Roj: **STS 3754/2018** - ECLI: **ES:TS:2018:3754**

Id Cendoj: **28079120012018100512**
Órgano: **Tribunal Supremo. Sala de lo Penal**
Sede: **Madrid**
Sección: **1**
Fecha: **23/10/2018**
Nº de Recurso: **1674/2017**
Nº de Resolución: **489/2018**
Procedimiento: **Penal. Apelación procedimiento abreviado**
Ponente: **ANTONIO DEL MORAL GARCIA**
Tipo de Resolución: **Sentencia**

T R I B U N A L S U P R E M O

Sala de lo Penal

Sentencia núm. 489/2018

Fecha de sentencia: 23/10/2018

Tipo de procedimiento: RECURSO CASACION

Número del procedimiento: 1674/2017

Fallo/Acuerdo:

Fecha de Votación y Fallo: 05/07/2018

Ponente: Excmo. Sr. D. Antonio del Moral Garcia

Procedencia: Sección Primera Audiencia Provincial de Vizcaya.

Letrada de la Administración de Justicia: Ilma. Sra. Dña. Sonsoles de la Cuesta y de Quero

Transcrito por: IPR

Nota:

RECURSO CASACION núm.: 1674/2017

Ponente: Excmo. Sr. D. Antonio del Moral Garcia

Letrada de la Administración de Justicia: Ilma. Sra. Dña. Sonsoles de la Cuesta y de Quero

TRIBUNAL SUPREMO

Sala de lo Penal

Sentencia núm. 489/2018

Excmos. Sres.

D. Andres Martinez Arrieta

D. Luciano Varela Castro

D. Alberto Jorge Barreiro

D. Antonio del Moral Garcia

D. Andres Palomo Del Arco

En Madrid, a 23 de octubre de 2018.

Esta sala ha visto el recurso de casación con el nº 1674/2017 interpuesto por **Maximiliano** representado por la procuradora Sra. Beatriz María González Rivero, bajo la dirección letrada de D. Jesús Urraza Abad contra Sentencia 23/2017 dictada el 1 de junio de 2017 por la Sección Primera de la Audiencia Provincial de Vizcaya en causa seguida contra el recurrente por un delito de administración desleal. Ha sido parte recurrida la mercantil Trimarine Internacional Spain representada por el procurador D. Luis Pablo López y bajo la dirección letrada de D. Pedro Learreta Olarra. Ha sido parte también el Ministerio Fiscal.

Ha sido ponente el Excmo. Sr. D. Antonio del Moral Garcia.

ANTECEDENTES DE HECHO

PRIMERO.- El Juzgado de Instrucción núm. 8 de Bilbao instruyó PA nº 3785/2014, contra Maximiliano . Una vez concluso lo remitió a la Audiencia Provincial de Bilbao que con fecha 1 de junio de 2017 dictó sentencia que contiene los siguientes **Hechos Probados:**

PRIMERO.- TRIMARINE INTERNATIONAL SPAIN S.L.U (en adelante TRIMARINE) fue constituida en fecha 8 de julio de 2004 por la mercantil TRIMARINE INTERNACIONAL PTE LTD, teniendo por objeto la comercialización de toda clase de pescados y mariscos y su centro de operaciones sito en la calle Ibáñez de Bilbao n° 13,1° izquierda de Bilbao.

El acusado Maximiliano , desde el 8 de julio de 2004 desempeñó los cargos de apoderado y secretario del consejo de administración de la mercantil TRIMARINE y desde el día 28 de mayo de 2007 desempeñó además el cargo de gerente en virtud de un contrato de alta dirección, cesando en todos ellos en fecha 16 de junio de 2011, al haber sido despedido por la sociedad, despido declarado procedente por la jurisdicción social.

El desempeño de estos cargos entre las fechas indicadas, hicieron del acusado el único gestor real de la mercantil, decidiendo todos los aspectos de la actividad de ésta y en concreto facturación, la determinación de los proveedores y clientes y los precios a los que se efectuaban las compras y las ventas.

El acusado Sr. Maximiliano ha llevado entre los años 2004 y 2011, por sí mismo o por medio de sociedades mercantiles a él vinculadas, una actividad empresarial y, en particular, toda una serie de operaciones comerciales propias del giro comercial de TRIMARINE y concurrentes con su objeto social. Las sociedades en cuestión son las siguientes:

-APIKALE S.L. (hoy en liquidación concursal)

-MONTE KALAMUA S.A. (hoy en liquidación concursal)

-ALIMENTOS LA FORMIDABLE S.L. (hoy en liquidación concursal)

-CONSERVAS Y ELABORADOS GUAU S.L. (hoy en liquidación concursal).

-ALIMENTOS AROSA S.L. (hoy en liquidación concursal).

También han intervenido en las operaciones que luego se concretan otras sociedades como FACORE, AQUARIUM, ACTEMSA, COMBLAN y BRISIÑA, sociedades éstas gestionadas por amigos o conocidos del Sr. Maximiliano .

El acusado, bien a través de su intervención activa, bien mediante una tolerancia omisiva, ha ejecutado una serie de operaciones comerciales de compra y venta de pescado con perjuicio patrimonial para TRIMARINE (por soporte de un sobrecoste, por pérdida de un margen comercial o por falta de recuperación del precio) y con correlativo beneficio personal para él o para sociedades con las que ostenta vínculos.

Y así ha sucedido :

Cuando ha propiciado- o permitido- la repercusión de un margen comercial desde un proveedor (a él vinculado) a TRIMARINE -al adquirir ésta de aquél cierto producto para su reventa.-GRUPO 1.

Cuando lo que ha ocurrido es que se ha ordenado (directamente por el acusado y en nombre de TRIMARINE) una venta a determinada sociedad (a él vinculada) a un precio inferior a aquél a repercutir por ésta al cliente final (con el cual el precio final ya estaba negociado por el acusado).- GRUPO 2.

Y cuando, TRIMARINE no ha podido recuperar el crédito generado con las sociedades controladas por el acusado (que han revendido a terceros el producto no abonado a TRIMARINE) finalmente en situación concursal.-GRUPO 3.

Respecto del grupo 1- Son cinco operaciones comerciales de compraventa de pescado, ejecutadas en el período comprendido entre los años 2008 y 2009, que parten como vendedora original de la sociedad Apikale y

que pasan sin solución de continuidad y sin margen comercial, como compradores y posteriores revendedores por las mercantiles Aquarium y Facore (vinculadas al Sr. Maximiliano), y que acaban como compradora final, a un precio superior al de compra y, por lo tanto, con un margen para el revendedor en TRIMARINE, resultando de las mismas la apropiación de un beneficio comercial de 8.610 euros (APIKALE, AQUARIUM,FACORE) en perjuicio de TRIMARINE, que soporta finalmente como mayor precio (sobrecoste) dicho margen:

