonial por reparación o sustitución del objeto material sobre el que habían operado dichas acciones.

Por ello se introdujo el tipo del que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o documentos informáticos y tras la reforma operada por LO 5/10 de 22 de junio se amplió su ámbito de un lado dándole carta de naturaleza propia al dejar de contemplarlo junto a las circunstancias cualificadoras de los daños, dotándole de autonomía sistemática y de otro lado recogiendo un elenco de conductas más amplio para solventar así todo debate en relación a su alcance, a que manipulaciones debían valorarse, pasando a contemplar prácticamente cualquier injerencia en un programa ajeno, con tal de que esta pueda tacharse de grave, ya que en su apartado primero como elenco de conductas punibles se alude a borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos, programas o documentos y en su apartado segundo a obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno introduciendo transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos.

Entre los procedimientos informáticos de ataque a los elementos lógicos de un sistema informático o vandalismo electrónico, se vienen citando los crash o programas de destrucción progresiva, las bombas lógicas de actuación retardada, virus programs, caballo de Troya, etc y entre los que se dirigen a la alteración u obstaculización del funcionamiento informático el mail bomber o las bombas ANSI y la denegación de servicio de ataques DDoS.

En ambos casos la conducta se ha de realizar sin autorización y de forma grave y el resultado ocasionado ha de ser igualmente grave.



El tipo no concreta los criterios para determinar la gravedad de la conducta, lo que plantea el problema de delimitar los ataques que puedan resultar realmente perturbadores o molestos pero penalmente insignificantes y distinguirlos de los que por su mayor gravedad revisten relevancia penal.

Las defensas solicitaron la libre absolución de los acusados de vulneración de derechos e irregularidad de las pruebas obtenidas y por estimar que los hechos no tendrían adecuado marco en los tipos objeto de acusación.

SEGUNDO. Han sido varias las cuestiones planteadas a lo largo del procedimiento, al inicio del juicio oral y en el transcurso del mismo, unas relativas al inicio de las investigaciones y origen de la imputación respecto de los acusados, otras relativas a defectos de forma del procedimiento y otras relativas a las pruebas practicadas que han sido impugnadas por vulneración de derechos fundamentales y por defectos de forma que se estima produjeron indefensión.

Algunas se rechazaron en el turno de intervenciones previo a la celebración del juicio.

Así la cuestión alegada por la defensa de de haberse producido el efecto de cosa juzgada respecto del primero de los hechos objeto de acusación por haberse formulado denuncia por el archivero bibliotecario de la Junta Electoral Central en fecha 19 de mayo de 2011 sobre la base de haber recibido desde las 19,00 horas del día anterior correos electrónicos masivos relacionados con la autorización de la concentración de la Puerta del Sol, que se seguían recibiendo con el consiguiente perjuicio al normal funcionamiento del sistema informático y de haberse producido esa misma mañana el acceso masivo a la página web de la junta que había ocasionado el bloqueo con otros usuarios y por haberse decretado por el juzgado de instrucción nº 5 de Madrid en fecha 25-5-12 el sobreseimiento libre y archivo de las actuaciones (Folios 1041 y ss), cuestión que se rechazó por no ser el juzgado de Madrid el juzgado competente y por no proceder valorar en ese momento la identidad de hechos y de sujetos, no procediendo por ello la expulsión del procedimiento de los referidos hechos.

Asimismo se rechazó la expulsión del enjuiciamiento del segundo de los hechos descritos en el relato fáctico del escrito de acusación, no recogidos en auto de fecha 24-2-14, sobre la base del criterio mantenido por la Sección Octava de la Audiencia Provincial de Oviedo entre otras en sentencia de 7-7-15 conforme al cual la delimitación del objeto del proceso penal, viene determinada por los escritos de acusación y solo puede producirse una delimitación negativa cuando el instructor excluye expresamente un hecho o determinado delito, estimando que los acusados conocían los hechos objeto de imputación, a lo que debe de añadirse que el auto cuestionado fue recurrido y fue confirmado en apelación.

En cuanto a la cuestión invocada por la defensa de , de vulneración de derechos fundamentales s derivada de la grabación, escucha e incorporación a la causa de las conversaciones entre abogado y cliente, como ya se indicó al margen de los extremos que hayan podido determinar la evolución en la investigación de los hechos y de la imputación de infracciones de que haya sido objeto a lo largo del





procedimiento el acusado , lo cierto es que la defensa de dicho acusado, en la fase de instrucción y concretamente en escrito de fecha 28 de junio de 2011 presentado en fecha 30 de junio de 2011, ante la comprobación efectuada tras tener acceso al registro de llamadas autorizadas por la juez de instrucción y al informe elaborado por la policía respecto al contenido de las conversaciones consideradas relevantes para la investigación de la causa, solicitó la retirada de las transcripciones de las conversaciones entre el letrado y incorporadas al informe de fecha 7 de junio de 2011 y que formaban parte de los folios 322, 332, 333, 339, 342 y 344, la retirada de las conclusiones sobre dichas conversaciones contenidas en los folios 260, 261 y 262 y la retirada de todas aquellas referencias al mismo en el sentido de la imputación de un delito de asociación ilícita producidas con posterioridad a la conversación de fecha 27 de mayo de 2011 y previo informe del Ministerio Fiscal, por la magistrada se dictó providencia en fecha 25 de julio de 2011 por la que se acordó accediendo a lo interesado en los dos primeros apartados del escrito, el desglose de las actuaciones de los folios 260, 261, 262, 322, 332, 333, 339, 342 y 344, es decir todos aquellos que la representación de había solicitado retirar, obrando seguidamente al folio 744 diligencia de constancia en que por la Secretaria Judicial se hace constar que se procede al desglose de los folios a que se refiere la anterior diligencia y que obran unidos al tomo II de las actuaciones, saltando en el mismo del folio 259 al 263, del 321 al 323, del 331 al 334, del 338 al 340, del 341 al 343 y de este al 345, devolviéndose los mismos a la Brigada de Investigación Tecnológica, y habiéndose denegado únicamente en la providencia antedicha la solicitud formulada en el apartado tercero del escrito de fecha 28 de junio, por estimar que la tipificación delictiva no dependería de las referencias que aparecieran en la causa acerca de figuras delictivas sino de los indicios de criminalidad que se encontraran al término de la instrucción.

El juzgado instructor acogió en su integridad la solicitud formulada de retirada de las conversaciones entre R y su letrado y pese a que se sostiene por dicha representación que dichas conversaciones aún constan en el procedimiento, por la juzgadora se ha comprobado que se desglosaron todos los documentos reseñados y como ya se manifestó al inicio del juicio, si alguna conversación no hubiera sido reseñada en su momento por dicha parte, en absoluto será tenida en cuenta por la juzgadora en el enjuiciamiento de los hechos, declarándolas en su caso nulas. Lo mismo cabe decir respecto de las conversaciones del mismo con su cliente que la defensa de Yuri López Ibáñez manifestó en el acto del juicio aún constaban en el procedimiento.

En principio la posible evolución en la imputación respecto a dicho investigado o la aportación de otras evidencias inculpatorias no se considera que venga necesariamente determinada por las escuchas de las conversaciones antes referidas o por el conocimiento de la estrategia de defensa, que en cualquier caso fue planteada desde un principio por la misma.

En otro orden de ideas no se aprecia la invocada parcialidad de la magistrada instructora alegada por la defensa de por retraso en la entrega de la



documentación reseñada por dicha defensa, pues aunque no cabe duda que hubo un retraso en el traslado de la misma y aunque es cierto que el Ministerio Fiscal solicitó en su momento su subsanación y la defensa no tuvo a su disposición los documentos hasta momento posterior, ello no supone parcialidad en la instrucción de la causa ni se estima se produjera vulneración del derecho a juez imparcial en el sentido invocado.

TERCERO. Se reiteró por la defensa de la cuestión planteada a lo largo del procedimiento con ocasión de los recursos interpuestos contra distintas resoluciones, de vulneración de derechos fundamentales por la identificación obtenida del proveedor de servicios de Telecable Asturias contra el contenido de la Ley 25/07 de conservación de datos, solicitando que como consecuencia de ello se declarase la nulidad de todas las pruebas derivadas de dicha identificación, invocando en último término la sentencia del T.J.U.E. de 8-4-14 y el planteamiento en su caso de la oportuna cuestión prejudicial.

Asimismo se argumentó que el agente que en el atestado figuraba con el pseudónimo Sprocket que se decía se había ganado la confianza de los acusados en las conversaciones de la red social, era un agente encubierto que no estaba amparado por autorización judicial y que incluso habría podido incurrir en delito provocado.

La defensa de invocó vulneración de derechos fundamentales por incumplimiento de la cadena de custodia, quiebra de fe pública judicial, nulidad de los desprecintos y volcados de datos de los efectos que se dicen intervenidos al acusado y asimismo por vulneración de derechos con ocasión de su detención y declaración.

La defensa de invocó también la vulneración del art 18 y 24 de la C.E. tanto en relación con el origen de la investigación respecto de dicho acusado, detención y declaración del mismo como respecto de los desprecintos y volcados de los efectos que se dicen intervenidos a dicho acusado, cuestión que asimismo fue planteada por la defensa de

Como ya se dijo al inicio del juicio oral dada la complejidad y naturaleza de las cuestiones invocadas, se consideró más adecuada su resolución en sentencia tras la aclaración de muchos de los extremos invocados por los testigos y peritos propuestos y por tanto tras la valoración de las pruebas practicadas.

Una vez incoadas las actuaciones en virtud de atestado en el que se solicitó la autorización para la entrada y registro en el domicilio de , en fecha 30 de mayo de 2011 se interpuso recurso de apelación contra dicha resolución de fecha 20 de mayo de 2011 que autorizó la entrada y registro en el domicilio de dicho acusado en el que se incautó material informático, solicitando la nulidad de lo actuado desde el momento en que se obtuvo dicha identificación.

En el escrito ya se apuntaba a que dicha identificación a la que se aludía en el atestado que dio lugar a la incoación de las diligencias en el juzgado de instrucción nº 4 de Gijón, debió de ser realizada previa solicitud motivada del juzgado y que fruto de la misma se autorizó la entrada y registro en el domicilio del acusado y se procedió a la retirada de material



informático para su remisión a la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía para el volcado de los datos contenidos y el análisis de los mismos.

Con ocasión del traslado del recurso al Ministerio Fiscal, el mismo ante la falta de constancia en autos de la resolución judicial mencionada en el folio 4 del atestado policial, que permitió la obtención de la identidad del titular de la línea de comunicación al que correspondía la dirección IP 93.156.74.169 y la determinación del domicilio respecto del cual se acordó la entrada y registro, solicitó mediante oficio que se remitiera exhorto al juzgado de instrucción nº 44 de Madrid, diligencias previas nº 3164/11 cuya referencia obraba en la contestación de Telecable cuya copia se aportó con el atestado (folio 23) en que acordaba dirigir el mandamiento a la operadora Telecable Asturias con objeto de que remitiera la información relativa a la IP de autos.

El recurso de apelación fue desestimado en su integridad mediante auto de fecha 2-12-11 de la Sección Octava de la Audiencia Provincial (folio 1034) en el que con referencia a la resolución en la que se acordaba librar el oficio a Telecable, razonó que se deducía dicha resolución del testimonio obrante al folio 22 y 23 del rollo de la Sala.

Se libró exhorto en fecha 9 de diciembre de 2011 a los juzgados de Madrid, y dicha resolución se incorporó a las actuaciones en fecha 28 de mayo de 2012.

A los folios 1157 y ss de las actuaciones consta que el juzgado de Madrid nº 44 remite el atestado nº 48081/11 al que se alude en la contestación de Telecable aportada con el atestado policial en virtud del cual se incoaron las actuaciones en el juzgado de instrucción nº 4 de Gijón, constando la solicitud de mandamiento judicial a Telecable de fecha 18 de mayo de 2011, para facilitar cuantos datos obren en sus archivos sobre el número de abonado, ubicación del mismo, y demás datos contractuales de la línea de teléfono a través de la cual se realizó la conexión a internet, a la que se asignó la IP 9315674169 entre el día 17 de mayo de 2011 entre las 18.51 GMT+2 y las 12,15 GMT+2 del día 18 de mayo de 2011.

En el atestado se hacía referencia a que a través del rastreo en la red se tuvo conocimiento de que estaba prevista la operación "V de Votaciones" protagonizada por el grupo Anonymous consistente en un ataque DDoS a las páginas webs de los partidos políticos PP, PSOE y CIU a realizar el día 20 de mayo a las 16,00 horas y tras explicar en qué consistía el ataque y la forma de actuar del grupo Anonymous, así como que los inspectores se habían ganado la confianza del administrador principal de pseudónimo Wicker que había comentado discrepancias con usuarios del canal hispano, que montaron un servidor casero anonhispanol.dynds.org, desde el que se organizarían ataques DDoS, se ofrecerían servicios de alojamiento para distribución de malware, páginas sobre operaciones de Anonymous, llegando a lucrarse de estas actividades, donde los atacantes se coordinarían darían instrucciones sobre las mismas a nivel nacional e internacional a través de su servicio de chat y que se había comprobado que dicha página se estaba resolviendo en la dirección IP 93.156.74.169, y que los días 17 de mayo de 2011 a las 18,51 GMT+2 y 18 de mayo a las 12,10 GMT+2 el dominio anonhispanol.dynds.org estaba activo y respondía





satisfactoriamente en dicha reacción IP, ante la previsión de nuevo ataque el día 20 de mayo, aportando las conversaciones de chat, se solicitó con urgencia mandamiento judicial a Telecable Asturias para que facilitara cuantos datos obraran en sus archivos sobre el número de abonado, titularidad, ubicación y demás datos contractuales de la línea de teléfono a través de la cual se había realizado la conexión a internet a la que se asignó la IP antes mencionada entre los días 17 de mayo a las 18,51 y 18 de mayo a las 12,15 horas.

Previo informe favorable del Ministerio Fiscal (1168 y 1169) empleando entre otros argumentos que del atestado aportado por la BIT Grupo de Seguridad Lógica parece desprenderse que personas integradas en el grupo anonymous cuyas vinculaciones, organización y estructura organizativa en este momento se desconocen, pudieran estar bloqueando o intentando bloquear las páginas web de partidos políticos y que considerando sin perjuicio de ulterior calificación jurídica a la vista del resultado que puedan arrojar las diligencias que se practiquen que podríamos estar en presencia de un delito tipificado en el art. 264 del C.P. que determina unas conductas típicas castigadas con penas privativas de libertad de 6 meses a dos años y de seis meses a tres años, sin perjuicio de tener atribuida pena superior en los supuestos determinados en el citado precepto, se dictó auto en fecha 19-5-11 por el referido juzgado en el que se acordó librar mandamiento a Telecable Asturias para que facilitaran a los funcionarios de la Brigada de Investigación Tecnológica, cuantos datos obraran en sus archivos sobre el número de abonado, titularidad, ubicación del mismo y demás datos contractuales de la línea telefónica da través de la cual se realizó la conexión a internet a la que se asignó la dirección IP antes reseñada, entre el 17 y 18 de mayo de 2011 (folio 1170), obrando al folio 1176 la respuesta de fecha 19 de mayo de 2011 de Telecable cuya copia fue aportada por la BIT en el juzgado de instrucción nº 4 con ocasión de la solicitud de entrada y registro en el domicilio del acusado

Consta que inicialmente las diligencias fueron sobreseidas provisionalmente el día 20-5-11 y que en fecha 28 de julio de 2012 se decretó su reapertura por el juzgado de instrucción nº 13 de Madrid y una vez solicitado informe a la BIT sobre el resultado de las investigaciones, se acordó su inhibición al juzgado de instrucción nº 4 de Gijón en fecha 8 de mayo de 2012.

Al margen del extremo referido, de que la resolución judicial que autorizó la identificación del acusado no obró en la causa hasta la fecha mencionada y de que en el atestado en virtud del cual se incoaron las actuaciones se hizo referencia al carácter urgente de la solicitud adjuntando únicamente la respuesta de Telecable al juzgado de Madrid que acordó el mandamiento, a ella se remitieron tanto la magistrada instructora como posteriormente la Audiencia Provincial para rechazar uno de los argumentos del recurso.

El auto de fecha 2-12-11 de la Audiencia Provincial por el que se desestima la apelación contra el auto de entrada y registro en el domicilio de , (folio 1034) se fundamenta además en que no lleva razón el recurrente en la menor gravedad de lo investigado, que no es un mero delito de daños sino que sin perjuicio ulterior calificación se trata de un delito continuado de daños informáticos de denegación





masiva de servicio con agravación del apartado tres, que no puede considerarse de afección poco masiva y contra intereses particulares pues se atacan webs de entidades y organismos como la junta electoral central y partidos políticos mayoritarios en periodo electoral, con lo que se están atacando los propios fundamentos del sistema constitucional español y de forma organizada, tanto a nivel nacional como internacional.