Nº doc.FechaKilosPrecioMargen aplicableMargen otros

D5.1 may-08 36.939 2,090 - 2.995

D5.1 may-08 2.919 1,890 - 234

D5.1 may-08 1.988 3,300 - 199

D5.2 Ago-09 78.753 1,019 - 2.406

D5.3 Ago-09 46.933 2,00 - 2.816

Transacciones **167.532** 8.610

Las del grupo 2 son 19 operaciones comerciales de compra y venta de pescado, ejecutadas en el periodo comprendido entre los arios 2005 y 2011, que parten como vendedora original de TRIMARINE, que pasan como compradores y posteriores revendedores por las mercantiles AQUARIUM,MONTE KALAMUA,ACTEMESA,COMBLAN Y BRISIÑA, en las que interviene como comprador e intermediario ante el cliente final APIKALE, y que concluyen en diversos clientes finales resultando de las mismas la apropiación de un margen comercial de 229.895 euros (APIKALE) y 79.358 euros (otras sociedades vinculadas con el Sr. Maximiliano) en perjuicio de TRIMARINE, que ve desplazado un margen comercial que debía haber permanecido en la sociedad.-

nº docFechaKilosPrecioMargen aplicableMargen otros

D5.4 Abr-05 49.490 2,650 - 7.424

D5.4 Abr-05 49.670 2,650 - 1.529

D5.4 Abr-05 49.510 2,650 - 4.951

D5.5 Jul-08 56.192 3.475 1.405 1.405

D5.5 Jul-08 2.336 2,900 117 117

D5.5 Jul-08 12.594 1,735 630 630

D5.6 Jul-08 24.657 3,800 -- 1.954

D5.7 Jul-08 28.400 1,750 3.266 994

D5.8 Sep-08 93.071 3,800 5.398 5.305

D5.9 Mar-09 321.780 2,975 136.215 ------

D5.10 Mar-09 24.353 2,250 4.871 1.218

D5.10 Mar-09 24.389 2,850 2.927 732

D5.11 Abr-09 51.750 3,000 14.490 -------

D5.12 Oct-09 434.200 0,807 ----- 7.011

D5.13 Oct-09 287.602 1,700 9.031 35.950

D5.14 May-10 342.994 1,800 28.126 6.174

D5.15 Sep-10 154.615 1,282 3.689 3.965

D5.16 May-11 51.975 3,600 5.198 -------

D5.17 jun-11 48.450 3,300 14.535 --------

Transacciones Trimarine es comprador ***2.108.028*** **229.895** ***79.358***

Las del grupo 3 se concretan en las siguientes operaciones. Entre el 26 de enero de 2011 y el 13 de junio de 2011 TRIMARINE vende pescado por un importe total de 2.763.782,60 euros a AROSA. Se giran dieciocho facturas para su cobro y todas son desatendidas a su vencimiento. El producto suministrado a AROSA fue en

todos los casos revendido por ésta de forma inmediata o incluso en el mismo día a APIKALE, la cual revendió la mercancía a terceros pero sin abonar su precio a AROSA.

VENTAS DE TRIMARINE A AROSA

Nº Factura Importe (+IVA)

032L 95.265,72

033L 95.265,72

034L 34.642,08

035L 88.646,40

048L 29.550,02

049L 53.190,03

050L 70.920,04

065L 146.830,16

165L 101.039,40

166L 30.953,45

167L 167.682,31

168L 125.756,06

179L 121.247,28

183R 253.727,64

185L 202.078,80

198L 181.764,00

206R 214.583,42

208R 750.640,07

2.763.782,60

VENTAS DE AROSA A APIKALE

Nº Factura Importe (+IVA)

OT 0002 97.171,03

OT 0001 97.171,03

OT 0004 35.334,92

OT 0003 90.419,33

OT 0005 156.745,80

OT 0007 153.312,48

OT 0008 103.062,18

OT 0009 31.572,51

OT 0010 171.035,96

OT 0011 128.271,96

OT 0012 123.672,23

OT 0013 258.802,19

OT 0014 206.120.38

PRST730000001 185.399,00

PESC725000001 218.875,08

PESC725000002 765.652,87

2.822.618,18

Entre el 17 de marzo de 2011 y el 6 de junio de 2011 se giran por TRIMARINE a FORMIDABLE, dieciocho facturas correspondientes a venta de pescado por un importe total de 1.954.262 euros. El producto suministrado a FORMIDABLE fue en todos los casos revendido por ésta de forma inmediata o incluso en el mismo día a APIKALE, la cual revendió la mercancía a terceros pero sin abonar su precio a LA FORMIDABLE.

VENTAS DE TRIMARINEA LA FORMIDABLE

N9 Factura Importe (+IVA)

111R 66.159,13

154R 440.127,16

151L 587.200,32

1371 11.536,56

136L 5.515,78

1451 7.682,69

146L 10.243,58

147L 5.121,79

148L 2.560,90

1491 12.804,48

155L 118.908,70

156L 120.426,26

157L 153.951,85

161L 23.569,92

162L 23.805,14

160L 181.814,54

201L 173.210,40

2021 9.622, 80

1.954.262,00

VENTAS DE LA FORMIDABLE A APIKALE

N-9 Factura Importe (+IVA)

VA38 67.483,37

VA49 448.929,71

VA50 598.944,33

VA53 11.767,29

VA51 3.013,98

VA52 2.586,50

VA54 39.181,71

VA46 121.284,94

VA47 122.834,79

VA 48 157.030,88

PRST7300001 24.984,12

VA56 24.043,20

700110025 186.041,77

PRST7300001 176.674,61

PRST7300002 9.815,26

1.994.616,36

SEGUNDO.- Maximiliano es español, mayor de edad y carece de antecedentes penales.

SEGUNDO.- La Audiencia de instancia dictó el siguiente pronunciamiento:

"FALLO.- Que condenamos a Maximiliano como autor de un delito continuado de apropiación indebida a la pena de CINCO años de prisión, inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena y ONCE meses de multa con una cuota diaria de 100 euros, con aplicación de la responsabilidad personal subsidiaria prevista en el artículo 53 del Código Penal en caso de impago. Asimismo le condenamos a el pago en concepto de responsabilidad civil a favor de TRIMARINE SPAIN de la suma de 5.035.907, 60 euros, cantidad que deberá incrementarse en lo que resulte de la aplicación del interés legal. También se le condena al pago de las costas incluidas las de la acusación particular".

TERCERO.- Notificada la Sentencia a las partes, se preparó recurso de casación por infracción de ley y vulneración de precepto constitucional, por el recurrente Maximiliano , que se tuvo por anunciado; remitiéndose a esta Sala Segunda del Tribunal Supremo las certificaciones necesarias para su sustanciación y resolución, formándose el correspondiente rollo y formalizándose el recurso, alegando los motivos siguientes:

Motivos aducidos en nombre de Maximiliano .

Motivo primero.- Por infracción de precepto constitucional al amparo del art. 852 LECrim (derecho a un proceso con todas las garantías). **Motivo segundo**.- Por infracción de precepto constitucional al amparo del art. 852 LECrim por vulneración del derecho fundamental a la intimidad, al secreto de las comunicaciones y a la protección de datos personales previstos en el art. 18.1, 18.2 y 18.4 CE. **Motivo tercero.- (subsidiario del motivo 2º).-** Por infracción de ley al amparo del art. 849.2º LECrim por indebida ignorancia del contenido literosuficiente de determinados documentos obrantes en autos. **Motivo cuarto**.- Por infracción de precepto constitucional al amparo del art. 852 LECrim por vulneración del derecho a la presunción de inocencia (art. 24.2 CE). **Motivo quinto.-** Por infracción de precepto constitucional al amparo del art. 852 LECrim por vulneración del derecho fundamental a la legalidad previsto en el art. 25.1 CE, y del derecho a la libertad (art. 17.1 CE). **Motivo sexto.-** Por infracción de ley al amparo del art. 849.1 LECrim por aplicación indebida de los arts. 252 y 250.1-5º CP (apropiación indebida cualificada). **Motivo séptimo.-** Por infracción de ley al amparo del art. 849.1 LECrim por aplicación indebida de los arts. 109 y 110 CP.