Iguales argumentos fueron empleados por la defensa con ocasión de la interposición de recurso de reforma y apelación contra el auto de fecha 21-5-11 de intervención, grabación y escucha de comunicaciones al acusado , y tanto la magistrada instructora en auto de fecha 3-10-11 como la Sección Octava de la Audiencia Provincial en resolución de fecha 8-2-12 (folio 1074) fundamentaron la desestimación en que el objeto del proceso no se determina ab initio sino a lo largo de la instrucción y considerando la medida de intervención proporcionada, ponderada por la gravedad de los hechos denunciados, por ser superior el beneficio para el interés general que el perjuicio que se causa con ella a otros bienes en conflicto (secreto comunicaciones) e idónea para el objeto propuesto y necesaria para avanzar en las investigaciones iniciadas, dada la dificultad de descubrir y constatar el delito y sus autores que posiblemente organizados, obstaculizaron, impidieron sin estar autorizados y de manera grave un sistema informático ajeno.

Asimismo la magistrada instructora en resolución de fecha 3-10-11 (folio 998) y la Audiencia Provincial en resolución de fecha 15-2-12 (folio 1070) con ocasión de la resolución del recurso contra el auto que acordó la apertura, copia y volcado de los datos contenidos en los dispositivos incautados, entre otros a , desestimaron el mismo con fundamento en el art. 579 de la L.E.Cr. y en que al tratarse de una actividad ilícita cometida por internet utilizando medios informáticos para preservar el anonimato y obtener la impunidad de la conducta, no existe medio menos lesivo de proseguir la investigación, atendida la gravedad del hecho, habida cuenta de los organismos y entidades públicas perjudicadas, la trascendencia social del hecho denunciado y la forma organizada de actuar los responsables, estimando la medida restrictiva proporcionada.

Aunque se trata de recursos contra distintas resoluciones, tanto la juez instructora como la Audiencia Provincial han venido corroborando los argumentos expuestos por el Ministerio Fiscal en oposición a las pretensiones de la defensa de Rodrigo Tuero acerca de la ilegalidad en la obtención de los datos del mismo a través de la dirección de IP fundamentándose en la doctrina del Tribunal Supremo y del Tribunal constitucional acerca de la determinación de la gravedad del delito a efectos de la injerencia de derechos, estimando que la obtención de nombre y dirección de abonado al que se asigna una dirección de IP es una afectación de la intimidad de menor intensidad a tener en cuenta al valorar la proporcionalidad de la medida.

El T.S. y T.C. tienen declarado al respecto de la intervención telefónica como causa de vulneración del derecho al secreto de comunicaciones que una medida restrictiva de dicho derecho solo puede entenderse desde la perspectiva de la proporcionalidad, ha de ser necesaria para alcanzar un fin constitucionalmente legítimo para la defensa del orden y





prevención de delitos calificables como infracciones punibles graves e idónea e imprescindible para la investigación de los mismos, y viene estimando que ha de valorarse al decidir sobre la intervención de comunicaciones telefónicas la existencia de una investigación en curso por un hecho constitutivo de un fracción punible grave en atención al bien jurídico protegido y a la relevancia social del hecho.

Se viene estimando que la gravedad de la infracción punible no puede estar determinada únicamente por la calificación de la pena legalmente prevista aunque es un factor a considerar sino que han de valorarse otros factores, como los bienes jurídicos protegidos y la relevancia social de los hechos, analizando las circunstancias concurrentes en el momento de su adopción.

En este sentido se comparte el criterio del Ministerio Fiscal mantenido por la magistrada instructora y ratificado por la Audiencia de que la realización de una actividad ilícita a través de una organización de cierta entidad objeto de investigación merecería un reproche social no escaso, por lo que se debe concluir con que se observó el principio de proporcionalidad, teniendo en cuenta que en materia excluida de la ley y Directiva que en principio supone un sacrificio de mayor intensidad de un derecho fundamental, se podría acordar la limitación para delitos calificados de menos graves pero la obtención de datos de nombre y dirección de abonado de una dirección de IP, que es una intromisión menos lesiva, no sería posible para investigar delitos con pena menos grave, lo que determinaría que quedarían impunes un número importante de delitos que se cometen a través de internet y que no alcanzan a ese nivel de gravedad.

El letrado de la defensa de mantiene en su escrito de conclusiones y en el acto de la vista, los argumentos ya expuestos con ocasión de la interposición del recurso contra el auto de entrada y registro en el domicilio del mismo, de vulneración del contenido de la Ley 25/07 de Conservación de Datos, que el único supuesto habilitante para la cesión de los datos es el servir a los fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal y en las leyes especiales.

Con invocación de la misma doctrina del TC sobre la superación del criterio penológico de los delitos graves, valorando el bien jurídico protegido y la relevancia social de los hechos, para analizar la proporcionalidad de una medida de intervención de comunicaciones, e invocando el principio de legalidad formal y material, argumentó asimismo que la LECr no pudo prever en su momento los medios de investigación y prueba y por ello el Tribunal Constitucional y el Tribunal Europeo de Derechos Humanos han venido supliendo las insuficiencias legales precisando los requisitos que la Constitución exige para la legitimidad de las intervenciones telefónicas.

Se invoca la Directiva 2006/24 del Parlamento europeo y del Consejo de 15-3-06 sobre la conservación de datos y en España la Ley 25/07 de Conservación de Datos y se alega que el primero de dichos textos delimita el alcance a los delitos graves definidos por la legislación nacional de cada estado miembro.



El art. 11-1 de la LCD 25/07 de 18 de octubre establece que esta ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados, siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el código penal y en las leyes penales especiales.

La referida cuestión alegada a lo largo del procedimiento, viene complementada por la defensa en su escrito de conclusiones y en el plenario por la invocación de la sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014 que ha declarado inválida la Directiva del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.

Se apunta en dicha resolución a que la directiva supone una injerencia de gran magnitud y especial gravedad en los derechos fundamentales al respeto a la privacidad y a la protección de datos de carácter personal, sin que esté limitada a lo estrictamente necesario.

Se establece en la referida sentencia que la seguridad aún siendo un valor muy relevante del que se derivan tanto un objetivo de interés general como un derecho subjetivo no tiene un carácter absoluto ni prevalente, y las medidas que se adopten para garantizar la seguridad deben ser proporcionadas, declarando que el legislador sobrepasó los límites que exige el respeto al principio de proporcionalidad, porque aunque la conservación de datos pueda considerarse adecuada para lograr la finalidad que persigue, la injerencia amplia y especialmente grave de la directiva en los derechos fundamentales que se trata no está suficientemente regulada para garantizar que dicha injerencia se limite efectivamente a lo estrictamente necesario. Considera que la conservación sin que los usuarios o abonados sean informados genera sensación de sometimiento permanente a vigilancia de la vida privada.

El tribunal no obstante considera necesaria la directiva, dictaminando que la conservación de datos para permitir autoridades nacionales acceso eventual a ellos responde objetivo de interés general y elemento útil en la investigación de delitos.

La anulación de la directiva europea no supone la prohibición de la conservación de datos sino que reclama la implantación de garantías adecuadas en la materia de protección de datos para corregir los defectos que se declaran en la sentencia.

Aún cuando la ley de Conservación de datos haya supuesto la transposición de la Directiva Europea, las regulaciones nacionales siguen siendo válidas y aunque no cabe duda de que habrán de tomarse las medidas necesarias para impedir la vulneración de derechos fundamentales a la espera de una nueva regulación europea, no se aprecian razones en el caso de autos para suspender el fallo hasta que el legislador pueda adoptar las referidas medidas.

En cuanto a lo que ha de entenderse por delito grave a efectos de la retención de datos, las reformas del C.P. y de



la L.E.Cr. LO 1/15 de 30 de marzo y LO 13/15 se han ocupado de ello.

La Audiencia Provincial con ocasión de la resolución de los recursos interpuestos, dejó clara su postura interpretativa de la norma, en línea con la doctrina del T.C. y T.S. rechazando el criterio penológico en cuanto a catálogo y calificación de delitos en el Código penal y leyes especiales y apuntando al carácter provisional de la calificación de los hechos, a la gravedad del bien jurídico protegido y relevancia social de los hechos, en el momento de la solicitud de la entrada y registro.

En el mismo sentido resoluciones como las de 16 de abril de 2014 de la Audiencia Provincial de Cáceres y 25 de febrero de 2015 de la Audiencia Provincial de Madrid.

Aún cuando es cierto que las sentencias del T.J.U.E. tienen en principio carácter vinculante para los estados miembros, se considera razonable el criterio mantenido por el Ministerio Fiscal, la legislación vigente al tiempo de los hechos cumplía los requisitos que justificaban la resolución, la misma no ha sido directamente anulada y la doctrina del T.S. y T.C. mencionada por la Audiencia Provincial y las resoluciones también invocadas por el Ministerio Fiscal justifican el rechazo de la cuestión planteada.

A parte de ello la cuestión prejudicial como se argumentó por la defensa ya ha sido planteada por otros órganos en otros procedimientos, y su planteamiento en el presente caso que impondría la suspensión del procedimiento se considera generaría una dilación excesiva del mismo, que carece de virtualidad en el presente caso, como luego se razonará.

CUARTO. Se cuestiona asimismo por las defensas la intervención del agente que bajo el pseudónimo de Sprocket se ganó la confianza de alguno de los acusados, llegando a considerar ante la documental relativa a las conversaciones mantenidas con los mismos que estamos ante un delito provocado o ante un agente encubierto que actuó sin autorización judicial.

En el atestado que obra a los folio 1157 y ss al que antes se hizo referencia que se remite por juzgado instrucción nº 44 de Madrid, en fecha 18-5-11 por el Inspector Jefe del Grupo de Seguridad Lógica se refiere que han tenido conocimiento en el rastreo llevado a cabo en la red que a través de diversos videos de youtube, redes sociales y canales de IRC, está prevista la operaciones "V Votaciones", protagonizada por el grupo Anonymous (movimiento de miles de "hacktivistas" que actúa de manera anónima a un objetivo acordado, coordinándose mediante diversos blogs en internet y servidores de IRC (chats) donde ofrecen información sobre a quién y cuándo harán los ataques y herramientas informáticas para efectuarlos) consistente en un ataque DDoS (denegación de servicio distribuida) a páginas webs de los partidos políticos PP, PSOE y CIU a realizar día 20 de mayo de 2011 a las 16,00 horas, que se realiza saturando el ancho de banda de una página web mediante cantidad descomunal de envíos de peticiones ilícitas de otros usuarios dejando la web totalmente inaccesible durante el tiempo que dure el ataque, que para ello el grupo Anonymous se vale de un programa llamado Loic y cuantos más



membros participen más potente es el ataque y más tiempo durará.

Se establece que al tener conocimiento de los canales utilizados para organizarse y perpetrar los ataques, funcionarios adscritos al grupo de la Brigada de Investigación Tecnológica, bajo el pseudónimo SPROCKET se conectan para realizar indagaciones sobre los objetivos de los ataques, infraestructuras y medios de organización, se ganan la confianza del administrador principal del canal llamado Hispania que utiliza el pseudónimo de WICKER que relata que tiene discrepancias con determinados usuarios del canal hispano los cuales habrían montado una red de servidores casera anonhispano 1.dyndins.org desde la que organizarían ataques DDoS, ofrecerían servicios de alojamiento para distribución de malware y páginas sobre operaciones de anonymous, llegando incluso a lucrarse de estas actividades, donde los atacantes se coordinarían y darían instrucciones sobre las mismas a nivel nacional e internacional a través de su servicio de chat.

Asimismo en el atestado obrante al folio 161 y ss de fecha 31-5-11 los funcionarios de la BIT con los números 111.452 y 103.490 relatan en ampliación de informes anteriores, que de las investigaciones en curso por el ataque sufrido a la Junta Electoral Central y de las conversaciones mantenidas en los servidores de chat de las redes Anonworld y Anonnet de las que formaba parte el servidor encontrado en el domicilio de Rodrigo Tuero, dentro del servidor Anonnet se logra establecer contacto y ganar confianza con el usuario que actúa bajo los nicks MUGEN/SERAF, bajo cuya identidad se esconde uno de los principales administradores de los canales de IRC de anonymous junto con el usuario WICKER, donde se ejecutan los ataques que previamente se han planificado y que en última instancia maneja el hive (canal donde los usuarios tienen el programa loic se conectan para que un operador disponga de sus conexiones de internet para efectuar ataques de manera más precisa).

Se añade que se comprueba que la coordinación es gestionada por los usuarios Nicks Seraf y Wicker, que el primero da orden de iniciar el ataque con la orden lazor start, que el 26 de mayo en conversaciones con Mugen Seraf manifiesta que está en Madrid, le proponen citarse para tomar algo, se fija y proporciona el chat número de móvil el funcionario nº 103.490 se desplaza a la Puerta del Sol a las 21,00 horas y dialogan, le dice de ir tomar algo y los agentes 88.018 109.544 y 110.682 proceden a su identificación resultando ser , que luego le dice al agente 103.490 "menos mal que no me han mirado el portátil que si no me llevan cuartelillo" y "tengo en casa un ordenador de sobremesa de refrigeración líquida desde el que también opero".

Se continúa relatando que tras la práctica de gestiones se concierta cita con él el día 31 de mayo de 2011 en Barcelona, y se le detiene por los agentes 103.490 111.452, manifestando el agente 103.490 que es el mismo con el que se había reunido unos días antes bajo el alias Mugen Seraf y Siplas.



Posteriormente consta que por el mismo se le intervienen determinados efectos y que autoriza acudir a su domicilio para la entrega de una torre de ordenador.

Los agentes refieren asimismo en el atestado que de la declaración de resulta que actúa bajo los nicks Mugen, Seraf y Siplas, reconociendo su pertenencia a Anonymous y que participa como administrador del hive junto con el otro usuario Wicker en ataques reivindicados por este grupo.

En oficio de fecha 2-6-11 se refiere que de la declaración de se desprende que son los principales administradores de los ataques DDoS en las últimas semanas, siendo Seraf y Wicker los que coordinan, ejecutan y manejan y que éste último que maneja el programa loic realiza operaciones, busca vulnerabilidades, investiga a otros usuarios, que es el más activo y principal, el que más medidas de seguridad toma y que le facilita el teléfono a siendo el número 6, que se corresponde según respuesta a mandamiento judicial emitido a (folio 217)

Asimismo se refiere que paralelamente a las investigaciones en red por este grupo se corrobora que el usuario registrado en canales de Anonymous con nick Wicker también usa Némesis e Irae, que tiene alta capacidad técnica y que además de coordinar ataques DDoS, ataca de manera individual objetivos que cree hostiles al grupo.

En el plenario compareció el funcionario nº 103.490 que entre otros extremos manifestó que por las denuncias presentadas decidieron utilizar los chats que frecuentaban, monitorizar los servidores y estar presentes en los canales de chat principales en los que se detectaron conversaciones, que detectó bastante actividad en los canales Anonworld y Anonnet y que entró en conversaciones con otros usuarios y mayoritariamente con los que utilizaban los nicks Mugen y Wicker, que quedó con el primero y que también estuvo en su detención y en cuanto a las conversaciones sobre las que fue interrogado en las que él utilizaba el pseudónimo Sprocket precisó que no las recordaba pero que no trataba de incitar la comisión de delitos, sino que eran manifestaciones para ganarse su confianza y utilizaba la misma jerga que ellos.

El funcionario nº 111.452 ratificó los informes aportados y asimismo refirió que aunque el inicio de las investigaciones tuvo lugar a finales de 2010 o principios de 2011 por denuncias del Ministerio de cultura, relacionadas con Anonymous, las operaciones anteriores no se judicializaron o no se pudieron acreditar, pero posteriormente vieron en la red los chats y blogs y apreciaron más actividad, decidiendo la monitorización e intervenir en el chat con pseudónimo, lo que autorizó el declarante dado que les constaban unos servidores, unos administradores que sabían estaban detrás y era la única forma de ganar su confianza e identificarlos, que localizaron la IP en la que resolvía anonhispanol.dyndns.org siendo la misma dirección que la del servido tokorotenn.anonworld.net y solicitaron mandamiento a Telecable en el juzgado de Madrid que facilitó el titular y domicilio y que posteriormente solicitaron en Gijón con urgencia el mandamiento de entrada y registro por constarles que iban a realizar ataques.

El T.S. entre otras en sentencias de 13-5-14, 24-4-15 y 6-4-16 tiene declarado que el delito provocado se integra por





una actuación engañosa del agente policial que supone una apariencia de delito, ya que desde el inicio existe un control absoluto por parte de la policía.