CUARTO.- El Ministerio Fiscal se instruyó del recurso interpuesto por el recurrente, impugnando todos sus motivos. La representación legal de Trimarine Internacional Spain, S.L. evacuó el trámite de instrucción conferido impugnando también el recurso. La Sala lo admitió a trámite, quedando conclusos los autos para señalamiento y Fallo cuando por turno correspondiera.

QUINTO.- Realizado el señalamiento para Fallo se celebraron la deliberación y votación prevenidas el día 5 de julio de 2018.

SEXTO.- Con fechas 19 de julio y 11 de septiembre de 2018 se dictaron autos de prórroga para dictar sentencia por un plazo de quince días y veinte días más respectivamente.

FUNDAMENTOS DE DERECHO

PRIMERO.- Por razones que aparecerán a lo largo del discurso argumental se anticipa el estudio del motivo segundo del recurso interpuesto por el condenado. Propugna la nulidad del examen efectuado del ordenador personal del acusado y, consiguientemente, la inutilizabilidad de todas las pruebas derivadas de ese escrutinio en el que se pudo acceder -se dice- a *miles* de correos electrónicos del acusado. Estaríamos ante pruebas afectadas por la prohibición consagrada en el art. 11.1 LOPJ y, por tanto, inaptas para fundar una condena.

La información obrante en tal ordenador, de uso habitual de Maximiliano , recurrente, y obtenida mediante el análisis no consentido del mismo, constituiría la base que sustenta el informe que daría lugar a la querella y en último término a la condena.

El examen se realizó a través de un programa informático que permitía seleccionar, por su contenido, correos electrónicos sin necesidad de abrirlos (vid. STC 26/2018, de 3 de marzo). Según referencias de los peritos, se seleccionaron 20.722 documentos y/o correos electrónicos con esa metodología. A la postre, solo 113 de ellos proporcionaron información relevante para los fines buscados.

SEGUNDO.- Sinteticemos los antecedentes de orden fáctico necesarios para dirimir esta cuestión. Solo conociendo el contexto y, singularmente, determinados elementos clave, se pueden ofrecer respuestas

atinadas sobre la legitimidad o no desde el punto de vista del art. 11.1 LOPJ de la actuación llevada a cabo por la empresa:

a) El acusado trabajaba como directivo para TRIMARINE SPAIN, S.L. Estaba ligado con ella por un contrato laboral de alta dirección.

b) El 17 de junio de 2011, con presencia notarial, un perito a instancia de esa mercantil se personó en sus oficinas y obtuvo *copia espejo* del ordenador que utilizaba habitualmente el querellado (en esa fecha en Estados Unidos donde se había desplazado siguiendo indicaciones de su empleadora).

c) El día anterior, 16 de junio, se había procedido al despido del ahora recurrente (por tanto, antes del examen del ordenador) al detectarse actuaciones que despertaban vehementes sospechas de deslealtad vinculada a su participación en empresas dedicadas a la misma actividad que su principal.

d) Entre los correos finalmente seleccionados (113), algunos serían ajenos a las relaciones comerciales de Trimarine. Se referían a otras empresas; justamente aquéllas en las que el acusado mantenía intereses.

e) El acusado no había asumido, al menos de forma explícita, la obligación de usar el ordenador en exclusiva para actividades o comunicaciones de la empresa. No existía prohibición de comunicaciones ajenas a sus funciones como gerente.

f) Tampoco había sido advertido de una hipotética reserva por parte de la empresa de su facultad para examinar tal dispositivo. Ni expresa ni tácitamente autorizó que la empresa pudiese acceder a las cuentas de correo usadas por él.

g) No ha quedado fehacientemente demostrado que el ordenador fuese de la titularidad de la empresa. Este dato -hay que apostillar- es irrelevante, como aclara incidentalmente con acierto la sentencia: lo importante a los efectos que ahora interesan no es la titularidad real, sino quién sea el usuario (y si lo era o no con exclusividad; hay que presumir que sí: nadie ha insinuado un uso compartido).

h) El examen del ordenador usado por el acusado (también, según se deduce de las actuaciones, se revisó el contenido del disco duro del dispositivo de otra empleada sin que conste ni su anuencia ni su oposición, y sin que esté delimitado si del mismo se obtuvo algún rendimiento probatorio), se llevó a cabo mediante una herramienta informática que, según explicaron los peritos, resultaba metódica y selectiva: solo se accedió a los archivos en los que aparecían unas palabras clave previamente acotadas. Eso permitía discriminar entre unos archivos y otros para acceder exclusivamente a aquéllos relacionados con tales "chivatos".

i) Asimismo se adoptaron cautelas para asegurar la fidelidad del copiado y mantener los efectos a disposición de quien pudiese recabar una nueva pericial para contrastar que se había llevado a cabo con las garantías necesarias para preservar la autenticidad.

Este es, ordenada y sintéticamente expuesto, el escenario sobre el que debemos resolver. Aparece como una encrucijada en la que confluyen lineas de fuerza en tensión y múltiples cuestiones en que la jurisprudencia no siempre ha ofrecido respuestas uniformes o coincidentes.

Hay que decidir primeramente si se puede hablar de violación de un derecho fundamental predicable de esa actuación de la mercantil **(a)**. Si la respuesta es afirmativa habrá que ventilar a continuación si *in casu* eso arrastra la inutilizabilidad de la prueba **(b)**. Finalmente y en un tercer escalón es preciso indagar sobre el alcance de tal consecuencia **(c)**, si es que se afirma.

TERCERO.- La extensión que deba conferirse a las facultades de supervisión del empresario en el marco de una relación laboral y, en concreto, si está habilitado para verificar el uso que da uno de sus empleados a los dispositivos informáticos o aquellos otros aptos para comunicaciones puestos a su disposición es cuestión salpicada de aristas, matices y recovecos. Contamos con un relativamente nutrido ramillete de resoluciones de distintos ámbitos jurisdiccionales. Su doctrina no siempre ha sido homogénea. Ni es lineal. Se detectan algunas discrepancias y muchos matices diferentes, a veces manifestación de una evolución interpretativa. Incluso en el seno de un mismo órgano se pueden apreciar divergencias y cambios. No es momento de hacer un recorrido exhaustivo; ni siquiera de brindar una panorámica completa de esa evolución o de esa jurisprudencia en la que merecerían apartados específicos destacados el TC (v.gr. SSTC 173/2011 de 7 noviembre, 96/2012, de 7 de mayo o 170/2013, de 7 de octubre), el TEDH (SSTEDH 3 abril 2007, *caso Copland),*la Sala Cuarta de este Tribunal (pronunciamientos varios que van desde la STS de 26 de septiembre de 2007 a las muy recientes 226/2017, de 17 de marzo y 119/2018, de 8 de febrero) o de esta misma Sala Segunda (STS 528/2014, 16 de junio que es analizada e invocada por Audiencia, recurrente y recurridos). Algunas referencias iremos haciendo en la medida en que resulten pertinentes: se trata de resolver este asunto concreto, y no de elaborar un tratado sobre un tema que tanta jurisprudencia y literatura ha alumbrado en los últimos años como consecuencia del imparable y acelerado desarrollo de las TICs.