Asimismo se establece que el delito provocado se integra por tres elementos: 1) un elemento subjetivo constituido por una incitación engañosa a delinquir por parte del agente a quien no está decidido a delinquir, 2) un elemento objetivo teleológico consistente en la detención del sujeto provocado que comete el delito inducido, y 3) un elemento material que consiste en la inexistencia de riesgo alguno para el bien jurídico protegido y como consecuencia la atipicidad de la acción.

Supuesto distinto es el de la actividad del agente tendente a verificar la comprobación del delito.

Se sostiene en este sentido que no puede hablarse técnicamente de delito provocado cuando los agentes de la autoridad sospechan o conocen la existencia de una actividad delictiva y se infiltran entre quienes la llevan a cabo, en busca de información o pruebas que permitan poner fin a la actividad delictiva.

En esos casos, los funcionarios policiales no provocan nada, sino que se limitan a comprobar la veracidad de la "notitia criminis", mediante técnicas de investigación, que pueden consistir en la comprobación directa de los hechos denunciados, tratando impedir la continuación del delito, y eventualmente, procediendo a la detención de sus autores, para frustrar nuevas realidades delictivas. No se provoca en estos casos nada que no estuviera ya en la ideación del sujeto activo del delito, sino que se trata de comprobarlo.

En sentencia del T.S. de 6-4-14 con relación al agente encubierto regulado en el art. 282 bis de la L.E.Cr. se establece que las razones que motivan la autorización judicial, radican tanto en las posibles injerencias en derechos fundamentales amparadas en un engaño o simulación; en la afectación de un derecho de nueva generación como es la autodeterminación informativa, así como también en la necesidad de dotar al agente encubierto de *inmunidad en sentido figurado* respecto de actuaciones que objetivamente podrían ser típicas y, por tanto, susceptibles de persecución penal.

Se sostiene sin embargo que las exigencias del derecho a la autodeterminación informativa, concernido de manera determinante, no son tan intensas en cuanto a la necesidad de intervención judicial. No toda incidencia en ese derecho reclama inexorablemente habilitación judicial.

Ciertamente, en teoría es clara la diferenciación entre el delito provocado instigado por la policía, y aquella otra actividad policial tendente a acreditar el delito ya decidido de forma autónoma y libre por la persona concernida reduciéndose la actividad del agente policial a comprobar tal delito.

En la práctica pueden darse situaciones ambiguas, a resolver en cada caso con el estudio de las circunstancias concretas.

En el mismo sentido en sentencia del T.S. de 6-11-13 al referir que las actividades criminales por su complejidad tiene ritmos y tiempo que pueden dilatarse en el tiempo y que demandan un seguimiento previo al objeto de contrastar los datos y de evitar actuaciones precipitadas.





Y que el acercamiento, contacto y diálogo para ganar confianza no son gestiones que necesiten autorización judicial.

En sentencia del mismo Tribunal de fecha 28-6-13 se establece que la existencia de contacto previo puede venir enmarcada en la relación derivada de labores de prevención y captación de formación sin que en principio conlleve una infracción de alcance constitucional,

Se dispone a su vez que no puede pedirse la intervención de agentes a ciegas con exclusión de contacto previo a la autorización judicial.

En las actuaciones dirigidas a la vigilancia, prevención y evitación de ilícitos en las redes informáticas cuya evidencia tiene lugar en fuentes abiertas en la web o canales no cerrados de comunicación, se viene sosteniendo que la ocultación de la condición de agente de la policía haciéndose pasar por un usuario más en la red, en principio no requiere autorización judicial.

En este sentido el T.S. en sentencia de fecha 3-10-2007 al establecer que los agentes de la autoridad cuando realizan labores habituales de vigilancia e investigación para prevenir la delincuencia informática, cuando tienen la convicción de estar ante hechos delictivos, deben confeccionar atestado y la oportuna denuncia.

En sentencia de fecha 14-7-10 en relación a la posible vulneración del secreto de comunicaciones a través de internet, se declara que no puede olvidarse que el acceso a la información puede efectuarla cualquier usuario, no precisando autorización judicial para lo que es público cuando el propio usuario de la red ha introducido dicha información, concluyendo con que la actuación del agente que actuó de forma encubierta haciéndose pasar por un usuario más de la red contactando con el acusado, fue una actuación de investigación lícita.

Sentado lo anterior aún siendo razonables las dudas que se plantearon las defensas sobre dicha cuestión a la vista de los datos obrantes en el atestado, lo cierto es que al margen de la conclusión valorativa que se adopte, no puede considerarse que los hechos objeto de enjuiciamiento se hubieran desarrollado a consecuencia de la iniciativa o sugerencia del agente cuestionado, ni que su actuación hubiera requerido anteriormente de autorización judicial, al tratarse de actuaciones encaminadas a efectuar averiguaciones y a abortar actividad delictiva, habiendo intervenido en todo caso en zonas públicas en las redes sociales, chats públicos en los que todos participan con identidades supuestas, pudiendo por ello participar los agentes en los chats públicos y no necesitando autorización para intervenir y controlar zonas públicas de internet sino en su caso para comunicaciones privadas. En este sentido además de las sentencias antes referenciadas la del T.S. de 6-4-16 invocada por el Ministerio Fiscal.

A parte de ello según obra en autos una vez que los agentes consideraron que dadas las investigaciones practicadas estaban confirmadas sus sospechas y estimaron que ante la información obtenida eran inminentes los ataques denunciados, solicitaron las oportunas autorizaciones judiciales, actuándose en consecuencia e informando del resultado de las mismas.



QUINTO. Se invocó también como se decía anteriormente por la defensa de el incumplimiento de garantías procesales, el rompimiento de la cadena de custodia, la recogida de piezas sin la adecuada custodia policial y judicial y la inexistencia de precintos, concluyendo con que se produjo una manipulación de los efectos intervenidos con vulneración del art. 24 de la C.E. Dicha cuestión fue asimismo planteada por la defensa de y por la defensa

La cadena de custodia viene constituida por los actos de recogida, guarda y traslado de las evidencias obtenidas en el curso de una investigación criminal que garantizan su autenticidad e indemnidad como posible prueba de cargo en el proceso penal y tiene relación con la prueba pericial cuando las mismas son objeto de estudio técnico. La constituyen pues el conjunto de medidas que se deben adoptar a fin de preservar la identidad e integridad de objetos que pueden ser fuente de prueba de hechos objeto de investigación, para garantizar su total eficacia procesal.

El Tribunal Supremo tiene declarado que la integridad de la cadena de custodia garantiza que desde que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio del tribunal es lo mismo.

En sentencia de dicho Tribunal de 8 de junio de 2016 se establece que la regularidad de la cadena de custodia constituye un presupuesto para la valoración de la pieza o elemento de convicción intervenido; se asegura de esa forma que lo que se analiza es justamente lo ocupado y que no ha sufrido alteración alguna (Sentencia del T.S. de 11-12-12). Y en cuanto a los efectos que genera lo que se conoce como ruptura de la cadena de custodia, dicha Sala tiene afirmado que repercute sobre la fiabilidad y autenticidad de las pruebas (Sentencia del T.S. de 28-12-13).

También se ha advertido que la ruptura de la cadena de custodia puede tener una indudable influencia en la vulneración de los derechos a un proceso con todas las garantías y a la presunción de inocencia, pues resulta imprescindible descartar la posibilidad de que la falta de control administrativo o jurisdiccional sobre las piezas de convicción del delito pueda generar un equívoco acerca de cualesquiera datos que resulten decisivos para el juicio de tipicidad. Lo contrario podría implicar una más que visible quiebra de los principios que definen el derecho a un proceso justo (sentencias de 8-11-12 y 14-10-13).

La Ley de Enjuiciamiento Criminal no contiene una regulación unitaria y sistemática sobre los requisitos y garantías de la cadena de custodia, pese a su relevancia para la fiabilidad de las fuentes de prueba, si bien regula de forma dispersa algunos aspectos relativos a esa materia.

Asimismo en sentencia de 26 de marzo de 2013 se establece que ha de estimarse que una infracción menor de la cadena de custodia solo constituye una irregularidad que no determina la exclusión de la prueba del proceso, por lo que debe igualmente ser valorada como prueba de cargo apta para desvirtuar la presunción de inocencia, sin perjuicio de que el defecto apreciado pueda afectar a su poder de convicción o fiabilidad. Por el contrario una infracción mayor o muy relevante de la cadena de custodia debe determinar la invalidez de la prueba, en la medida que su valoración afectaría al derecho a un proceso con las debidas garantías, al no poderse garantizar la autenticidad de la fuente de prueba.

Procede ante las alegaciones efectuadas por dicha defensa y por las defensas de los otros dos acusados, relacionar los distintos efectos intervenidos a los acusados y medidas adoptadas con relación a los mismos.

En primer lugar en cuanto a los efectos intervenidos previa autorización judicial a _____, el día 20 de mayo de 2011 se practica entrada y registro en su domicilio sito en la calle Gijón, por los funcionarios nº 11.452, 103.490 Y 103.017 (folios 32 y ss del tomo I) dando fe la secretaria judicial del juzgado nº 4 de Gijón y en presencia de la madre y abuela del acusado, que manifiestan que el mismo se encuentra embarcado.

En el acta se hace constar que se registra en primer lugar la segunda habitación a la derecha que dicen es la

y se le intervienen diversos dispositivos electrónicos: router Motorola color negro, punto de acceso Wireless Linksys, careta con perilla y bigote, torre de ordenador con pegatina Ubuntu enchufado al cable Mordor, (al tirar de dicho cable se apaga la pantalla del ordenador que estaba encendido el cual queda precintado en este acto, sellado y rubricado), HUB marca Uplink, seis torres más de ordenador de distintas marcas, disco externo Philips, destructora de papel marca Lervia color gris con tapa negra, consola Xbos, router wifi, colador con antena wifi, tarjeta de recarga de teléfono móvil de prepago Lebara, bola de acero con pinchos color negro, CD de Windows mobile correspondiente a un Smartphone y disco externo marca Seagate.

Además de la reseña que se efectúa con relación al ordenador que estaba encendido, se refiere por la secretaria judicial al describir cada dispositivo antes relacionado que queda en este acto precintado, sellado y rubricado y al final del acta se hace constar que todos los objetos intervenidos quedan en poder de la policía a disposición de la autoridad judicial.

En cuanto al acusado _____ consta asimismo que previa autorización judicial mediante resolución de fecha 3 de junio de 2011, se acude al domicilio sito en _____, dando fe el secretario judicial del juzgado de instrucción nº 3 de dicha localidad, (folios 537 a 540) y entre otros los funcionarios 11452 y 103490 que abre la puerta _____, y se procede al



registro interviniendo en la segunda habitación a la derecha la mayor parte de los efectos y el resto en la tercera habitación y en el salón. Así consta que se intervienen siete cables modem de distintas marcas, un disco duro externo iomega, cinco lápices de memoria, Ipod de 8 GB marca Apple con su cargador, PSP Sony, tres CD-Rom, dos DVDs, libreta de anillas rojas con anotaciones y doce posits que se encontraban adheridos a la mesa de ordenador de la habitación a la libreta antedicha introduciéndose una bolsa con la anotación libreta de anillas rojas, catorce folios de distintos tamaños con diversas anotaciones que se introducen en otra bolsa con la inscripción "anotaciones", libreta de anillas rojas con anotaciones y pegatinas y envío de propaganda electoral que se introducen en una bolsa con la inscripción libreta de anillas negras, publicación Hack paso a paso, sello de caucho, navaja tipo mariposa, disco duro externo conceptronic, dispositivo gireles, dispositivo de memoria externa, cámara web negra Microsoft, dos torres de PC una con la inscripción funciona y otra con la de energy system, dos módulos de memoria ram, un modem Adsl y dos ordenadores portátiles uno azul con la inscripción "point of view" en el salón de la vivienda y otro marca Toshiba con su cargador en la segunda habitación a la derecha.

Al final del acta se hace constar "una vez reseñados todos los objetos intervenidos se procede ante mí, el secretario judicial a su precinto con cinta con el anagrama DGP, procediéndose a la firma de todos ellos".

Se hace constar por los funcionarios que elaboran el informe obrante a los folios 222 y ss en el que se relaciona también el material intervenido al referido acusado, que están a la espera de analizar el material informático intervenido.

En cuanto al acusado en el atestado obrante a los folios 161 y ss a que se ha hecho referencia con anterioridad, se hace constar que con ocasión de su detención, que tuvo lugar en Barcelona, en la que intervienen entre otros los agentes 111.452 y 103.490 se le incautan un teléfono móvil Nockia gris, un pendrive Nockia con una tarjeta sd insertada de 2 GB, un ordenador portátil negro marca Packard bell, modelo pe w91 con su cargador, tres folios en blanco y negro impresos con la careta de anonymous y el texto escrito "ellos nos esconden la verdad así que nosotros escondemos sus eslogans" (folio 168).

Se añade que el mismo autoriza la entrada en su domicilio Barcelona y que hace entrega voluntaria del ordenador que tiene en el domicilio siendo una torre de ordenador de color negro marca Thermaltake modelo M5 con refrigeración líquida (folio 178) que queda en depósito en las dependencias de la BIT a la espera de emisión informe si se considera oportuno, constando el acta de entrega al folio 186 en presencia de la madre y hermano de , con intervención de los funcionarios 111.452 y 103.490.

En el folio 178 se hace constar que la torre de ordenador entregada voluntariamente y los demás efectos incautados en el momento de la detención quedan en depósito en las dependencias de la Brigada de Investigación Tecnológica de Madrid a la espera del correspondiente informe pericial por la Comisaría General de la Policía científica si por parte de VI se considera oportuno.





En el atestado en el que se solicita el desprecinto y volcado de todos los efectos intervenidos a los tres acusados, se hace constar al folio 118 que los efectos incautados y el efecto entregado voluntariamente por el acusado

no se encuentran precintados. Dicho extremo se hace constar asimismo en resolución judicial de fecha 15-6-11 en la que se autoriza el desprecinto y volcado solicitado, concretamente a los folios 124 y 125.

Asimismo en la diligencia de efectos incautados a J no consta se hubiera procedido a precinto alguno de los mismos (folio 167).

Sin embargo en el acta de entrega de la torre de ordenador negra Thermaltake, consta al folio 186 que se precinta en dicho acto.

En el acta de desprecinto y volcado practicada los días 6, 7, 11 y 12 de julio de 2011, ante secretario judicial del juzgado de instrucción nº 54 de Madrid, respecto a la torre de ordenador negra Thermaltake no se refiere desprecinto alguno, respecto a un ordenador portátil negro Packard Bell con cinta aislante blanca DGP se refiere que se quita en ese acto, se hace referencia a que hay una caja pequeña de CNP "diligencias nº 1251/10 juzgado uno de Paterna", cerrada con cinta adhesiva blanca DGP que contiene teléfono Nokia IMEI, tarjeta sim, tarjeta sandisk negra y dispositivo Nokia con tarjeta añadida,

Se aportaron asimismo (folios 1.652 a 1.654) fotografías relativas a rueda de prensa emitida por la policía donde aparecen imágenes de material supuestamente incautado a la cúpula de Anonymous en las que aparecen diversos dispositivos con cinta blanca de DGP y se ve un ordenador portátil negro abierto sin que se aprecie en la fotografías si los puertos están sellados y se ve asimismo un teléfono móvil no apreciando que se halle en el interior de caja alguna.

A ello debe de añadirse que en el acta de desprecinto y volcado realizada ante el juzgado de instrucción nº 54 al comienzo de la misma se dispone por el Secretario Judicial "en cuanto a desprecintos, nada cumplía la norma mínima de garantía que pudiera considerar precintado algo, encontrándose las vías de acceso (puertos USB) de las torres, libres y sin tapar".

Sobre los extremos relativos a los precintos poco aclararon los testigos, remitiéndose todos ellos al atestado y refiriendo en relación al acta de entrega voluntaria por parte de en su domicilio en que no recordaban si estaba presente letrado pero que no era necesario y que no recordaban si las tomas de las fuentes de alimentación se precintaron pero que es lo que se hace normalmente, precisando en otros momentos que como fue una entrega voluntaria no era necesario el precinto.

Asimismo todos ellos manifestaron que los dispositivos no los enviaron al juzgado sino que se hizo constar en los atestados relativos cada uno de los investigados que quedaban en custodia en las dependencias de la BIT de Madrid.

Los funcionarios que intervinieron en el primer volcado 107.353 y 112.958 hicieron referencia a que los efectos respecto de los que se hizo el volcado estaban precintados y en cuanto a los puertos o fuentes de alimentación manifestaron que creían recordar que la cinta no permitía el acceso. Asimismo refirieron que en el acta del secretario apreciaron errores entre otros relativos a los datos de precintos y respecto de la caja blanca pequeña que contenía un Nokia en la





que constaba el número de otras diligencias del juzgado de Paterna, manifestaron que estaba cerrada con cinta adhesiva.

Por tanto a la vista de los datos obrantes en el atestado acerca de los dispositivos incautados a los acusados, de los datos reflejados en las actas de los registros en los domicilios de los acusados en el acta de entrega de la torre ordenador por y en la diligencia de intervención del resto de efectos al mismo y del contenido del acta extendida por secretario judicial con ocasión de la realización del primer volcado, se aprecian datos confusos y contradictorios acerca de los precintos no solo de los dispositivos intervenidos a sino también de los incautados a los otros dos acusados, que no fueron aclarados de forma razonable por los funcionarios intervinientes en las distintas diligencias sino que al contrario incurrieron en contradicciones y se apreció confusión en sus manifestaciones, lo que viene a evidenciar que no se han adoptado medidas suficientes para preservar la identidad e integridad de los mismos y por tanto las garantías necesarias en la obtención de dicha prueba de cargo.

Ello debe a su vez de enlazarse con la siguiente cuestión planteada por la defensa de a la que también se adhirieron las defensas de y relativa al quebrantamiento de la fe pública judicial y nulidad de los volcados practicados.

En fecha 26-5-11 se presentó en el juzgado solicitud de desprecinto y volcado de los discos duros contenidos en el referenciado como 4 torre ordenador con pegatina Ubuntu Linux For Muham Beings, que estaba encendido y sería el único que podría albergar información operativa de relevancia para la continuidad de las gestiones de investigación (folio 40) y consta que mediante auto de fecha 27 de mayo de 2011 (folio 46 y ss) se acuerda autorizar dicho desprecinto y volcado y notificarlo en forma a . Al folio 68 consta que se le da por notificado porque se lo ha comunicado su madre y se le cita por el juzgado para declarar.

En fecha 15-6-11 se presenta escrito en que argumentando que fue solicitada la práctica del desprecinto y volcado en el en el juzgado nº 42 de Madrid pero que como no figuraba fecha y hora, pasó el plazo y se devolvió y dada la urgencia que ya no justifica el desprecinto y volcado de un solo equipo, se solicita el desprecinto y volcado de todos los efectos intervenidos a los tres investigados (folios 116 Y SS), lo que según obra al folio 121 fue autorizado mediante auto de fecha 15-6-11. En el mismo la magistrada acuerda la apertura, copia y volcado a practicar el día 2 de junio de 2011 en las dependencias de la BIT para acceder al estudio de la documentación incautada por parte del CNP y la emisión de posterior informe, añadiendo que la apertura, copia y volcado se realizará a presencia del secretario judicial de guardia que levantará acta de su desprecinto e identificará el material que bajo su fe pública será copiado, así como en presencia de los interesados y por los funcionarios del CNP nº 112.958 y 121.666.

Contra el auto de 15 de junio de 2011 se interpuso recurso por la representación de .

Consta que se cita a los investigados en diligencia obrante al folio 812 y que pueden asistir representados, se





facilitan los teléfonos por la policía y se remite citación, constando al folio 817 que en fecha 30 de junio de 2011 solo se contacta con _____ y no con los otros investigados al saltar el buzón de voz.

Se libró exhorto que fue turnado al juzgado de instrucción nº 54 de Madrid (folios 807 y ss) para proceder a la apertura y análisis de los datos informáticos intervenidos a los acusados en presencia de los funcionarios de la BIT.

A los folios 831 y ss figura acta extendida por el Secretario judicial de dicho juzgado correspondiente a la diligencia realizada los días 6, 7, 11 y 12 de julio de 2011, en la que consta que intervienen entre otros los funcionarios 107.353 112.958 y los letrados de Rodrigo Tuero y José María Zaragoza.

Comienza el secretario judicial afirmando "el método de trabajo consistirá en dejar constancia de las nuevas operaciones de enganche de cableado pues de nada más puedo dar fe, ya que ni puedo comprobar el contenido de los discos duros intervenidos ni los discos que aporta la policía y manifiesta cosa que no sé, que están en blanco, no puedo por tanto dar fe de nada y menos de que se hayan volcado datos de un sitio a otro, puesto que ni tan siquiera puedo comprobar que estos existieran, en cuanto a desprecintos decir que nada cumplía la norma de garantía que pudiera considerar precintado algo, encontrándose las vías de acceso, puertos usb de las torres, libres y sin tapar.

Solamente recogeré según dice la policía "Nº Hush" lo que aparece en las pantallas de las máquinas que los agentes dicen ser clonadoras pero que yo no sé si lo son por carecer de conocimientos, el método será hacer constar número serie de discos intervenidos (según la policía) número de serie de máquina a la que se enganchan cables y número de serie de discos que aporta la policía, manifestando que están en blanco, cosa que ni sé, ni puedo comprobar. Por tanto no me consta la existencia de datos ni menos que se hayan copiado".

En fecha 3-10-11 se dicta auto desestimatorio del recurso de reforma interpuesto por la representación de _____ contra el auto de 15-6-11 que autorizó el desprecinto y volcado (folio 998) y en fecha 15-2-12 se desestimó el recurso de apelación interpuesto contra el mismo por la Audiencia Provincial (folios 1070 a 1072).

Según consta a los folios 952 y ss por los funcionarios de la Secretaría Técnica de la BIT se remitió en fecha 9-8-11 informe técnico de errores del volcado realizado, en el que consta que recibida acta del juzgado de instrucción de Madrid nº 54 se aprecian diferentes errores por lo que se procede a cotejarla por los funcionarios actuantes durante el proceso de clonado con los logs generados en las máquinas clonadoras y una vez analizada el acta en profundidad y viendo la seriedad de los errores encontrados, se decide realizar el informe técnico de errores, realizando imágenes de los discos intervenidos durante los registros, relacionando a continuación los diversos errores.





Al folio 1024 obra oficio del Inspector Jefe del Grupo de Seguridad Lógica de fecha 1-11-11 en el que insistiendo en los errores apreciados se solicita nuevo volcado o directamente en ese nuevo volcado se realice un informe pericial sobre los dispositivos originales intervenidos o si no se considera necesario el nuevo volcado, en su caso análisis de la información obtenida tras la práctica del desprecinto y volcado realizado en su día, y en su caso se autorice la realización del desprecinto de la destructora de papel intervenida en el domicilio de Rodrigo Tuero realizándose reportaje fotográfico para reconstruir en la medida de lo posible los documentos más significativos para la instrucción.

Previo informe del Ministerio Fiscal a favor del nuevo volcado, se autorizó el mismo mediante auto de fecha 16-4-12 (folio 1077), contra el que se interpuso recurso de reforma por la representación de al que se adhirió la representación de y que fue desestimado mediante de fecha 23-8-12 (folio 1107).

En el auto de 16-4-12 se resuelve que se autoriza la apertura y análisis de todos los efectos intervenidos a los investigados por parte de los funcionarios de la policía nacional 112.958 y 121.666, que la apertura y volcado acordada se practicará en las dependencias de la BIT citándose a los representantes legales de y , y que tiene por objeto el que se pueda acceder al estudio de la documentación incautada por parte del CNP y la emisión del posterior informe.

Se añade que la apertura, copia y volcado se realizará a presencia del secretario judicial de guardia que levantará acta identificará el material que bajo su fe pública será copiado así como en presencia de los interesados y por los funcionarios del CNP indicados.

Entre los argumentos expuestos para justificar la denegación de los recursos contra el nuevo volcado, se refiere que la presencia de secretario judicial no es imprescindible en diligencias de volcado de acuerdo con jurisprudencia del T.S. y T.C. y que no obstante se acordó el primer volcado en presencia de fedatario judicial para una mayor garantía.

En fecha 17 de abril de 2012 se dictó providencia autorizando el desprecinto de la destructora intervenida en el domicilio de y la reconstrucción de los documentos por parte de los funcionarios del CNP mediante acta con reportaje fotográfico para reconstruir en la medida de lo posible los documentos que parecieran significativos para la instrucción de la causa.

El exhorto fue turnado al juzgado de instrucción nº 16 de Madrid, constando a los folios 1121 y ss cédulas de citación a los acusados y sus representantes de fecha 16-5-12 para la apertura, copia y volcado y desprecinto de la destructora de papel intervenida en el domicilio de y reconstrucción de los documentos por parte de los funcionarios de la CNP.





La diligencia de volcado acordada mediante auto de fecha 16 de abril de 2012 y la decretada mediante providencia de fecha 17 de abril de 2012, se practicó en el juzgado de instrucción nº 16 de Madrid en fecha 30 de mayo de 2012, con asistencia del Secretario Judicial y estando presentes el letrado de Rodrigo Tuero, y los policías 120.932 107.353, 112.958 103.490 103.017 (folios 1125 y ss).

En el acto del juicio los funcionarios que intervinieron en el primer volcado manifestaron que se procedió al desprecinto de equipos informáticos, extrajeron los discos duros de esos dispositivos, dijeron los números de serie de esos dispositivos al Secretario y realizaron el volcado, cuya realización consiste en que mediante máquinas forenses conectan los discos duros originales a las máquinas y se realiza copia de bit a bit a un medio en otros discos duros que aportaron, en el proceso la máquina clonadora registra la operación con un log y el nº Hush acredita la identidad del disco con el original. En cuanto a la posible alteración de los datos manifestaron que se vuelcan a un fichero y ese sí se puede alterar pero que eso se podría comprobar.

Manifestaron que normalmente el secretario toma nota en el acta y como hay muchos números y letras ellos van cotejando con las notas del secretario, que en este caso el secretario no quiso cotejar, que fue tomando nota manuscrita y cuando el volcado finalizó no pudieron cotejar el acta, se envió a las dependencias y vieron numerosos errores, fueron al juzgado a contrastar el acta y el secretario no accedió al cotejo, y que se apreciaron incluso errores en el número de los agentes y en los datos de precinto, refiriendo que sobre los efectos que se realizó el volcado estaban precintados, y no recordando este extremo respecto de los puertos usb o fuentes de alimentación.

Los funcionarios que intervinieron en el segundo volcado no aclararon extremos como el de que en el primer volcado constara que se extraían dos discos duros de la CPU de color negro intervenida a uno de los acusados y en el segundo se extraen tres discos duros y tampoco que se aludiera al desprecinto del portátil Packard Bell a que no se hizo referencia en la primera diligencia. Asimismo tampoco aclararon extremos como los relativos a las horas de análisis de los dispositivos consignados en las pantallas, anteriores a la hora de comienzo de la segunda diligencia.

Desde el principio llamó la atención de la juzgadora el contenido del texto con el que el Secretario Judicial que asistió al primer volcado comenzó el acta describiendo el método de trabajo y el estado de los dispositivos intervenidos.

Al respecto debe de significarse que el art. 453 de la LOPJ establece que corresponde a los Secretarios Judiciales, (actualmente Letrados de la Administración de Justicia), con exclusividad y plenitud el ejercicio de la fe pública judicial y que en el ejercicio de esa función, dejarán constancia fehaciente de la realización de actos procesales en el Tribunal o ante éste, y de la producción de hechos con





transcendencia procesal mediante las oportunas actas o diligencias.

Es cierto que los funcionarios que intervinieron en dicho volcado y que emitieron posteriormente el informe de errores, solicitaron que se procediera al nuevo volcado de los datos de los efectos intervenidos, o directamente dado el número de errores e inexactitudes apreciadas en el acta de volcado se realizara un informe pericial sobre los dispositivos originales intervenidos en las entradas y registros practicadas por la policía o en su caso si no se consideraba necesario un nuevo volcado, se procediera al análisis de la información obtenida tras la práctica del desprecinto y volcado por el juzgado nº 54 de Madrid, y en y que previo informe del Ministerio Fiscal, se acordó por la magistrada instructora mediante resolución de fecha 16-4-12 un nuevo volcado, resolución que fue recurrida en reforma y cuyo recurso fue desestimado.

No puede acogerse sin embargo el argumento del Ministerio Fiscal para prescindir del contenido del acta del primer volcado y dar plena validez al segundo volcado, de imputar a las defensas no haber solicitado un análisis sobre la posible manipulación de los dispositivos o que no hubieran propuesto una contra pericial en primer lugar porque la prueba de cargo corresponde a las partes acusadoras y en segundo lugar porque las defensas no solo formularon recursos contra las resoluciones que acordaron los dos volcados, sino que tanto la defensa de [redacted] como la defensa de Y

[redacted] aportaron en su momento informes periciales contradiciendo entre otros extremos los informes emitidos por la BIT acerca de los dispositivos intervenidos a ambos acusados.

Y concretamente el perito D. Josep Lluís Ferrer Gomila, refirió en su informe obrante a los folios 1702 y ss y ratificó en el plenario la gran susceptibilidad de manipulación de los dispositivos informáticos y la dificultad y en ocasiones imposibilidad de detectar dicha manipulación, considerando recomendable realizar un volcado de la información contenida en los soportes a otros de carácter temporal que no permitiera la manipulación intencionada o accidental de los originales, para poder verificar siempre la coincidencia de la copia con el original realizando un resumen digital de la información que debería coincidir en los dos soportes, dado que si se manipula un solo bit de alguno de los soportes el resumen ya no coincidirá. Se manifiesta por el perito que a la vista del informe de fecha 9-8-11 el volcado de la información de los objetos incautados no fue realizado de manera adecuada dado que no coinciden los resúmenes del secretario judicial que dan garantía de que la información contenida en el dispositivo original y la volcada en un dispositivo secundario coinciden y no han sido modificadas y si se trataba de dar fiabilidad a la prueba informática, en todos los dispositivos en que no coinciden los resúmenes indicados por el Secretario y la BIT se habría perdido la fiabilidad.

Sobre este extremo fueron interrogados los funcionarios 107.353 y 112.958 que como se decía anteriormente tras describir el procedimiento empleado en el primer volcado en que intervinieron, al ser preguntados sobre si los datos se podían alterar, manifestaron que los datos se volcaban a un



fichero y ese si se podía alterar pero que no se podía comprobar.

Pese a que la resolución judicial de fecha 16-4-12 conforme a lo solicitado por la BIT y a lo dictaminado por el Ministerio Fiscal autoriza el segundo volcado y la resolución fue ratificada con fundamento entre otros en la no necesidad de secretario judicial, ello no impide la valoración por la juzgadora de las afirmaciones contenidas al inicio del acta de la primera diligencia pues aunque el TS y el TC no consideren necesaria la presencia de secretario judicial en diligencias de volcado por carecer de conocimientos técnicos, en el caso de autos tanto en la resolución que autorizó el primer volcado y que fue confirmada tras la interposición de recursos de reforma y apelación, como en la que autorizó el segundo volcado, se acordó la asistencia de secretario judicial "para mayor garantía", por lo que si se acuerda su intervención para mayor garantía no se puede después ignorar lo que el fedatario hace constar y que revela una clara discrepancia con lo que declaran los agentes en extremos no solo relativos a los datos de volcado sino también en extremos relevantes para el enjuiciamiento de los hechos que no requieren de especiales conocimientos técnicos como el tema de precintos.

El propio Ministerio Fiscal admitió en su informe que se pudo incurrir en falta de diligencia o que se pudieron cometer errores, considerando no obstante que no se vulneró derecho fundamental alguno lo que no se comparte por la juzgadora.

Pese a que el T.S. tiene declarado entre otras en sentencias de 7-7-10 y 26-4-16 que no basta la mera sospecha sino la evidencia de la ruptura de la cadena de custodia, en el presente supuesto la confusión y contradicción apreciadas acerca de la adopción de garantías suficientes para preservar la identidad e integridad de los efectos incautados a los tres acusados y sobre la posible manipulación o contaminación de los mismos, exceden como se decía anteriormente de la mera sospecha y vienen a evidenciar la ruptura de la cadena de custodia y asimismo exceden de la mera irregularidad o infracción menor a que se refiere la jurisprudencia más reciente y valorados los datos relativos a los efectos incautados y las medidas adoptadas respecto de los mismos en relación con los datos relacionados acerca de los volcados de datos, las manifestaciones efectuadas por el secretario judicial con ocasión del primer volcado en clara contradicción con las de los testigos y peritos que elaboraron los informes de errores y solicitaron y practicaron un nuevo volcado, los defectos de forma apreciados con ocasión de la citación de los investigados, las contradicciones acerca de los efectos examinados en relación con el anterior volcado incluso relativas al número de efectos examinados, y las afirmaciones relativas a que no se examinan determinados dispositivos por carecer de interés, etc que no fueron debidamente aclarados en el plenario por los testigos y peritos, se considera que debe acogerse la cuestión invocada por las defensas por estimar que se produjo la vulneración del derecho a un proceso con las debidas garantías y en consecuencia del derecho de defensa y el derecho a la tutela judicial efectiva consagrada en el art. 24 de la C.E. en contra de lo que sostiene el Ministerio Fiscal y en consecuencia prescindir de la prueba relativa a los efectos incautados a los acusados y la prueba de análisis de los mismos que de ella trae causa.