Que hay derechos fundamentales en juego nadie puede dudarlo: como se ha dicho gráficamente, con frase feliz y, por ello muy repetida, los trabajadores no dejan ni su intimidad ni el resto de sus derechos en las puertas de la oficina o empresa.

También es una obviedad por nadie discutida que la relación laboral impone modulaciones, en esos derechos, aunque nunca absolutas, como se ha preocupado de resaltar la jurisprudencia (vid arts. 18 y 20.3 del Estatuto de los trabajadores; de redacción un tanto obsoleta y no acompasada con las nuevas -o ya no tan nuevas- realidades tecnológicas). Esas limitaciones admisibles en el seno de la relación empresario-trabajador no serían sin más extrapolables a otros ámbitos (vid. voto particular de la STC 26/2018, de 3 de marzo).

"...hemos declarado -afirma nuestro Tribunal Constitucional- que la intimidad protegida por el art. 18.1 CE no se reduce a la que se desarrolla en un ámbito doméstico o privado; existen también otros ámbitos, en particular el relacionado con el trabajo o la profesión, en que se generan relaciones interpersonales, vínculos o actuaciones que pueden constituir manifestación de la vida privada (STC 12/2012, de 30 de enero, FJ 5). Por ello expresamente hemos afirmado que el derecho a la intimidad es aplicable al ámbito de las relaciones laborales (SSTC 98/2000, de 10 de abril , FFJJ 6 a 9; 186/2000, de 10 de julio , FJ 5)". (vid igualmente STS -Sala 4ª- 119/2018, de 8 de febrero).

CUARTO.- Cuáles sean los derechos fundamentales implicados en la descrita medida intrusiva de investigación o vigilancia es punto que necesita aclaración. No es baladí. El nivel de protección y los requisitos para una injerencia legítima varían según cuál sea el derecho afectado. Una cosa es el derecho al secreto de las comunicaciones blindado en el art. 18.3 CE; otra la intimidad; y otra el derecho a la autodeterminación informativa. Hay puntos comunes e interferencias pero su reconocimiento constitucional está diferenciado. Eso arrastra a regímenes legales no idénticos. No son derechos coextensos ni asimilables en su blindaje normativo.

Para entrometerse en las comunicaciones ajenas en curso es indispensable consentimiento o autorización judicial. A ese supuesto alude principalmente la famosa y por todas citada STS 528/2014 (ponencia del Excmo. Sr. D. José Manuel Maza). De ahí que introduzca en el *obiter dicta* que representa todo su discurso sobre este tema, una incidental pero relevante modulación: no es lo mismo un proceso de comunicación en marcha que un proceso de comunicación cerrado. Solo el primero está indiscutiblemente vinculado al derecho al secreto de las comunicaciones. En el segundo caso se detectan profundas diferencias. Estaremos más bien en el campo de la intimidad, la privacidad o, en su caso, la autodeterminación informativa.

A este argumento se agarran sentencia de instancia querellante, y Ministerio Fiscal para rechazar las conclusiones que pretende alcanzar el recurrente: se habría accedido a correos ya recepcionados. No hubo necesidad de abrirlos *ex novo.* Esa actuación se asemeja, no a la interceptación de una correspondencia que no ha llegado todavía a su destinatario, es decir, en tránsito, sino a la incautación, v. gr., de la carpeta donde guarda alguien sus cartas abiertas y ya leídas.

Con independencia de que esa idea, en lo esencial suscribible y suscrita por la jurisprudencia, presenta matices derivados de la dificultad probatoria (habría de sentarse con rotundidad que está acreditado no solo que no se ha accedido a ningún correo sin abrir, sino que el mecanismo informático utilizado lo impedía), las obvias diferencias entre la morfología de las comunicaciones más tradicionales -correspondencia postal; conversaciones telefónicas- y las que se llevan a cabo por estas nuevas vías telemáticas, hace desconfiar de un método exegético basado en el paralelismo sin matices o en un mimetismo absoluto. Esa dualidad (comunicación *in fieri,* comunicación finalizada) no conduce a un escenario de absoluta libertad para el empresario en la segunda alternativa. Están concernidos otros derechos fundamentales: intimidad, autodeterminación informativa.

En esa línea es relevante alguna consideración que extraemos de la STC 70/2002, de 3 de abril: "... la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos". Igual tesis es proclamada por la STC 123/2002, de 20 de mayo. Finalizada la comunicación, la protección constitucional de la comunicación recibida, escapa del ámbito del art. 18.3 de la CE y pasa a residenciarse en el esquema de protección constitucional del derecho a la intimidad (art. 18.1 CE). El criterio ha sido acogido, entre otras, en las SSTS 1235/2002, de 27 de junio , o 1647/2002, de 1 de octubre, ó 864/2015, de 10 de diciembre.

Se puede ver afectada la intimidad pero no la inviolabilidad de las comunicaciones. Y la afectación de la intimidad no exige siempre como presupuesto autorización judicial. Dirá al respecto la STS 777/2013, de 7 de octubre: " *¿Es necesario que toda medida que afecte o pueda afectar a un derecho fundamental sea siempre acordada por un Juez? La respuesta no puede ser rotundamente afirmativa, por más que en ocasiones se puedan leer poco meditadas aseveraciones en ese sentido. Hay casos en que puede hacerlo la Policía*

Judicial de propia autoridad. En muchos supuestos -no todos- si concurre un consentimiento libre (por ejemplo, una exploración radiológica). En otros, incluso coactivamente (cacheos externos). No puede proclamarse precipitadamente el monopolio jurisdiccional como requisito indispensable de toda afectación de un derecho fundamental: la legitimidad constitucional de la detención policial es prueba clara de lo que se afirma. Ni siquiera sería totalmente exacto afirmar que ese es el principio general, solo excepcionado cuando la ley autorice a la policía ***expresamente****. Actuaciones como la obligación a expulsar unas bolsas de la boca (STS de 25 de enero de 1993) o la toma de huellas dactilares (STS de 12 de abril de 1992) pueden resultar admisibles sin necesidad de una previa validación judicial ni de una ley específica habilitante. Será necesaria la previa intervención judicial cuando la Constitución o las Leyes así lo exijan (registros domiciliarios, interceptación de comunicaciones). La afectación de un derecho fundamental por sí sola no es argumento siempre suficiente para postular como presupuesto imprescindible la previa autorización judicial salvo explícita habilitación legal (vid SSTC 206/2007, de 29 de septiembre , ó 142/2012, de 2 de junio ...). Que una actuación pueda menoscabar la intimidad -registro de una maleta o unos papeles- no significa* a priori *y como afirmación axiomática que no pueda ser acordada por autoridades diferentes de la jurisdiccional. La jurisdiccionalidad es exigible en algunos casos; en otros, no. Por eso la constatación de la incidencia de la medida -análisis químico- en la intimidad no comporta automáticamente previa habilitación judicial inexcusable. Como no necesita autorización judicial el interrogatorio de un testigo por la policía a fin de averiguar datos precisos para una investigación, aunque haya afectación de la privacidad propia o de otras personas (preguntar sobre alguna de sus actividades, si el interrogado estuvo con determinada persona, tipo de relaciones mantenidas con ella...). No es que se quiera equiparar uno y otro tipo de diligencias. Es obvio que no son equiparables. Esta consideración se hace a los únicos efectos de destacar que no es legal ni constitucionalmente correcta la ecuación afectación de la intimidad-necesidad inexcusable de previa habilitación judicial. La incidencia en la privacidad no lleva a cuestionar que pueda recibirse declaración a un testigo por la policía como medio de averiguación del delito, sin necesidad de previa autorización judicial motivada, ni de ningún otro requisito especial. Ni siquiera cuando ese interrogatorio, por exigencias de la investigación, conduce a adentrarse en reductos más sensibles de la privacidad...".*