SEXTO. Prescindiendo de las pruebas relativas a los dispositivos incautados a los acusados y las periciales que de ellas traen causa, contamos con prueba documental, testifical y con las declaraciones de los acusados.

Como se decía anteriormente en los razonamientos referentes a las cuestiones previas planteadas, se incorporaron a los autos diversos atestados e informes remitidos por la Brigada de Investigación Tecnológica. Así, a los folios 1 y ss obra atestado de fecha 20 de mayo de 2011 en el que por los funcionarios nº 11.1452 y 103.017 se solicita la entrada y registro en el domicilio de [redacted] ero, a los folios 71 y ss obra atestado de fecha 31-5-11 en que por los funcionarios 111452 y 103490 dando cuenta de las diligencias de investigación llevadas a cabo en los canales de chat, se solicita la intervención del teléfono de [redacted] a los folios 161 y ss obra atestado de fecha 31-5-11 en que los funcionarios 111.452 y 103.490 informan de las diligencias practicadas y detención de [redacted], a los folios 212 y ss obra informe de fecha 2-6-11 en que por el Jefe del Grupo de Seguridad Lógica se solicita entrada y registro en el domicilio de [redacted] sobre la base de las declaraciones de [redacted], las capturas de pantalla realizadas y las investigaciones llevadas a cabo en la red y a los folios 222 y ss atestado de fecha 4-6-11 en que por los funcionarios 111.452 y 103.490, se da cuenta de la detención de [redacted]. Asimismo a los folios 1158 y ss obra informe de fecha 18-5-11 del Inspector Jefe de Seguridad Lógica sobre solicitud de mandamiento a Telecom para la IP 93.156.74.169 y a los folios 876 y ss oficio del Inspector Jefe de Seguridad Lógica de fecha 4-8-11 informando acerca de los días que [redacted] estuvo embarcado.

En los mismos se establece que el colectivo Anonymous está constituido por una pluralidad de usuarios informáticos, tanto de España como de otros países, que actúa anónimamente y de forma coordinada hacia un objetivo acordado generalmente, siendo su pilar básico entre otras actividades, la organización de ataques de Denegación de Servicio Distribuido denominados ataques DDoS que consisten en la saturación de un entorno informático o de una página web, mediante múltiples peticiones simultáneas, de tal forma que no tiene capacidad suficiente para responder, se colapsa y queda sin funcionamiento e inaccesible para los usuarios.

Se establece que para la realización de dichos ataques el colectivo utiliza una herramienta informática llamada LOIC y que la coordinación de los diversos usuarios intervinientes en los ataques la realiza a través de los diversos blogs de internet y sus redes de servidores de IRC chats, en los que fijan los objetivos y se facilitan herramientas informáticas y los usuarios se conectan para que un operador gestione sus conexiones haciendo de esta forma que el ataque sea más efectivo. Y ello por cuanto cuantos más miembros participen en el ataque más potente será y más durará el mismo.

Se refiere que los servidores ofrecen diversos canales que entre los más frecuentados está el canal Hispania, que las redes de IRC utilizadas para organizarse y perpetrar los





ataques son: Irc.anonworld.net, irc.anonops.li y irc.anonnet.org, siendo la primera la única con capacidad de ataque y la que más actividad registra, formada por los siguientes servidores: remanon.anonworld.net, gatomon.anonworld.net y Tokorotenn.anonworld.net,

Asimismo se hace constar que en España dicho colectivo ha reivindicado diversos ataques como la Operación contra la ley Sinde, Operación Hipoteca, contra las páginas webs de partidos políticos, de la SGAE, el congreso, Ministerio de Cultura, Ministerio de Trabajo, Senado y academia de cine, y contra las páginas webs de principales entidades financieras españolas.

Como también se reseñaba anteriormente en dichos informes con ocasión de la solicitud de diversos mandamientos judiciales se establece que en el rastreo llevado a cabo en la red se tuvo conocimiento de que estaba prevista la operación "V Votaciones" protagonizada por el grupo Anonymous, actuando coordinados mediante diversos blogs en internet y servidores de IRC ofreciendo información sobre la forma de realizar los ataques consistentes en ataques DDoS a páginas webs de partidos políticos mediante el envío masivo de peticiones ilícitas y que dado que tenían conocimiento de los canales utilizados, se asignó a un funcionario del grupo para investigar entrando en conversaciones con los mismos y ganando la confianza del administrador principal del Canal Hispania, que utiliza el pseudónimo Wicker que relata las discrepancias con los usuarios del canal hispano que montaron una red de servidores casera anonhispano.1.dynds.org desde la que organizan ataques DDoS ofrecen servicios de alojamiento y se coordinan y dan instrucciones sobre las mismas a nivel nacional e internacional.

Se refiere que les constan entre once líderes que tienen tareas diferenciadas, uno de ellos Devnuller se encarga de la creación de páginas webs relacionadas con Anonymous siendo la principal Anonymous spain.com y el resto a la creación y mantenimiento de los servidores, que se comprueba como a través de esta página web anonhispano.dyndns.org se está resolviendo en la misma dirección IP 93.156.74.169 que el servidor tokoroten.anonwordl.net que se identifica pertenece al domicilio de , con correo de contacto mordor.telecable.org.

Asimismo se relata que en fecha 18 de mayo comienza la operación Spanish Revolution, el ataque a DDoS a la página de la Junta Electoral Central dejándola inaccesible, estando activo a primeras horas de la mañana y que fue alentado desde el servidor IRC anonworld.net.

Como también se ha expuesto anteriormente, se refiere que tras recabar mandamiento a Telecable se informa que la conexión ha sido realizada utilizando la línea telefónica del domicilio sito en la calle

, constando empadronado en el mismo Sala, el más activo conocido con el nick Tuerinator asociado a la cuenta de correo bajo el cual se hace referencia a ataques contra servicios informáticos, que el servidor de chat Tokoroten. Anonworld.net fue utilizado para



organizarse, reunirse, coordinarse y perpetrar el ataque a la Junta Electoral Central, siendo el domicilio de la calle 17 agosto el utilizado anteriormente contra distintas páginas web y convocados contra las páginas del PSOE, PP y CIU para el día 20 por lo que se solicitó la entrega y registro para acceder a los equipos informáticos.

Asimismo se informó de que sobre las 12,30 horas del día 21 de mayo de 2011 al consultar el perfil Tuerinator en twitter donde figuraba una foto del mismo, el mismo había sido borrado

En informe obrante a los folios 100 y ss por el inspector jefe del grupo de la BIT se hace constar que tras el análisis de los logs de los servidores del chat que han ido monitorizando, se concluye con que el usuario con el nick Devnuller es y se hace referencia a la imagen del mapa de red que figuraba al acceder al servidor

en la IP antes reseñada donde figura que dispone además del material intervenido de un portátil y agenda electrónica, a que en atestado 2897/07 de la comisaría de Gijón consta interpuso denuncia por sustracción de una PDA, de la que se aporta copia (folio 210) coincidente con la que está en esquema de red, y a que en conversaciones con el mismo hace referencia a su página de nodos de tor, que al ser consultada poniendo la dirección de IP del servidor hallado en su domicilio, sale reflejado como tal.

Se manifiesta que aunque en el momento del registro no estaba en Gijón, sino embarcado en Almería, el servidor instalado en el domicilio de estaba permanentemente conectado a la red para dar cobertura y servicio a todas las operaciones de ataques DDOS, que les constaba que tenía acceso a internet y se adjuntó declaración de director de recursos humanos de la empresa Remolques Marítimos S.A. para la que trabaja el mismo.

Consta asimismo que paralelamente se solicitó la intervención, grabación y escucha del número de teléfono del que Rodrigo Tuero es usuario, IMEI al que se encuentra asociado desde enero y el listado de llamadas entrantes y salientes con identidad de titulares y usuarios, en su caso operadora a la que pertenecen y posicionamiento del repetidor al que da cobertura, intervención que fue autorizada mediante resolución de fecha 21-5-11 y se decretó su cese en fecha 7-6-11, obrando al folio 109 y ss de la pieza separada resumen de las mismas.

Asimismo en fecha 22 de mayo de 2011 haciendo referencia a un ataque que sufrió uno de los miembros de Anonymous Ryan, y a que cotejada al lista que publica el mismo con los miembros de canales de IRC que han estado monitorizando aparecen nicks de administradores de canales y servidores en España, Pacotron, Mugen Seraf, Pikaro, Neuro-Risper, de los que se reseñan las distintas direcciones de IP, se refiere que se solicitó mandamiento a distintas operadoras para que se aportaran los datos de las mismas dictándose auto en fecha 24-5-11 en el que se acordó librar los oportunos mandamientos y

obrando a los folios 130 y ss las contestaciones de las operadoras, no correspondiendo ninguna de las IP referidas a los acusados.

Se informa asimismo de que de las declaraciones de se desprende que el administrador de los ataques DDoS denunciados tiene los alias Wicker y Némesis con número de teléfono y se solicita mandamiento de la titularidad desde uno enero 2011 listado llamadas entrantes y salientes y listados de sms entrantes y salientes que fue autorizado por el juzgado, habiéndose aportado en la pieza separada resumen de conversaciones de las que se solicitó en su momento el desglose y devolución de conversaciones mantenidas con el letrado de .

Por otra parte como se ha expuesto anteriormente en el atestado obrante al folio 161 y ss se hace constar que de las investigaciones en curso por el ataque sufrido a la Junta Electoral Central y de las conversaciones mantenidas en los servidores de chat de las redes Anonworld y Anonnet de las que formaba parte el servidor encontrado en el domicilio de , dentro del servidor Anonnet establecen contacto y ganan la confianza del usuario que actúa bajo los nicks MUGEN/SERAF, bajo cuya identidad se esconde uno de los principales administradores de los canales de IRC de Anonymous junto con el usuario WICKER, donde se ejecutan los ataques que previamente se han planificado y que en última instancia maneja el hive (canal donde los usuarios tienen el programa loic se conectan para que un operador disponga de sus conexiones de internet para efectuar ataques de manera más precisa.

Refieren que se comprueba que la coordinación es gestionada por los usuarios Nicks Seraf y Wicker, dando el primero la orden de iniciar el ataque con la orden lazor start, introduciendo en el informe capturas de pantalla de los hechos relacionados.

Se relata asimismo la cita en Madrid por el funcionario 103.490 con el que resulta ser que le manifiesta tras la identificación policial "menos mal que no me han mirado el portátil que si no me llevan cuartelillo y tengo en casa un ordenador de sobremesa de refrigeración líquida desde el que también opero", y tras referir que posteriormente se citan en Barcelona donde se procede a su detención y el funcionario 103.490 lo identifica como el mismo con el que se vio en Madrid, se le intervienen los efectos anteriormente reseñados.

Aluden asimismo a los datos que resultan de su declaración de dicho acusado tanto respecto a su pertenencia a Anonymous como a su participación como administrador del hive junto con el usuario Wicker entre otros en el ataque a la Junta Electoral y a los efectos que entrega voluntariamente.

Se reseña que de las declaraciones de se desprende que respecto de la red Anonnet de la que es operador y administrador de los ataques otra persona que está con él en todos los ataques es Wicker, siendo los dos los que deciden objetivos y duración de los ataques y coordinan y ejecutan y que asimismo hace referencia a numerosos miembros coinciden con los administradores y usuarios de canales que el



grupo se encuentra monitorizando por ser los utilizados para ataques DDoS.

Sobre la base de que el administrador que aparece en ataques DDoS es el que tiene los alias Wicker o Némesis, se entregan CDs con conversaciones de chat de los que se mete reseña, se dice que tiene el móvil número y se solicita mandamiento y mediante providencia de fecha 1-6-11 se accede a ello (folio 90), obrando a los folios 91 y 92 mandamiento de fecha 1-6-11 a telefónica Movistar solicitando datos del titular y listado de llamadas entrantes y salientes entre 1 de enero y la fecha de la solicitud.

Se refiere que paralelamente a las investigaciones en red por ese grupo se corrobora que el usuario registrado en los canales Anonymous con nick Wicker también usa Némesis e Irae, que tiene alta capacidad técnica y además de coordinar ataques DDoS, ataca de manera individual objetivos que cree hostiles al grupo, y que en la declaración de José María Zaragoza refiere que es uno de los administradores principales que maneja el loic y operaciones, busca vulnerabilidades, investiga a otros usuarios, es el más activo y principal, el que más medidas de seguridad toma.

Se añade que el mismo le proporciona el teléfono a José María con el número , que se corresponde según respuesta a mandamiento judicial a

y se añade que en el registro efectuado en dicho domicilio se le interviene un portátil con el número de teléfono de Mugen que coincide con

Se informa por otra parte al folio 230 y ss tras detención de , sobre la división interna entre administradores de Anonymous en abril 2011, en dos redes: red ANONWORDL en la que se coordinan ataques protagonizados en Sudamérica contra intereses españoles como la Junta Electoral Central y partidos políticos estando alojado uno de los servidores de la red Tokoroten en domicilio de alias Tuerinator y Devnuller que según consta en declaración de está al corriente y participa activamente en los ataques y red ANONNET que surge tras escisión de algunos de miembros de Anonworld siendo uno de los dos administradores que participa en el reciente ataque a la Junta Electoral Central, mossos de escuadra y UGT, administrando el hive junto a él el usuario Wicker Némesis y antes Irae, que es

Respecto de éste se establece que este administrando el hive en el ataque a la Junta Electoral Central siendo su intervención directa controlando el canal y que utiliza medios sofisticados para evitar ser descubierto, que crea malware indetectable por antivirus para infectar ordenadores sin consentimiento de usuario y dispone de herramientas diseñadas para cometer fraudes o penetrar ilícitamente en redes ajenas porque en domicilio no existe conexión a internet propia y que es un experto programador, consigue programas maliciosos indetectables para antivirus, actividad conocida como fud para infectar ordenadores y controlarlos.

Concluyen con que es el cabecilla de la red Anonnet de Anonymous en España que ha participado, gestado y promovido al menos los ataques a página de congreso, UGT, mossos y JEC, y su actividad va mas allá de administrador de los ataques con utilización programa loic.





Se remitieron oficios informando del resultado de conversaciones telefónicas y de resumen de conversaciones de chats.

Se adjuntaron asimismo pantallazos de las conversaciones mantenidas por el agente Sprocket, entre otras las siguientes: a los folios 162 y 163 pantallazo en el que se reseña que la coordinación de hive la gestiona Mugen/Seraf, al folio 163 en el que siendo el objetivo el ataque a la Junta Electoral Central da la orden Seraf, al folio 164 conversaciones entre Sprocket y Mugen, al folio 209 conforme a consulta de los nodos de tor en que se refleja que poniendo la IP de Rodrigo Tuero, sale como estatus, al folio 232 conversaciones con Wicker, al folio 232 conversaciones con Némesis, al folio 234 en que Wicker dice que tiene 3 a 3000 bots repartidos por Europa en un botnet tipo Zeus, al folio 236 en que consta ayudando a hacer fud sus bots para que no se detecten y programar mejor, al folio 465 pantallazo de conversación con Wicker en que aparece como administrador con la IP 93.156.74.169 y como datos contacto asociado al perfil de twitter Tuerinator, al folio 466 el día 18 de mayo coincidiendo con el ataque de la comisaría especial del Congreso de los Diputados, en el twitter de se hacen referencias explícitas al ataque a la página de la Junta Electoral Central, y al folio 467 en que consta el uso de la frase en su perfil de twitter "el conocimiento humano pertenece al mundo" la misma que los agentes refieren que aparece en las conexiones a servidores de chat de Anonworld Anonnet emplea el usuario con el nick Devnuller.

Por otra parte se aportaron los oportunos informes técnicos sobre los dispositivos intervenidos a los acusados de cuya valoración se prescinde y el inspector jefe del grupo de seguridad lógica en fecha 2-9-13 con ocasión de la remisión del último de dichos informes, según obra a los folios 1300 y ss emite informe en el que sobre la base de las evidencias encontradas y reseñadas en los informes, de cuya valoración se prescinde, concluye con la pertenencia de los acusados en el grupo Anonymous y la participación en los hechos objeto de acusación.

En definitiva se sostiene por los funcionarios de la BIT que los acusados

y z formaban parte del colectivo Anonymous y que además de tener prevista para el día 20 de mayo de 2011 a las 16,00 horas la operación V de Votaciones contra las páginas webs de los partidos políticos PSOE, PP y CIU, que no llegó a realizarse por la intervención policial, participaron el día 18 de mayo de 2011 bajo el nombre de operación Spanish Revolution en el ataque DDoS a la página web de la Junta Electoral Central, a la página web de la Unión General de Trabajadores y la del Congreso, precisando que el ataque fue dirigido y coordinado a través de la red irc.anonworld.net, compuesta por los servidores renamon gatomon y Tokoroten, y siendo éste último servidor que resolvía en el domicilio de el que se utilizó para organizar y coordinar el ataque a la junta, que para ello utilizaba la cuenta de correo y los nicks de Tuerinator y Devnuller, creando una red de servidores casera, anonhispanol.dndns.org que resolvía en la misma IP y que la coordinación y dirección se realizó también a través del servidor de chat Anonnet. Asimismo se sostiene que el acusado





con los nicks Mugen, Seraf y Siplas era uno de los principales administradores del canal Anonnet donde se ejecutaban los ataques previamente planificados, y que manejaba el hive, canal a través del cual los usuarios que tenían el programa Loic se conectaban para ejecutar los ataques de forma más precisa, que prestaba asesoramiento a otros usuarios para tomar medidas de seguridad e impedir la identificación y que coordinó el ataque a la junta dando la orden de iniciación y que el acusado que utilizaba los nicks Wicker, Némesis e Irae, era otro de los principales administradores del canal de Anonymous Anonnet, en el que ese ejecutaban los ataques planificados, que gestionaba los servidores, creaba y regulaba canales de chat y fijaba objetivos y analizaba las vulnerabilidades de las páginas web para facilitar los ataques y dirigir los ataques planificados, habiendo actuado como administrador del hive durante el ataque a la junta electoral central.

Se aportó por otra parte por la defensa de Sala copia de atestado incorporado a Procedimiento Abreviado nº 61/14 del juzgado de instrucción nº 7 de Toledo de fecha 18-11-13 en el que se hace referencia a que el Grupo Anonymous no es un grupo cerrado en sí sino que existen multitud de células repartidas por todos los países del mundo, las cuales no tienen que conocerse o coordinarse para llevar a cabo sus actos reivindicativos, más bien cada célula decide los objetivos a atacar, normalmente páginas web de partidos políticos o ideologías contrarias a la suya. Pese a que entre los integrantes del grupo se encuentran personas con altos conocimientos informáticos, la gran mayoría son personas con nociones básicas de informática, normalmente jóvenes, afines a la ideología de este grupo, que colaboran de forma desinteresada a la hora de efectuar estos ataques, existiendo por otra parte gran número de personas afines a Anonymous que aunque difunden su ideología lo hacen sin cometer ningún hecho delictivo, por lo que no se puede asociar Anonymous a una organización criminal, sino a una organización de personas con ideales más o menos afines de las cuales algunas de estas personas deciden cometer actos delictivos para reivindicar su forma de pensar y otras no.

En el acto del juicio comparecieron los funcionarios nº 103.490, 111.452 y 103107 que comenzaron ratificando los informes obrantes en autos y sus respectivas intervenciones y asimismo que les constaban las conclusiones del informe respecto del colectivo Anonymous cuya copia aportó la defensa

El funcionario 103.490 como se decía anteriormente entre otros extremos manifestó que por las denuncias presentadas decidieron utilizar los chats que frecuentaban, monitorizar los servidores y estar presentes en los canales de chat principales en los que se detectaron conversaciones, que detectó bastante actividad en los canales Anonworld y Anonnet y que entró en conversaciones con otros usuarios con el pseudónimo Sprocket y mayoritariamente con los que utilizaban los nicks Mugen y Wicker.

Como se reseñó anteriormente no recordó ninguna de las manifestaciones efectuadas por él mismo sobre las que fue interrogado en las que utilizaba el pseudónimo Sprocket pero refirió que no trataba de incitar la comisión de delitos, sino que en todo caso eran manifestaciones para ganarse la



confianza de los investigados y utilizaba la misma jerga que ellos.

Refirió que Mugen estaba muy implicado e intentaba mejorar herramientas loic para mejorar el ataque. Como también se indicó anteriormente manifestó haber quedado con Mugen y que tras haber sido identificado le dijo que menos mal que no le habían intervenido el portátil, pero refirió que no recordaba si le había preguntado el motivo de dicha afirmación, que estuvo en su detención, que no le dijeron que le imputaban delito de pertenencia a un grupo terrorista y que declaró de forma espontánea, no recordando si lo hizo ante abogado. Preguntado por la declaración documentada en autos manifestó que no recordaba el documento ni la forma en que se redactó, que fueron a su casa a recoger los efectos que él quiso aportar y allí no recordaba si estaba el letrado presente.

No recordó si Wicker llevaba anotaciones con teléfono de Mugen, ni si este facilitó el teléfono de aquél.

Manifestó que le sonaba que se había hablado de que Mugen proponía publicar datos de la policía en foros pro etarras, pero que no recordaba cuándo.

Declaró que Anonworld y Anonnet eran redes de IRC y que José María Zaragoza no tenía relación con Anonworld sino con Anonnet y con Criteren, pero que no sabía se respecto de Criteren si era administrador.

No pudo precisar que se hubiera acreditado que Mugen usara la IP del domicilio de

Refirió que Devnuller era el nick que utilizaba , y manifestó haber llegado a dicha conclusión sobre todo por las conversaciones de los chats y páginas públicas, que era marino mercante y tenía el servidor en su casa y que posteriormente lo confirmó el examen de los peritos.

No recordó si era necesario tener un usuario registrado para acceder a los chat o canales de IRC que monitorizaron y no recordó tampoco si había aconsejado sobre como registrarse para que otro usuario diferente no usara su nick.

En cuanto al dato aportado relativo a un twitter que atribuían a que decía que se estaba realizando el ataque a la Junta Electoral Central refirió que ponía la dirección del servidor que coordinaba la conexión del ataque y salió una foto de él que se borró al día siguiente de la detención, no recordando la hora del twitter y no recordando si hubo un retwitter de otro usuario.

No pudo precisar si los datos relativos a minutos posteriores al ataque eran una captura de pantalla suya.

Refirió que Anonworld y Anonnet eran servidores distintos, de los que formaba parte el servidor encontrado en casa de , que no recordaba si éste tenía relación con Anonworld pero sí con Anonnet, y que lo dedujeron de las conversaciones, que ese servidor prestaba servicios a esas redes.

Preguntado respecto de los treinta y dos archivos aportados con el atestado con extensiones loic que recogen conversaciones, cuáles eran cogidos de Anonworld, manifestó que no podía precisar pero que los de eran los de Tokoroten.anonnet, y que no sabía cómo se generaban esos ficheros con el cliente.

Manifestó que no sabía cuántos servidores de IRC había en el mundo y no podía precisar por que la mayoría eran de Anonymous, que tendría que ver el contexto en que lo dijo.

En cuanto a la posibilidad de que Devnuller no tuviera que ver con el servidor, manifestó que no sabía, que no podía precisar.

En cuanto a la conversación el 17 de mayo con Devnuller en la que Sprocket aconsejaba que revisara que apreciaba que tenía bajos niveles de seguridad, manifestó que no recordaba haber hablado y haberse reído de ello con otro usuario.

Preguntado sobre si era posible que se metiera un tercero que no era Devnuller y sobre si era posible que Devnuller no tuviera que ver con el propietario del servidor manifestó que no lo sabía.

No recordó si Devnuller habló de atacar a la Junta Electoral Central, y no recordó si se habló de enviar correos, precisando que creía que había hablado en todo momento de ataque DDoS utilizando el loic, que este programa lo conocía y creía no servía para enviar correos y que no sabía si se había efectuado ataque a la junta enviando correos.

Refirió que se enteró del ataque a la Junta electoral Central por las redes sociales y por el chat y no sabía si había avisado a la junta, que el día del ataque la página de dicha junta estaba caída, que no sabía cuántas comprobaciones se habían realizado sobre dicha caída y que no sabía si el grupo Anonymous la había atacado.

No pudo precisar porque los registros de los servidores reseñados en los informes no estaban en la causa, ni si se acudió a los dueños de los servidores para el registro de conexiones de IP.

En cuanto a los documentos sobre cuyo contenido fue interrogado relacionados en sus respectivos informes y consistentes en capturas de pantalla manifestó que suponía procedían de fuentes abiertas o conversaciones con los detenidos.

El funcionario nº 111.452 como se decía anteriormente refirió que dado que una vez producido el ataque ya era imposible investigar, para poder conocer quién estaba detrás, decidieron monitorizarse con pseudónimo, siendo la única forma de investigar ganarse la confianza de ellos y que por ello decidió asignar a un agente del grupo para que investigara y el mismo utilizó el pseudónimo de Sprocket y que aunque empezaron las investigaciones a finales de 2010. en el momento previo a los hechos fue cuando más ataques detectaron y fue cuando intervino el agente, siendo las conversaciones las que se aportaron y que posteriormente los peritos corroboraron las conclusiones que sacaron de las mismas.

Manifestó que era inviable conocer todas las IP que podía haber peticiones falsificadas y cabía que los resultados fueran erróneos.

Precisó que resolvía desde la IP que se aportó, que el servidor físico que manejaba era el del domicilio el que tenía el dominio y que lo podía hacer de forma remota, pues tenía acceso informático en su trabajo.

Refirió que Devnuller era uno de los administradores, conectados a ese servidor, y que no detectaron que otra persona usara ese nick, que era el administrador del chat.

En cuanto al dato de la fotografía de twitter manifestó que vio la foto y que aunque no conocía al acusado

, tenía un parecido razonable con la que aparecía en la foto de la ficha del DNI y que al día siguiente de los hechos fue borrado.



Refirió que el servidor Tokoroten que encontraron estaba compuesto por varios canales siendo la temática común el concierto para realizar ataques DDoS y que ese chat estaba enlazado o conectado a otros, que los servidores pertenecían a Anonworld que tenía otros enlazados, y que aunque hubiera otros administradores, no se enlazaban sin motivo, precisando que los ataques se realizaban desde anonworld.net.

Admitió que el administrador podía crear un usuario en un ordenador y darle permiso para leer, escribir y ejecutar archivos, y si le daba el privilegio de hacer lo que quisiera podía hacerlo.

Asimismo admitió en relación a la función de los servidores de nombres de dominio, que una cosa es la dirección IP que resuelve el contenido en base a un número y otra cuando la máquina busca un dominio y se le indica la dirección IP donde debe buscar, admitiendo que una persona puede indicar a una máquina que tiene un nombre de dominio y que las peticiones que se hagan a ese nombre las va a asistir una máquina que está en una dirección IP que se puede facilitar.

Preguntado si entonces esa persona no tendría por qué ser responsable del dominio principal o máquina en que estaba asignada la dirección de IP manifestó que era cierto aunque para él el responsable último era el primero, admitiendo asimismo que la dirección de IP de un dominio concreto estuviera en máquina diferente a la que resolvía la petición en la que podía haber varios usuarios además del administrador.

Manifestó por otra parte que un servidor máquina en casa no se podía tener porque es muy ruidoso y que lo comprobaron en el registro en el domicilio de .

En cuanto a manifestó que se basaron además en sus declaraciones y se localizaron notas con el teléfono de Wicker, se remitió al atestado en cuanto a su declaración negando que lo hubieran coaccionado para prestar declaración y refiriendo que no intervino en el trámite y no recordaba si estaba el abogado cuando entregó el ordenador, pero que no era necesario, no recordando si estaba ya detenido, y no teniendo conocimiento de si se accedió a su móvil y a su agenda de contactos estando en las dependencias, añadiendo que si fue detenido el día 31 de mayo y no lo presentaron en el juzgado hasta el día 2 de junio, lo hicieron en plazo legal y suponía tendrían que acabar las diligencias.

En cuanto a la detención de en Alicante manifestó que no estaba el comisario Jefe de la BIT y no se entrevistó con el detenido.

Refirió no haber investigado los correos enviados a la Junta Electoral Central porque no se aportaron

El agente 103.017 manifestó haber intervenido en el registro en el domicilio de y precisó que la solicitud de autorización judicial del mismo se realizó por haber tenido conocimiento de que la IP desde la que resolvían los ataques estaba domiciliada en Gijón donde estaba empadronado y porque a la vista de las conversaciones de chat se veía que tenían intención de realizar un ataque a las páginas webs de partidos políticos PP, PSOE y CIU, por lo que era urgente entrar en el domicilio y desactivar el servidor para evitar el ataque.

Refirió que tuvieron conocimiento del ataque a través del servidor de chat Hispano de que se estaba organizando a través de Anonhispano.dynds.org y Tokoroten.anonworld.net que





Anonhispano era un dynds dinámico un nombre de dominio que se podía recibir de internet y era necesario luego que en el router doméstico el que tenía la administración se conectase, lo habilitase y configurase manualmente y luego una vez que tuviera acceso desde cualquier ordenador se preguntase a Anonhispano que te dirigía a la IP del servidor siendo ese servidor Tokoroten, configurado en el canal Hispano en el que se definían los ataques.

Asimismo refirió que Anonhispano era un dns dinámico un servicio entonces gratuito que un proveedor externo de servicios une ese nombre dinámico con una IP y a partir de ahí esa IP puede cambiar.

Precisó que en el registro el ordenador que luego fue examinado estaba en una habitación, estaba encendido y lo desenchufó el declarante y que hacía mucho ruido y estaban los ventiladores en pleno funcionamiento.

Refirió por otra parte que no recordaba si se había intervenido el router, que era un dns del que no recordaba modelo, que de los archivos de configuración unos están en el servidor y otros en el router y que para acceder al router se precisaba contraseña para analizarlo, que no la tenían y que con los medios que tenían no podían hacerlo.

Los peritos intervinieron básicamente para ratificar sus informes técnicos, concretamente los funcionarios nº 107353 y 10295 respecto su intervención en el primer volcado y los funcionarios nº 120932 y 103490 respecto de su intervención en el segundo, de cuya valoración se prescinde.

Respecto a la posibilidad de haber realizado los hechos el acusado encontrándose en la fecha de autos embarcado, se aportó con uno de los oficios del Inspector Jefe del Grupo de la BIT de fecha 5 de agosto de 2011 testifical de Alberto Pérez Vallejo (folio 880) que en fecha 27-7-11 director de recursos humanos de Remolques marítimos S.A. en las dependencias de la policía manifestó que era empleado desde , aportando las hojas de movimientos embarques y desembarques entre el 1-1-11 y el 27-7-11, y refiriendo que la planificación mensual estaba sujeta a variaciones por circunstancias de servicios e instrucciones de Sasemar, que los horarios de cuando el barco estaba atracado eran de lunes a viernes de 8 a 13 y 14 a 17, y a partir de ahí se turnaban el capitán y él, por las tardes y en caso de salir del barco ningún tripulante podía salir fuera a un radio superior a veinte metros.

Asimismo manifestó que en el barco había acceso a internet, existiendo cuatro ordenadores con conexión a internet a través de Movistar y que la tripulación contaba con dos modem usb de Movistar para conectarse en sus ordenadores portátiles particulares, existiendo en la zona donde trabajaba Rodrigo Tuero una dotación de diez tripulantes por turno de embarque.

En la documentación aportada consta que estuvo trabajando del 3 al 29 de mayo de 11 en Sar Almería/Motril y que era primer oficial de puente.

En el plenario tras remitirse a las declaraciones obrantes en autos relativas a turnos de guardia y accesos a internet, manifestó que desconocía los detalles de los sistemas



informáticos del buque, que era un barco nuevo, que cuando estaba atracado y el capitán hacían turnos por la tarde a partir de las cinco que era cuando acababa el horario del barco, siendo posible que algún día Rodrigo Tuero entre las 17,00 y las 12,00 horas estuviera como responsable como primer oficial.

Manifestó no saber si el capitán prohibía el uso del móvil en la guardia en el puente de mando, que había conexión remota a internet y los tripulantes podían usar dispositivos pero que había un listado de uso, que había gente que tenía dispositivos particulares y que el capitán no le dijo que tuviera un dispositivo particular.

En cuanto a la denuncia a que se hizo referencia en el atestado acerca del ataque a la página web de la Junta Electoral Central bloqueándola e impidiendo su funcionamiento, obra al folio 27 copia de la misma formulada en fecha 19 de mayo de 2011 por F en la comisaría de la policía nacional de Madrid en representación de la Junta Electoral Central en la que relata que sobre las 19,00 horas de ayer comenzaron a recibir correos electrónicos de forma masiva al correo de la Junta Electoral Central@Congreso.es y Manuel delgado@Congreso.es, relacionados con la concentración en Puerta del Sol, que actualmente siguen recibiendo a 40 o 50 por minuto, con el consiguiente perjuicio en el funcionamiento del sistema informático de la Junta Electoral Central, en la madrugada de hoy se tuvo constancia de un acceso masivo a página web lo que ocasionó su bloqueo a otros usuarios, siendo su dirección www.jce.es y que se han adoptado por el departamento de informática del Congreso medidas para mitigar los efectos nocivos de este ataque.

No se propuso el testimonio del mismo para el acto del juicio oral, proponiéndose el de B director del servicio técnico de la Junta Electoral Central.