La STS 786/2015, 4 de diciembre, en dirección semejante, aborda un asunto con problemas de acceso a mensajes de correos electrónicos ya recepcionados y guardados en el correspondiente archivo informático. Algunas consideraciones contenidas en la STC 173/2011, de 7 de noviembre le servían de referencia. Estamos ante espacios de privacidad e intimidad lo que no empece a que esos derechos pueden ceder " *en presencia de otros intereses constitucionalmente protegibles, a la vista del carácter no ilimitado o absoluto de los derechos fundamentales, de forma que el derecho a la intimidad personal, como cualquier otro derecho, puede verse sometido a restricciones (SSTC 98/2000, de 10 de abril, FJ 5 ; 156/2001, de 2 de julio, FJ 4 ; 70/2009, de 23 de marzo , FJ 3). Así, aunque el art. 18.1 CE no prevé expresamente la posibilidad de un sacrificio legítimo del derecho a la intimidad -a diferencia de lo que ocurre en otros supuestos, como respecto de los derechos reconocidos en los arts. 18.2 y 3 CE -, su ámbito de protección puede ceder en aquellos casos en los que se constata la existencia de un interés constitucionalmente prevalente al interés de la persona en mantener la privacidad de determinada información"* (STS 786/2015).

QUINTO.- Algunos precedentes alientan la aparición de un derecho vinculado a los mencionados pero con cierta vocación de emanciparse para cobrar autonomía e identidad propias. Partiendo de la plurifuncionalidad de los datos que se almacenan en cualquier ordenador y otros dispositivos asimilables por su capacidad de acumular información vinculada a una persona (*smartphone*) se conviene en la necesidad de un tratamiento unitario a partir de la proclamación de un **derecho al entorno digital**. Sería un derecho de nueva generación que serviría para alumbrar y justificar distintos escalones de protección jurisdiccional (SSTS 342/2013, de 17 de abril; 587/2014, de 24 de febrero, y 587/2014, de 18 de julio).

De ahí que en nuestra renovada legislación procesal haya emergido en fechas recientes, como diligencia específica que reclama garantías singulares (diferentes al registro de un vehículo o una maleta, por ejemplo) el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a) LECrim y ss, introducidos por la LO 13/2015, de 5 de octubre). Es normativa, no aplicable al presente supuesto: el mandato va dirigido a las fuerzas policiales y, además, es legislación no vigente en el momento de los hechos. Pero ayuda la referencia en cuanto que en buena medida tal legislación se limita a conferir formato normativo a ideas ya presentes y exigidas en jurisprudencia precedente.

Es buena guía, por ello, para interpretar la normativa previgente. Se aprecia una diferencia no simplemente cuantitativa, sino también cualitativa entre lo que supone registrar los cajones de la mesa que un empleado despedido venía utilizando, o sigue usando; y el acceso a un dispositivo electrónico de exclusivo uso como es un ordenador. En este caso hay un *plus* determinado no solo porque puede suponer *desnudar* virtualmente a una persona, sino porque incide también en otro derecho de nueva generación como es la autodeterminación informativa.

Esta idea era repetida en la jurisprudencia, antes de la citada reforma de la LECrim que surge a remolque de elaboraciones jurisprudenciales. Los principios rectores establecidos en el nuevo art 588 bis a) LECrim, según asume expresamente la exposición de motivos de la LO 13/2015, suponen la proclamación normativa de axiomas que el Tribunal Constitucional, y también esta Sala, ya habían definido como determinantes de la validez de los actos de injerencia en la privacidad del investigado en un proceso penal.

Justificando la regulación establecida en el nuevo capítulo VIII del Título Octavo de la Ley Procesal Penal la exposición de motivos expone: " *descarta cualquier duda acerca de que esos instrumentos de comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción. De ahí la exigente regulación respecto del acceso a su contenido".*

Expresiones como esa recuerdan indisimuladamente pronunciamientos de esta Sala Segunda.

La autorización se precisa tanto en los supuestos en los que al aparato se ocupa durante un registro domiciliario, como cuando se incauta fuera del domicilio del investigado.

Establecen los nuevos artículos 588 sexies a y b, de la LECrim:

"Artículo 588 sexies a. Necesidad de motivación individualizada . 1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de **ordenadores,** instrumentos de comunicación telefónica o telemática **o dispositivos de almacenamiento masivo de información digital** o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

Artículo 588 sexies b. Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado.

La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización".

La necesidad de esta autorización judicial (subsidiaria del consentimiento: si el afectado accede de forma libre, no hay cuestión) obedece a la consideración de estos instrumentos como esferas de almacenamiento de una serie compleja y densa de datos que afectan de modo muy variado a la intimidad del investigado (comunicaciones tuteladas por el art 18 3º CE; contactos, fotografías, archivos personales, tuteladas por el art 18 1º CE; datos personales y de geolocalización, que pueden cobijarse en el derecho a la protección de datos, art 18 4º CE). La contemplación disgregada de cada una de esas realidades con regímenes de protección diferenciados resultaría ineficaz. Permitido, por ejemplo, el acceso directo de los agentes policiales a estos instrumentos para investigar datos únicamente protegidos por el derecho a la intimidad (v.gr., los contactos incluidos en la agenda), no se podría acceder o consultar también otros datos tutelados por el derecho a la inviolabilidad de las comunicaciones albergados en el mismo dispositivo. El Legislador con buen criterio ha optado por otorgar un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando ese derecho constitucional de nueva generación, el derecho a la protección del propio entorno virtual.

SEXTO.- Este criterio, como se ha dicho, estaba presente en la doctrina jurisprudencial de esta Sala. La STS 342/2013, de 17 de abril, es punto claro de referencia. Eso y su apelación a otros precedentes justifica la longitud de la cita que sigue:

" *A) El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar -de hecho, normalmente albergará- información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los*

programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones.

En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policía, ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal.

La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso ***su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria.*** *Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de* nomen iuris *propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital.*

Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías.

La STC 173/2011, 7 de noviembre , recuerda la importancia de dispensar protección constitucional al cúmulo de información personal derivada del uso de los instrumentos tecnológicos de nueva generación. Allí puede leerse el siguiente razonamiento: " si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. ***A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie***

de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información" .