Obra en autos a los folios 1564 y ss informe de fecha 6-2-15 suscrito por el mismo sobre los perjuicios ocasionados, en el que refiere que entre los días 18 y 20 mayo 2011 se detectaron operaciones inusuales en el entorno informático de la Junta Electoral Central residente en el Congreso de los Diputados, que analizada la situación se observó que las operaciones provenían de un ataque informático externo que afectó a los servicios de correo electrónico y página web de la Junta Electoral Central y que el correo aumentó de forma considerable en los buzones del Secretario General y Director de la Secretaria Técnica de la Junta y en el buzón de la propia Junta.

Se concreta que los mensajes recibidos fueron: domingo 15, 6.883, lunes 16, 20.198, martes 17, 21.034, miércoles 18, 27.945, jueves 19 130.841, viernes 20, 214.103, sábado 21 34.043 y domingo 22 26.715.

Respecto a la página web se refiere que los atacantes consiguieron dejarla fuera de servicio de forma intermitente y que la monitorización del sistema permitió observar ataques externos que intentaban bloquearla mediante una denegación de servicio y que el procedimiento para evitar las consecuencias del ataque consistió en cortar la comunicación a las direcciones de IP que lanzaban gran número de peticiones en

esperar respuesta, (en algún momento se detectaron más de dos millones de paquetes de comunicaciones desde la misma IP). Además de estas medidas, la máxima vigilancia y al atenuación de los ataques en días posteriores permitieron el normal funcionamiento de la página.

Concluye el informe refiriendo que el coste del trabajo para responder a los ataques se estima en 700 euros correspondientes a dos jornadas de un consultor experto en seguridad, si bien fue el impacto negativo en el normal desarrollo del trabajo lo que ocasionó mayores perjuicios.

En el plenario el testigo ratificó que se produjo un envío masivo de correos que excedían mucho de las peticiones ordinarias, con interrupción intermitente de la página, que se dejó fuera de servicio en intervalos de minutos, que no se supo su contenido, que el correo siguió funcionando y que sufrieron daños por importe de 700 euros, aclarando que el trabajo en la web lo realizó un empleado con nómina en plantilla del congreso y no se le pagó nada más por este servicio, que no se conservó nada y por tanto no sabía si los hechos tenían relación con el grupo Anonymous, que empezaron a las 18,000 horas de la tarde los envíos masivos y que cayó la página el 19 de mayo, que no estaba seguro si fue de madrugada o por la mañana y que la página web tenía programas para intentar la seguridad general.

Refirió que el ataque provocó caídas intermitentes que en menos de una hora quedó resuelto, que la página caía se arreglaba y caía y que de la denuncia que puso la Junta se enteraron mucho después y no contactó con la policía para informarse sobre la gestión de la denuncia.

En cuanto a las declaraciones de los acusados, en comisaría y en el juzgado instructor (folio 105) se acogió a su derecho a no prestar declaración y en el plenario negó los hechos de autos, respondiendo de forma clara, contundente y precisa a todas las preguntas que se le fueron efectuando sobre todos los extremos apuntados en la causa que le relacionaban con los hechos de autos.

Manifestó que vivía en Gijón en la calle de , que tenía ordenadores personales y servidores caseros, que el nick o apodo Tuerinator y Devnuller los usaba esporádicamente pero que los usaba más gente, siendo el significado de Devnuller conforme a un chiste informático, basura, así como que era habitual en un chat tener varios nicks y cambiarlos y hacerse pasar por otros o troleear, por lo que un tercero pudo usar el nick Devnuller y le constaba que lo habían hecho, siendo por otra parte fácil de comprobar la existencia de numerosos perfiles con dicho nombre.

Refirió que no le constaba que el servidor de su casa se hubiera utilizado para ataques de denegación DDoS, que en el mismo no se alojó software ilegal ni red de ordenadores fantasmas, precisando que servidores caseros los tenía desde hacía muchos años y se dedicaba a dar soporte a páginas webs de amigos, foros de astronomía locales y direcciones de correo electrónico pero no con finalidad delictiva, que todo estaba en el servidor que se le intervino, que un servidor es un ordenador normal y configurar un servidor es arrancar un programa.



Declaró que el servidor no se llamaba tokoroten.anonworld.org sino telecable.org que conocía la cuenta, que era la cuenta del administrador del servidor, que estaba la cuenta en la página principal con todos sus datos y con el aviso legal de que si había alguna actividad abusiva o ilegal se contactara con esa dirección y no recibió ningún aviso.

En cuanto a la cuenta anonhispanol.dnds.org, manifestó que no la conocía antes de la denuncia, que los servidores dynds se contratan gratis por cualquiera en internet y él no lo había hecho porque ya tenía configurada una dyn.

Refirió que en su ordenador, era él el administrador y otros usuarios tenían permiso que él daba pero cualquiera podía lanzar programas o ejecutar tareas dentro del servidor, dentro de ciertos límites, que eso se podía hacer en todos los ordenadores incluso con restricciones de usuarios.

Preguntado sobre si sabía por qué el servidor tokoroten.anonworld.net resolvía en la IP de su domicilio respondió que esa dyns no estaba registrada a su nombre, que no se investigó legalmente quién era el propietario y nunca estuvo registrado a su nombre, que él podría crear un dynds y asignarlo a un ordenador y que no tenía por qué ser el del propietario.

Precisó que Ircserv era el que hacía reglas y añadía y borraba usuarios, insistiendo en que una cosa es el servidor acceso físico a administrador servidor y otra el programa acceso a la aplicación del servidor, que él creó el servidor IRC porque daba servicios a empresas y colectivos y asociaciones y que no sabía si por twitter alguien pidió alojamiento para aumentar la red ya existente y él accedió sin intención alguna.

En cuanto a alguna de las capturas de pantalla que se aportaron con los informes policiales como el obrante al folio 465 manifestó que era el aviso legal que se leía cuando alguien ponía un servidor, y que en el servidor había varios usuarios.

Precisó que el usuario que utilizaba habitualmente era Panera, que cualquier usuario podía acceder a la carpeta panera y quedaba registrado, que la aplicación xchat era una aplicación de mensajería que no permitía lanzar servicios, y que él no quería actividad ilegal ni ataques y así lo había declarado y que lo que había en la causa consideraba era de terceras personas o entidades.

Negó haber enviado correos y haber participado en el ataque a la Junta Electoral Central del que dijo se enteró a posteriori al salir del trabajo en un cibercafé creía que por twitter.

Preguntado por la posibilidad de manejar el servidor de forma remota, declaró que de manera restringida porque hay cosas que requieren acceso físico, como conectar, desconectar el disco duro y ver determinados ficheros y archivos, que autorizar accesos sí y crear y borrar usuarios sí pero para ello tenía que tener internet y que en Almería en el barco había ordenadores corporativos con restricción de usuario, que había ordenador en la oficina del buque, en el despacho del capitán y en el del jefe de máquinas, y que en el puente no había conexión de red, que arriba estaban las antenas, que la empresa suministraba usb, pero el capitán restringió su uso, que aunque lo normal era instalar un punto de acceso wifi, era un barco nuevo y no estaba instalado. Asimismo refirió que en





la empresa había un formulario y cuando se entregaban los usb se exigía la identificación y constaba la entrega y devolución, que en el barco tenía móvil sin aplicación de datos y que ni le serviría para acceder remotamente a un servidor, y que él trabajaba de 8,00 a 13,00 y 14,00 a 17,00 m que de ocho a doce doblaba turnos, que por cuestiones de logística el capitán acordó que el subalterno al que correspondía la guardia realizara el trabajo físico y él hiciera guardias de mantenimiento y siempre había un oficial de guardia y por la tarde si el capitán hacía alguna gestión él le sustituía.

Argumentó por otra parte que no tenía acceso a todo, que había cajas fuertes, que el capitán cerraba el despacho con llave y que además de la restricción de usuarios, él no podía ejecutar ni dar instrucciones, pues tendría que instalar un programa que no tenía.

Manifestó que habló con el capitán para que certificara que a las doce estaba en su puesto de trabajo y el abogado redactó el escrito que se le remitió y firmó

Precisó que ahora conocía los nicks Mugen Seraf y Siplas pero no le sonaban de antes y que conocía el grupo Anonymous pero no formó parte nunca del mismo ni en consecuencia dio órdenes como jefe o representante del mismo ni las recibió.

Asimismo manifestó que no conocía a los coacusados.

Respecto al texto a que hacía referencia la policía sobre la explicación de cómo acceder a internet sin limitación cuando estaba embarcado, manifestó que en esa fecha estaba en un barco con otra empresa con internet cada diez minutos y que en ningún caso hubiera podido ni entonces ni al tiempo de los hechos estar ni con el móvil ni con un ordenador varias horas.

No recordó haber denunciado en 2007 la sustracción de una PDA ni la existencia de foto alguna con un portátil, que alguno de los agentes reseñaron en el atestado y refirieron presentaba gran parecido con él.

Preguntado acerca de la mención en los informes policiales relativa a Wicker manifestó que cualquier usuario tiene libertad de movimientos y si la policía decía que Wicker había sido baneado es que no podía acceder al servidor, pero que él no redactó la regla que impedía a Wicker participar.

detenido en fecha 31 de mayo en las circunstancias antes expuestas, declaró en comisaría en presencia de letrado (folios 508 a 512) manifestando que desde octubre de 2010 había comenzado a interactuar en los chats del grupo Anonymous como un usuario más participando en ataques DDoS de manera individual conectando el programa loic a los servidores de ataque que gestionaban americanos y que tras el ataque a la SGAE se produjo una división interna en el grupo, dividiéndose los españoles en dos grupos Anonworld y anonnet, que el primero era un servidor privado de un usuario llamado Devnuller y el segundo un servidor público en el que ellos crearon el canal Hispania.

Manifestó que a nivel nacional junto con la red anonnet a la que pertenecía eran coordinadores del ataque a la junta electoral central y que utilizaba los nicks de Mugen, Seraf y Siplas.

Refirió que el hive era un programa para controlar remotamente todos los loics, es decir gente que quiere participar en un ataque y no tiene suficientes conocimientos conecta el loic al canal y es un administrador quién lo controla, que dentro de la red anonnet coordinando los ataques





además de él mismo, estaba el usuario Wicker y puntualmente Xetra y Luna.

Manifestó que Wicker era uno de los administradores principales que manejaba el loic y las operaciones, buscaba vulnerabilidades, registraba ip de usuarios, investigaba a otros usuarios, proponiendo algún objetivo para ser atacado y aportó el número de teléfono.

Finalmente manifestó tras acceder a entregar el ordenador y a entrar en su domicilio, que tenía claro dejar el movimiento y los ataques una vez finalizadas las elecciones municipales, al sentirse engañado.

En el juzgado de instrucción (folio 518) tras manifestar en presencia de letrado que ratificaba sus anteriores declaraciones, refirió que la actividad comenzó en 2010 y cesó con su detención, si bien hacía una semana pensaba dejar de dedicarse a ello, que por esos hechos no obtuvo beneficio alguno económico, que no podía aportar más del resto de personas implicadas aunque pudiera tener algún número de teléfono en su agenda de móvil que estaba en poder de la policía, que autorizó en su momento la intervención de los efectos y la entrada en su domicilio, y que el motivo de pensar abandonar la actividad era porque se había visto decepcionado al darse cuenta de que no puede de esta forma cambiar la sociedad y que la gente que intervenía en los hechos tampoco estaba dispuesta a hacerlo.

En el acto del juicio manifestó que cuando fue detenido sobre las 13,00 horas del día 31 de mayo de 2011 en la Diagonal en Barcelona habiéndose citado con una persona, le cogieron varios agentes le enseñaron la placa y le llevaron en el vehículo policial con las sirenas a comisaría a Vía Layetana y una vez allí estuvo en calabozo hasta las 19,00 horas, que entre tanto los agentes le decían que no sabía dónde se había metido y que le iban a meter un delito de pertenencia a grupo terrorista, que luego le dieron el documento ya escrito que firmó cuando llegó el abogado y posteriormente le llevaron los agentes al domicilio de sus padres en Arenys de Mar estando ya detenido pero que no estaba su abogado.

Negó todos los hechos de autos, tanto la pertenencia a grupo criminal como la intervención en el ataque a la Junta Electoral Central y en la planificación del ataque a los partidos políticos, refiriendo que los nicks Mugen y Seraf eran muy utilizados en las redes sociales, que él no era administrador de anonworld ni de anonnet que anonnet era como un servidor de un whatsapp público en el que debatían diversos temas, que él creó un grupo público en el servidor anonnet y en él debatían de todo pero que no administraba canal alguno en anonworld.

Manifestó por otra parte al serle exhibidos distintos documentos de los informes policiales que al folio 1203 se veía una impresión de su carpeta, y se apreciaba un corta y pega, que la persona que realizaba el ataque se debería identificar a través de la IP, que había que mirar el registro del servidor que hacía el ataque y filtrar con el nick a ver si coincidía con la IP y eso no se había comprobado en la causa.



Fue preguntado sobre varias imágenes contenidas en el informe técnico de la BIT cuya valoración no procede pero en cualquier caso negando su intervención en los hechos.

Así exhibido el folio 1229 manifestó que se veía que alguien usaba el nick Seraf, que era un registro que aparecía en su ordenador y se veía que se lanzaba un comando de ataque a la Junta Electoral Central y el servidor respondía que no tenía permiso. Refirió que la gente se debe de identificar y nada más ponía el comando que hacía el ataque y el servidor decía que no tenía permiso para manejar esa botnet.

En el folio 1228 manifestó que el servidor criten salía en teoría de su ordenador aunque en los CDs aportados a la causa no aparecía.

En el folio 163 refirió se veía una imagen colgada de internet que no constaba ni se acreditaba de donde salía ni quien la tomaba, que se veían dos nicks que no se podían identificar porque no había registros, que parecía una orden de ataque del día diez o fecha que no se vía bien, siendo de mala calidad y siendo claramente modificable.

En el folio 164 manifestó que se veía una conversación en la que alguien que usa el nick Mugen queda con alguien que usa el nick Sprocker, que si él se desconectaba posteriormente otra persona podía usar ese nick, y que para saber si Mugen está conectado posteriormente tendrían que haberse investigado los registros del servidor y no estaban en la causa y no constaba que se hubieran pedido a los dueños de esos servidores.

en comisaría se acogió a su derecho a no prestar declaración (folios 570 y ss).

En el juzgado instructor (folios 586 a 587) manifestó que era cierto que utilizaba el nick Wicker a través de la red anonnet pero que no realizó ninguna modificación en la página de la Junta Electoral Central, admitiendo asimismo utilizar los nicks Némesis e Irae, pero negó haber administrado el hive en el ataque a la Junta Electoral Central aunque admitió que pudiera aparecer su intervención al apagar.

En cuanto a las anotaciones en su domicilio de reventar correos del PP y PSOE y atacar libertad digital o cuentas de Angeles González Sinde, Ministra de Cultura refirió que pudieran ser anotaciones que hizo por enfado por el resultado de las elecciones pero que no materializó, que no tenía conexión internet, que utilizaba conexiones de bares a cambio de consumición o bien de personas cerca del domicilio sin autorización, y que se dedicaba a realizar trabajos de configuración de páginas web para universidad Murcia toxicología y fauna silvestre.

Admitió haber manifestado a través de los canales la posibilidad de obtener datos privados de fuerzas y cuerpos de seguridad miembros de gobiernos y otros estamentos públicos, pero refirió que las personas a las que iba dirigido no sabrían como hacerlo y él se había concentrado en otros asuntos, con lo que eso ya estaba olvidado.

En el acto del juicio manifestó que tenía formación informática autodidacta, que diseñaba páginas web y tenía conocimientos de lo esencial para seguridad informática, diseñando herramientas para evitar ataques y que comprobaba la vulnerabilidad de las páginas pero que la investigación de

vulnerabilidad era más de artesanía, no teniendo interés en ataques de denegación de servicio DDoS.

Manifestó por otra parte que en las fechas próximas al 15 M se sentía frustrado y tenía interés por lo que pasaba, interesándose principalmente por ese movimiento y por otros, que investigó qué pasaba con Anonymous pero solo por seguridad informática, pero negó formar parte de anonymous, y negó haber participado en el ataque a la Junta Electoral Central y en la planificación de ataques a los partidos políticos.

Refirió que había visto los chats aportados en CD a la causa y que eran claramente manipulables, negando ser el Wicker de las conversaciones, salvo algunas, precisando que se podía suplantar la personalidad de los usuarios, que él usaba el nick Wicker y también lo utilizaban otros y entonces él entonces no podía entrar con el mismo sino con un número y si estaba baneado de un servidor no podía entrar ni con ese nick ni con otro, por lo que no podía interactuar en ese servidor.

Precisó por otra parte que en las conversaciones aportadas, los nicks reflejan personas que hablan pero no se sabe quien escucha, que en esos nicks había un Sprocket y que cualquiera podía infiltrarse y utilizar el nick Wicker.

Manifestó que comprobaba vulnerabilidades por seguridad informática, comprobando si funcionaba bien o no una página y que las herramientas utilizadas no afectaban al sistema, que comprobó superficialmente semanas antes de los hechos la vulnerabilidad de la Junta Electoral Central, que hizo pin al dominio de la Junta Electoral Central lo que supone enviar un único paquete de datos para saber si existe y esperar respuesta sobre si esta caído o activo y la respuesta fue que estaba activo, pero que no participó en el ataque.

SEPTIMO. Es reiterada la doctrina del T.C. que señala que la presunción de inocencia ocasiona un desplazamiento de la carga de la prueba a las partes acusadoras a quienes incumbe exclusivamente probar los hechos constitutivos de la pretensión penal, debiendo ser suficiente para generar en el juzgador la evidencia de la existencia un hecho punible y de la responsabilidad penal que haya tenido en él el acusado o acusados, así como sustentarse la actividad probatoria en auténticos medios de prueba obtenidos con respeto a los derechos fundamentales y practicados en el juicio oral bajo los principios de igualdad, contradicción, inmediación y publicidad.

En la facultad de apreciación de la prueba que el art. 741-1 de la Ley de Enjuiciamiento Criminal concede al Tribunal de instancia entra el estimar, entre las declaraciones contradictorias de una misma persona -acusada o testigo-, aquella que a su juicio valorativo resulte más convincente y se acomode mejor a los datos disponibles y a la realidad de los hechos, pudiendo para ello confrontar entre sí las distintas declaraciones prestadas para elegir la que, en conciencia, considere ajustada a la verdad.

En el mismo sentido el T.S. es constante al afirmar que cuando las declaraciones de un acusado o testigo en el juicio oral, difieren de las efectuadas en la fase de instrucción con todas las garantías, el juzgador puede conceder credibilidad a unas u otras, de acuerdo con el principio de inmediación y libre valoración, al haber percibido directamente la actitud del declarante, sus vacilaciones o contradicciones.

Se viene admitiendo por ello la valorabilidad de la confesión sumarial cuando el acusado se retracta en el juicio oral y niega haber tenido intervención en el hecho de que se le acusa, exigiendo en todo caso que la confesión haya sido prestada en presencia judicial con asistencia letrada, con información de los derechos que asisten al confesante y explicando la razón de su cambio de declaración.

No obstante solo es susceptible de ser valorada como prueba de cargo la confesión realizada ante la autoridad judicial, no interesando a este respecto las prestadas por el imputado en presencia policial en el atestado que da inicio a la causa penal, pues las mismas tienen el valor de mera denuncia al haber sido realizadas en una fase preprocesal anterior a la incoación del sumario con el que se inicia el proceso penal.

Así se viene declarando por el T.S. entre otras en sentencias del T.S. de fechas 23-3-00 y 7-10-00 que una manifestación espontánea del imputado de carácter auto inculpatario realizada antes de haber sido instruido de sus derechos por los agentes actuantes, acerca de cuáles son sus derechos (a no declarar, a no confesarse culpable, entre otros), ha de ser considerada inválida.

Sólo si posteriormente esa inicial manifestación es ratificada por el propio acusado subsanando así aquella ilegalidad originaria, cabría valorarla como prueba de cargo.

Asimismo se viene estableciendo por la jurisprudencia del T.S. la exigencia de que la declaración autoinriminatoria no presente ningún condicionante externo que la haga sospechosa de no ser plenamente libre, esto es, voluntaria y consciente de lo que se hace, y además que se efectúe en un momento procesal en que concurren todas las garantías legales.

La declaración debe practicarse ante el juez previa información al inculpado de sus derechos constitucionales, en particular del derecho a no confesarse culpable y a no declarar contra sí mismo, con posibilidad de guardar silencio o de no contestar a alguna o algunas de las preguntas que se le formulan. El imputado ha de estar debidamente asistido del letrado. Cuando se presta la declaración en que se admiten los hechos no debe estar acordado el secreto de las actuaciones, ya que ello limitaría notablemente el derecho de defensa, debe tratarse de una declaración voluntaria y espontánea, sin vicios ni situaciones sugestivas que puedan alterar dicha voluntariedad. Ha de concurrir cierto distanciamiento en el tiempo entre la fecha de la acción delictiva (y, en su caso, la detención) y la admisión por el imputado de la ejecución del hecho delictivo, como forma de garantizar la espontaneidad y voluntariedad de la declaración.

Es por ello en el acto del juicio donde concurren todas las garantías para que una declaración de carácter inculpatario pueda surtir plenos efectos jurídicos.

Asimismo y como regla general la confesión solo será válida como prueba de cargo independiente de prueba que haya sido obtenida con vulneración de derechos fundamentales,

cuando sea prestada en el acto del juicio oral, pues solo en ese momento se conoce la pretensión acusatoria y las pruebas en las que se basa; se han planteado ya los términos de la defensa, y la decisión del acusado puede considerarse totalmente libre y adoptada y es en esta fase en la que concurren todas las garantías para que pueda surtir plenos efectos jurídicos (sentencia del T.S. de 12-1-14).

Sentado lo anterior en cuanto a la documental aportada relativa a las investigaciones realizadas en las redes sociales y concretamente a las conversaciones de chat con los usuarios de los nicks Mugen/Seraf y Wicker y a los datos extraídos de los pantallazos aportados con ocasión de la investigación de la llamada operación "V de Votaciones" y del ataque a la Junta Electoral Central, no obstante no haberse declarado la nulidad pretendida por las defensas de la intervención del agente nº 103.490 que con el usuario Sprocket se ganó la confianza de los mismos, tras la apreciación directa de sus manifestaciones en el plenario, no se puede considerar debidamente ratificada dicha prueba, por cuanto el agente tras un detallado interrogatorio respondió a la mayoría de preguntas que le fueron formuladas como se reseñó anteriormente con las respuestas "no se" y "no recuerdo". Tampoco se puede salvar a los efectos reseñados la falta de memoria de dicho agente en el plenario pese a su insistencia a que se preguntara sobre todo lo que él manifestó no saber o no recordar al instructor, con las declaraciones del funcionario nº 111.452 que si bien fue el que autorizó la intervención del agente Sprocket y ratificó todos los informes aportados, no fue el que intervino directamente en las conversaciones sino que supervisó las mismas.

Aunque dirigió y supervisó el resto de investigaciones, no pueden tomarse en consideración sus conclusiones acerca de los informes técnicos que dijo corroboraban sus sospechas y de cuyo contenido se ha prescindido.

Por otra parte llegó a admitir en el plenario que el administrador podía crear un usuario en un ordenador y darle permiso y si le daba el privilegio de hacer lo que quisiera lo podía hacer, que una cosa es la dirección IP que resuelve el contenido en base a un número y otra cuando la máquina busca el dominio y se le indica la dirección IP que debe buscar, admitiendo que una persona puede indicar a una máquina que tiene un nombre de dominio y que las peticiones que se hagan a ese nombre las va a asistir una máquina que está en una dirección IP que se le puede facilitar, en cuyo caso esa persona no tendría por qué ser el responsable del dominio principal o máquina en que estaba asignada la dirección IP, y la dirección IP de un dominio concreto podía estar en máquina diferente a la que resolvía la petición en que podía haber varios usuarios.

Manifestó también que no era viable conocer todas las direcciones IP, que podía haber peticiones falsificadas y que cabía que los resultados fueran erróneos.

Por su parte el funcionario nº 103.017 que intervino en el registro del domicilio de y precisó haber desconectado el ordenador que estaba encendido, manifestó que parte de los archivos de configuración estaban en el router y que con los medios de que disponían no podían analizarlo.

Aparte de ello respecto de las conversaciones de chat cuyos resúmenes fueron aportados, en las mismas constan



diversos usuarios registrados y tanto los testigos como los acusados manifestaron que los mismos utilizan pseudónimos y que aunque en principio se puede bloquear el mismo para evitar sea utilizado por otras personas, es habitual que se utilice el mismo pseudónimo por varios usuarios.

Las intervenciones telefónicas cuyos resúmenes se aportaron, una vez descartadas las conversaciones con los letrados, nada de interés aportaron y ni siquiera se hizo referencia a las mismas en el plenario, salvo en lo relativo a la conversación de [redacted] con el capitán del buque a las que antes se hizo referencia.

Las declaraciones del acusado [redacted] como se decía anteriormente se apreciaron contundentes y en las mismas negó con rotundidad los hechos de autos y rebatió con claridad todos los extremos objeto de imputación incluso relativos a extremos apuntados a los peritos de la acusación que ninguno de los testigos y peritos aclararon debidamente en el plenario.

Asimismo ofreció explicación de descargo acerca de la limitación de disponibilidad de internet con ocasión de hallarse embarcado, y las declaraciones en el plenario del testigo de cargo aportado [redacted], con remisión a la documentación aportada en su día, no se consideraron contundentes ni suficientes para desvirtuar las declaraciones del acusado en el plenario acerca de los medios de que disponía cuando estaba embarcado y de la posibilidad de haber ejecutado los hechos de forma remota, no habiéndose propuesto el testimonio del capitán del buque con el que el mismo se sustituía y no considerando tampoco dato objetivo suficiente para deducir su intervención en los hechos las manifestaciones de los agentes que efectuaron el registro acerca de que el servidor ordenador que estaba encendido en el momento del registro hacía mucho ruido, a falta de otros datos.

Por otra parte se llegó a admitir por los testigos y por los peritos que no era lógico que usando la IP que se le asignó se llegara a un servidor que en la primera página diera todos los datos personales del mismo si estaba realizando una actividad ilegal.

El acusado [redacted] tampoco admitió los hechos de autos ni en la fase de instrucción ni en la de plenario y aunque admitió poseer determinadas herramientas que según los testigos eran utilizadas para perpetrar ataques, precisó que eran habitualmente empleadas en personas con conocimientos informáticos como los que él posee.

En el mismo sentido el perito D. José Luis Ferrer Gomila estimó que los datos que obraban en las actuaciones acerca de [redacted] derivados del chat y de la declaraciones que pudo efectuar en su día [redacted] no permitían atribuir ninguna acción concreta al mismo. El perito manifestó que las herramientas que el mismo reconoció poseer son habituales en usuarios de profundo conocimiento informático y en materia de seguridad relativa al mismo y precisó que no había apreciado datos que revelaran que hubiera hecho un mal uso de las mismas considerando que deberían haberse practicado pruebas adicionales.

En cuanto al acusado [redacted] por supuesto en virtud de la doctrina anteriormente expuesta carecen de valor probatorio alguno las manifestaciones que pudo efectuar al agente nº 103.490 cuando fue citado por el mismo en la Puerta del Sol en Madrid, respecto de las cuales en su caso las del



agente hubieran podido constituir un mero testimonio de referencia y ello por cuanto fueron manifestaciones realizadas sin garantía alguna cuando ni siquiera sabía quién era el agente y éste con ocasión de su declaración como testigo manifestó no recordar ni siquiera si le había preguntado el por qué de dichas manifestaciones.

Su detención según se ha expuesto tuvo lugar sobre las 13,30 horas del día 31 de mayo de 2011, se le informó de sus derechos sobre las 14,30 horas solicitando abogado de oficio y la comunicación a su hermana, se le recibió declaración a las 19,00 horas y a las 20 horas se desplazó con los funcionarios de la policía conforme a lo que consta manifestó en su declaración de acceder a entregar un ordenador al domicilio en Arenys de Mar, constando acta de entrega de dicho efecto a las 21,00 horas sin presencia de letrado.

Al margen de las circunstancias de dicha entrega, que resulta irrelevante ante la conclusión a que se ha llegado en relación a la custodia de los efectos intervenidos, desprecintos y volcados de los mismos, la declaración en el juzgado de dicho acusado con remisión inicialmente a aquella fue mucho más genérica, habiéndose realizado ambas declaraciones cuando las diligencias eran secretas y habiendo sido puesto en libertad provisional sin fianza alguna, y en el plenario rebatió con contundencia todos los extremos objeto de acusación e incluso sobre documentos contenidos en los informes que no fueron tampoco aclarados debidamente en el plenario por los peritos.

El perito D. José María Rodríguez Sánchez manifestó entre otros extremos que existían dudas razonables para determinar quién estaba detrás de los canales de chat con el usuario Seraf Mugen y haría falta visualizar los ficheros del la log del servidor del irc para verificar la IP física que se está conectando al servidor y cotejar con el proveedor de servicios del mismo, si realmente es él o alguien de su entorno, lo que no se comprobó en el caso de autos, estimando que no estaba demostrado que en todos los casos en las conversaciones de chat fuera el Sr. el que estaba detrás de Mugen o Seraf, que si bien es verdad que cada uno tiene su clave privada esta es fácilmente recuperable por terceros y mas para los usuarios que se conectan a estos chats que poseen un avanzado nivel informático y es un proceso fácil de crackear y además no se verificó dentro de los archivos del log el momento de la conexión ni la IP física desde la que se realiza la misma.

El perito afirmó además que a la vista de las imágenes obrantes en autos, de poca calidad sería necesario un estudio más a fondo de este extremo.

A parte de ello en cuanto al delito de daños, al margen de que de las declaraciones de los funcionarios de la BIT se desprende que en las investigaciones practicadas detectaron que se ejecutaron ataques de DDoS uno de ellos contra la página web de la Junta Electoral Central y que estos son medios de los que se viene considerando que afectan a la funcionalidad del sistema informático, se alegó que dichos ataques afectaron de forma importante el funcionamiento del correo de la Junta Electoral Central y que se remitieron múltiples peticiones simultáneas que ocasionaron el bloqueo de la página web de dicha Junta, si bien los agentes en el plenario refirieron que no examinaron los correos y las manifestaciones antes reseñadas del director del centro de TIC



del Congreso D. en el plenario vinieron a aminorar tanto la entidad de los hechos en su día denunciados como la de sus resultados al referir que se produjo una interrupción intermitente de la página que quedó fuera de servicio en intervalos de minutos y el problema quedó resuelto en una hora, que el correo siguió funcionando y que los perjuicios derivados de los hechos inicialmente estimados en setecientos euros no eran tales porque el trabajo lo realizó un empleado en nómina al que no se le abonó cantidad alguna por dichos servicios.

En definitiva tras la apreciación directa en el plenario de la prueba testifical, de la pericial en extremos no relativos a los dispositivos incautados y de las declaraciones de los acusados en relación con la documental aportada, se concluye con que no ha sido acreditado que los acusados pertenecieran al colectivo Anonymous con el objeto de cometer de forma concertada uno o varios delitos menos graves o de la perpetración reiterada de faltas, ni que con ocasión de la celebración en España de las elecciones locales y autonómicas de fecha 22 de mayo de 2011, con la finalidad de entorpecer el proceso electoral se hubieran puesto de acuerdo y hubieran preparado dos ataques de Denegación de Servicio Distribuido (DDoS), uno el día 18 de mayo de 2011 bajo el nombre de operación "Spanish Revolution" contra el entorno informático de la Junta Electoral Central residente en el Congreso de los Diputados, contra la página web de la Unión general de Trabajadores y contra la página web del Congreso, que hubiera afectado de forma importante al normal funcionamiento del correo electrónico obstaculizando los trámites previos al proceso electoral y remitiendo múltiples peticiones simultáneas ocasionando el bloqueo de la página web de la Junta electoral central, ni que hubieran acordado realizar sobre las 16,00 horas del día 20 de mayo de 2011 la operación V de Votaciones, contra las páginas web del PP, del PSOE y de CIU, procediendo en consecuencia decretar la absolución de los mismos respecto de ambos delitos objeto de acusación.

OCTAVO. Conforme a los artículos 109 del C.P. y 239 y ss de la L.E.Cr. procede declarar de oficio las costas procesales.

Vistos los artículos citados, y demás de general y pertinente aplicación.

FALLO

Que debo absolver y absuelvo a los acusados

del delito de pertenencia a grupo criminal y del delito continuado de daños por los que venían siendo acusados por el Ministerio Fiscal, declarando las costas de oficio.

Notifíquese la presente resolución a las partes y hágase saber que contra la misma puede interponerse recurso de apelación ante la Audiencia Provincial en el plazo de diez días a partir del siguiente al de su notificación, durante cuyo período permanecerán las actuaciones en Secretaría a disposición de las partes.

Así, por esta mi sentencia, de la que se unirá certificación a los autos, lo pronuncio, mando y firmo.

E/.





PUBLICACIÓN.- Dada, leída y publicada fue la anterior sentencia por la Ilma Magistrada en audiencia pública en el día de la fecha, de lo que yo el Letrado de la Administración de Justicia, doy fe.