Así por ejemplo, la STS 444/2014, de 9 de junio recuerda que " *conviene hacer referencia a la STC (Pleno) 115/2013, de 9 de mayo , que se refiere al acceso por parte de los agentes de la Policía Nacional, sin consentimiento del afectado y sin autorización judicial, a la relación de números telefónicos contenidos en la agenda de contactos telefónicos de un teléfono móvil (entendiendo exclusivamente por agenda el archivo del teléfono móvil en el que consta un listado de números identificados mediante un nombre) que fue encontrado por los agentes en el lugar de comisión de un delito, y considera que esta actuación no afecta al derecho al secreto de las comunicaciones (art. 18.3 CE) del usuario de dicho aparato de telefonía, sino exclusivamente al derecho a la intimidad (art. 18.1 CE). Recuerda el Tribunal Constitucional que la intervención de las comunicaciones requiere siempre de autorización judicial, pero el art. 18.1 CE no prevé esa misma garantía respecto del derecho a la intimidad, por lo que se admite la legitimidad constitucional de que la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que exista la suficiente y precisa habilitación legal y se hayan respetado las exigencias dimanantes del principio de proporcionalidad. Estima el Tribunal Constitucional que con el acceso a la agenda de contactos del teléfono móvil del recurrente los agentes de policía no obtienen dato alguno concerniente a un proceso de comunicación emitida o recibida mediante dicho aparato, sino únicamente un listado de números de teléfono introducidos voluntariamente por el usuario del terminal, equiparable a los recogidos en una agenda de teléfonos en soporte de papel, por lo que debe descartarse que el derecho al secreto de las comunicaciones quede afectado por esta actuación policial.*

Distinto sería el caso si se hubiese producido el acceso policial a cualquier otra función del teléfono móvil que pudiera desvelar procesos comunicativos, como por ejemplo el acceso al registro de llamadas entrantes y salientes".

Con carácter general señala la STS 493/2010, de 25 de abril, que " *sobre el examen o la observación del listado de teléfonos de la agenda de un teléfono móvil tiene establecido la jurisprudencia de esta Sala que no se trata de una intromisión en el derecho al secreto de las comunicaciones sino en el derecho a la intimidad; por lo cual,* ***se le aplica la doctrina que el Tribunal Constitucional tiene plasmada sobre la limitación de ese derecho fundamental con motivo de las investigaciones delictivas por los agentes policiales, principalmente las SSTC 114/1984, de 14 de febrero , 70/2002, de 3 de abril , y 120/2002, de 20 de mayo*** .

La doctrina de esta Sala de Casación, según las reiteradas sentencias que ha dictado sobre casos similares relativos al conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles (SSTS 316/2000, de 3-3 ; 1235/2002, de 27-6 ; 1086/2003, de 25-7 ; 1231/2003, de 25-9 ; 449/2006, de 17-4 ; y 1315/2009, de 18-12), afirma que la agenda de un teléfono móvil, entendiendo por agenda, en este caso, el archivo de dicho aparato en el que consta un listado de números identificados normalmente por un nombre, es equiparable a una agenda en soporte de papel o electrónica con el mismo contenido de direcciones y números de teléfono. Por ello su registro u observación no supone la inmisión o injerencia en el derecho al secreto de las comunicaciones sino en el derecho a la intimidad, con las importantes consecuencias que de ello se derivan. Pues así como la injerencia en el primero de tales derechos requeriría, sin duda ni excepción, la previa autorización judicial, por venir así expresamente dispuesto en el artículo 18.3 de nuestra Constitución , la diligencia que afecta a la intimidad del investigado se encuentra, en cambio, legalmente autorizada a las fuerzas del orden, ***siempre por supuesto que la misma resulte justificada con arreglo a los criterios de urgencia y necesidad y que se cumpla el requisito de proporcionalidad al ponderar los intereses en juego en el caso concreto"***..

SÉPTIMO.- En el orden social la STS (Sala Cuarta) de 26 septiembre de 2007, marcó los primeros lineamientos de esta materia en el ámbito de la contratación laboral. Una revisión técnica por el defectuoso funcionamiento del ordenador de un trabajador, desveló antiguas visitas a archivos pornográficos causantes quizás de la ralentización del ordenador. Eso desencadenó su despido.

El Tribunal Supremo recalca "... la existencia de un **hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores.** Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio".

El reconocimiento de esa expectativa impone el deber a la empresa de poner en conocimiento del trabajador los mecanismos que el empresario se reserva para hacer realidad ese control. "... Lo que debe hacer la empresa -razona la sentencia- de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos ".

La sentencia, pese a reconocer -con cita de la sentencia del TEDH de 3 de abril de 2007- la conexión entre el derecho a la intimidad y la información que proporciona el conocimiento de la navegación por Internet, sugiere la necesidad de un distinto tratamiento entre el derecho a la inviolabilidad de las comunicaciones, derivado del uso del correo electrónico, y otras manifestaciones de la intimidad. Fruto de esas reflexiones será la confirmación de la ilegalidad del despido del recurrente: "... en efecto, en el supuesto de que efectivamente los archivos mencionados registraran la actividad del actor, la medida adoptada por la empresa, **sin previa advertencia** sobre el uso y el control del ordenador, supone una lesión a su intimidad en los términos a que se ha hecho referencia en los anteriores fundamentos. Es cierto que la entrada inicial en el ordenador puede justificarse por la existencia de un virus, pero la actuación empresarial no se detiene en las tareas de detección y reparación, sino que, como dice con acierto la sentencia recurrida, en lugar de limitarse al control y eliminación del virus, "se siguió con el examen del ordenador" para entrar y apoderarse de un archivo cuyo examen o control no puede considerarse que fuera necesario para realizar la reparación interesada. De esta forma, no cabe entender que estemos ante lo que en el ámbito penal se califica como un "hallazgo casual" (sentencias de 20 de septiembre, 20 de noviembre y 1 de diciembre de 2006), pues se ha ido más allá de lo que la entrada regular para la reparación justificaba".

La STS de 8 de marzo de 2011 (Sala 4ª) insiste en esas bases maestras: "... no consta que, de acuerdo con las exigencias de la buena fe, la empresa hubiera establecido previamente algún tipo de reglas para el uso de dichos medios -con aplicación de prohibiciones absolutas o parciales- ni tampoco que se hubiera informado a los trabajadores de que se iba a proceder al control y de los medios a aplicar en orden a comprobar su correcto uso, así como las medidas a adoptar para garantizar la efectiva laboral del medio informático cuando fuere preciso".

La clave de la ilegitimidad de la intromisión y, consiguientemente, de la nulidad probatoria se sitúa en la vulneración de la expectativa de intimidad por parte del trabajador. Una expectativa, basada en un uso social de tolerancia respecto de una moderada utilización personal de esos instrumentos, que, no es ajena a los contenidos de la protección constitucional del derecho a la intimidad. Sólo el conocimiento anticipado por parte del trabajador (deducible o explícito) de que puede ser objeto de fiscalización por el empresario, legitimaría el acto de injerencia en los sistemas informáticos puestos a su alcance por la entidad para la que trabaja.

La doctrina vuelve a aparecer en la STS de la misma Sala de 6 de octubre de 2011. La empresa había enviado a todos los trabajadores una carta, recibida y firmada por quienes luego resultaron despedidos, "... quedaba terminantemente prohibido el uso de medios de la empresa (ordenadores, móviles, internet, etc.) para fines propios tanto dentro como fuera del horario de trabajo". Transcurridos unos meses de la recepción de esa misiva, la empresa decidió hacer una comprobación sobre el uso de sus medios de trabajo para lo que procedió a la motorización de los ordenadores de los trabajadores afectados. Para ello se valió de la instalación de un "software de monitorización" que la sentencia de instancia definía como "... un sistema "pasivo" poco agresivo que no permitía acceder a los archivos del ordenador que están protegidos por contraseñas de cada uno de los usuarios".

El Pleno de la Sala de lo Social -con cinco votos particulares que disentían del criterio mayoritario- declaró la procedencia del despido, confirmando así el criterio de la instancia. Lo que singularizaba el presente caso -se razona- era que "... existía una prohibición absoluta que válidamente impuso el empresario sobre el uso de medios de la empresa (ordenadores, móviles, internet, etc.) para fines propios, tanto dentro como fuera del horario de trabajo, y no caprichosamente sino entre las sospechas fundadas de que se estaban desobedeciendo las órdenes impartidas al respecto. Y sentada la validez de prohibición tan terminante, que lleva implícita la advertencia sobre la posible instalación de sistemas de control del uso del ordenador, no

es posible admitir que surja un derecho del trabajador a que se respete su intimidad en el uso del medio informático puesto a su disposición. Tal entendimiento equivaldría a admitir que el trabajador podría crear, a su voluntad y libre albedrío, un reducto de intimidad, utilizando un medio cuya propiedad no le pertenece y en cuyo uso está sujeto a las instrucciones del empresario".

Hay un relevante signo diferenciador entre el acceso por el empresario y el acceso por agentes públicos; el primero en virtud de sus facultades de supervisión del trabajo que se presta por una relación laboral; los segundos, en virtud de potestades públicas. En el primer caso nos movemos en el marco de una relación contractual entre particulares. La clave estará en si el trabajador ha consentido anticipadamente reconociendo esa capacidad de supervisión al empresario y, por tanto, cuenta con ello; está advertido; es decir, es una limitación conocida y contractualmente asumida.

En las relaciones con los Poderes Públicos, sin embargo, no cabe esa "cesión" anticipada o renuncia previa a ese espacio de intimidad virtual.

El reconocimiento previo, explícito o implícito, de esa facultad de empresario constituye el *punctum dolens* la clave, en el ámbito de las relaciones laborales. En una investigación penal lo será la autorización judicial o el consentimiento actual.

OCTAVO.- En el ámbito de la jurisprudencia constitucional, resultan de obligada cita, por su estrecha conexión con el tema que nos ocupa, dos precedentes. El primero, de ellos, la STC 241/2012, de 17 de diciembre . El segundo, la STC 170/2013, de 7 de octubre .

La demanda de amparo que dio lugar al proceso que culminó con la STC 241/2012, entendía que la empresa habría vulnerado los derechos de la trabajadora al acceder a los ficheros informáticos en que quedaban registradas las conversaciones mantenidas con otra trabajadora a través de un programa de mensajería instalado por ellas mismas en un ordenador de uso común y sin clave de acceso. Esas conversaciones de carácter íntimo, a su juicio, estaban protegidas por el mandato constitucional del secreto de las comunicaciones. No concurrían, en otro orden de cosas, exigencias de necesidad, idoneidad y proporcionalidad de la medida para salvaguardar el interés empresarial de vigilar y controlar la actividad laboral.

El Tribunal Constitucional rechaza la queja "... fue la propia demandante y la otra trabajadora quienes realizaron actos dispositivos que determinaron la eliminación de la privacidad de sus conversaciones, al incluirlas en el disco del ordenador en el cual podían ser leídas por cualquier otro usuario, pudiendo trascender su contenido a terceras personas, como aquí ocurrió al tener conocimiento la dirección de la empresa". El conocimiento de lo que había sido objeto de distintas conversaciones sólo fue posible porque ambas interlocutoras "...con sus propios actos, (...) con su voluntaria actuación", hicieron posible -como de hecho ocurrió- que un tercero, trabajador de la empresa que informó a sus superiores, accediera a esas conversaciones.

Descartó también infracción alguna del derecho a la inviolabilidad de las conversaciones estimando: **a)** que el flujo de comunicación entre ambas trabajadoras se había verificado a partir de un canal abierto de comunicación; **b)** que el acceso a lo comunicado se había producido como consecuencia de un hallazgo casual de otro trabajador que lo comunicó a la dirección de la empresa. Se razona así: "... estamos ante comunicaciones entre dos trabajadoras que se produjeron al introducirse el programa en un soporte de uso común para todos los trabajadores de la empresa sin ningún tipo de cautela. En este sentido, quedan fuera de la protección constitucional por tratarse de formas de envío que se configuran legalmente como comunicación abierta, esto es, no secreta" (FJ 7º).

Del mismo modo, se excluyen de la protección constitucional aquellas informaciones obtenidas en virtud de hallazgos no intencionados: "... no puede calificarse como vulneradora del derecho al secreto de las comunicaciones la intervención empresarial analizada, por cuanto que, además, la misma se produce a partir de un hallazgo casual de uno de los usuarios, trabajador de la empresa, que transmite su contenido a la dirección, ajustando ésta su actuación de control a un suficiente canon de razonabilidad, sin que se atisbe lesión de derechos fundamentales de las trabajadoras afectadas puesto que el acceso al contenido del programa de mensajería "Trillian" sólo se produjo cuando la empresa tuvo conocimiento de la instalación del programa".

En relación a los datos que se contienen en ordenadores u otros soportes informáticos, este Tribunal en la STC de 7 de noviembre, FJ 3, recordó que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos y con carácter general, ha venido reiterando que el poder de dirección del empresario, es imprescindible para la buena marcha de la organización productiva (organización que refleja otros derechos reconocidos constitucionalmente en los arts. 33 y 38 CE). Expresamente en el art. 20 del texto refundido de la Ley del estatuto de los trabajadores (LET) se contempla la posibilidad de que el empresario, entre otras

facultades, adopte las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales. **Mas esa facultad ha de producirse, en todo caso, dentro del debido respeto a la dignidad del trabajador, como expresamente nos lo recuerda igualmente la normativa laboral en los arts. 4.2 c) y 20.3 LET (STC, de 10 de julio, FJ 5).**

De esta forma, los equilibrios y limitaciones recíprocos que se derivan para ambas partes del contrato de trabajo suponen que también las facultades organizativas empresariales se encuentran limitadas por los derechos fundamentales del trabajador, quedando obligado el empleador a respetar aquéllos (STC de 18 de octubre, FJ 4).

5. Concretamente, en relación con la utilización de ordenadores u otros medios informáticos de titularidad empresarial por parte de los trabajadores, puede afirmarse que la utilización de estas herramientas está generalizada en el mundo laboral, correspondiendo a cada empresario, en el ejercicio de sus facultades de autoorganización, dirección y control fijar las condiciones de uso de los medios informáticos asignados a cada trabajador. En el marco de dichas facultades de dirección y control empresariales no cabe duda de que ***es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales****.*

Las consideraciones precedentes no impiden que se proceda a dotar de ***una regulación*** *al uso de las herramientas informáticas en la empresa y, en particular, al uso profesional de las mismas* ***, por medio de diferentes instrumentos como órdenes, instrucciones, protocolos o códigos de buenas prácticas,*** *de manera que la empresa no quede privada de sus poderes directivos ni condenada a permitir cualesquiera usos de los instrumentos informáticos sin capacidad alguna de control sobre la utilización efectivamente realizada por el trabajador.*

A tal fin y en pura hipótesis ***, pueden arbitrarse diferentes sistemas, siempre respetuosos con los derechos fundamentales, orientados todos ellos a que los datos profesionales o los efectos de la comunicación profesional llevada a cabo alcancen al conocimiento empresarial, sin que se dé, en cambio, un acceso directo o cualquier otra intromisión del empresario o sus mandos en la empresa, en la mensajería o en los datos personales de los trabajadores, si este uso particular ha sido permitido****. En ese ámbito, aunque pudiera caber la pretensión de secreto de las comunicaciones, actúa a su vez legítimamente el poder directivo, con la posibilidad consiguiente de establecer pautas de flujo de la información e instrucciones u órdenes del empresario que aseguren, sin interferir injustificadamente el proceso de comunicación y sus contenidos, el acceso a los datos necesarios para el desarrollo de su actividad, al igual que ocurre en otros escenarios en los que, sin control directo del empresario, los trabajadores a su servicio desarrollan la actividad laboral ordenada en contacto con terceros y clientes.*

Partiendo del uso común del ordenador, desde la perspectiva de los derechos fundamentales, es esencial determinar si elacceso a los contenidos de los ordenadores u otros medios informáticos de titularidad empresarial puestos por la empresa a disposición de los trabajadores, y en un medio al que puede acceder cualquiera, vulnera el art. 18.3 CE , para lo que ***habrá de estarse a las condiciones de puesta a disposición, pudiendo aseverarse que la atribución de espacios individualizados o exclusivos puede tener relevancia desde el punto de vista de la actuación empresarial de control.*** *Es el caso de asignación de cuentas personales de correo electrónico a los trabajadores, o incluso a las entidades sindicales, aspecto éste que fue abordado en nuestra STC 281/2005 , de 7 de noviembre .* ***El ejercicio de la potestad de vigilancia o control empresarial sobre tales elementos resulta limitada por la vigencia de los derechos fundamentales, si bien los grados de intensidad o rigidez con que deben ser valoradas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin****.*

Lo expuesto no impide afirmar que en el desarrollo de la prestación laboral pueden producirse comunicaciones entre el trabajador y otras personas cubiertas por el derecho al secreto del art. 18.3 CE , ya sean postales, telegráficas, telefónicas o por medios informáticos, por lo que pueden producirse vulneraciones del derecho al secreto de las comunicaciones por intervenciones antijurídicas en las mismas por parte del empresario o de las personas que ejercen los poderes de dirección en la empresa, de otros trabajadores o de terceros. **Así lo ha afirmado también la jurisprudencia del *Tribunal Europeo de Derechos Humanos en la Sentencia de 3 de abril de 2007, caso Copland c. Reino Unido, § 41, al recordar que, según la reiterada jurisprudencia del Tribunal (SSTEDH de 25 de junio de 1997, caso Halford c. Reino Unido, § 44 , y 16 de febrero de 2000, caso Amann c. Suiza , § 44) las llamadas telefónicas que proceden de locales profesionales pueden incluirse en los conceptos de "vida privada" y de "correspondencia" a efectos del artículo 8 del Convenio, y del mismo modo los correos electrónicos enviados desde el lugar de trabajo y la información derivada del seguimiento del uso personal de Internet".***

El segundo de los precedentes apuntado - STC 170/2013, de 7 de octubre- considera prueba lícita la aportación por la empresa al proceso por despido del contenido de determinados correos electrónicos del trabajador, obtenidos mediante el acceso a un ordenador portátil propiedad de la empresa. Se ponían de manifiesto contactos con terceros ajenos a la empresa, a los que había remitido información detallada sobre las previsiones de cosecha de 2007 y 2008. Esta conducta, implicaba la comisión de la falta laboral muy grave, (revelación de datos de reserva obligada).

Recuerda el Tribunal Constitucional, como pautas para el ejercicio de balanceo entre los intereses convergentes, que ... "el contrato de trabajo no puede considerarse como un título legitimador de recortes en el ejercicio de los derechos fundamentales que incumben al trabajador como ciudadano, que no pierde su condición de tal por insertarse en el ámbito de una organización privada" (STC 88/1985, de 19 de julio)". Pero tampoco puede desconocerse -como ya se anticipó en la STC 99/1994, de 11 de abril - "... que la inserción en la organización laboral modula aquellos derechos en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva; reflejo, a su vez, de derechos que han recibido consagración en el texto de nuestra norma fundamental (arts. 38 y 33 CE). En aplicación de esta necesaria adaptabilidad de los derechos del trabajador a los razonables requerimientos de la organización productiva en que se integra, se ha afirmado que "manifestaciones del ejercicio de aquéllos que en otro contexto serían legítimas, no lo son cuando su ejercicio se valora en el marco de la relación laboral".

A partir de esta doctrina, el Tribunal examina si en el caso concreto existía o no una expectativa de confidencialidad digna de protección constitucional. Concluye que los términos en los que el convenio colectivo regía las relaciones laborales entre la empresa y el trabajador -en el que se tipificaba como falta leve la " ... utilización de los medios informáticos propiedad de la empresa (correo electrónico, Intranet, Internet, etc.) para fines distintos de los relacionados con el contenido de la prestación laboral"-, neutralizan cualquier expectativa de intimidad. "... cabe entender (...) en el presente supuesto -argumenta la citada STC- que no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial. La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe [arts. 5.a) y 20.2 y 3 LET]. En el supuesto analizado la remisión de mensajes enjuiciada se llevó pues a cabo a través de un canal de comunicación que, conforme a las previsiones legales y convencionales indicadas, se hallaba abierto al ejercicio del poder de inspección reconocido al empresario; sometido en consecuencia a su posible fiscalización, con lo que, de acuerdo con nuestra doctrina, quedaba fuera de la protección constitucional del art. 18.3 CE ".

Tampoco aprecia esta sentencia vulneración de la intimidad (art. 18.1 CE). El trabajador no estaba en condiciones de asegurar su propio espacio de exclusión, en la medida en que "... la habilitación por la empresa de esta herramienta informática como medio para llevar a cabo el adecuado cumplimiento de la prestación de trabajo y el hecho de que su uso para fines distintos de los relacionados con el contenido de la prestación laboral estuviera tipificado en el Convenio colectivo aplicable como infracción sancionable impiden considerar que su utilización quedara al margen del control empresarial". Los mecanismos de fiscalización fueron considerados acordes con elementales exigencias de proporcionalidad: "... la naturaleza de la infracción investigada y su relevancia para la entidad, no pueda apreciarse que la acción empresarial de fiscalización haya resultado desmedida respecto a la afectación sufrida por la privacidad del trabajador. En consecuencia y como ya se ha indicado, una vez ponderados los derechos y bienes en conflicto en los términos vistos, este Tribunal considera que la conducta empresarial de fiscalización ha sido conforme a las exigencias del principio de proporcionalidad".

NOVENO.- Hito reciente y extremadamente relevante de la jurisprudencia recaída en esta materia viene constituido por STEDH de 5 de septiembre de 2017 (Gran Sala): asunto ***Barbulescu***. Es invocada por el recurrente. Otras sentencias posteriores del mismo órgano, inciden también en esta temática aunque de forma oblicua (videovigilancias: SSTEDH de 28 de noviembre de 2017 asunto *Antori and Murkon* de 9 de enero de 2018 asunto *López Ribalde* ; o también examen de un ordenador, asunto *Libert*, STEDH de 22 de febrero de 2018)

No puede decirse que la sentencia ***Barbulescu*** II sea totalmente rupturista con los criterios que han ido cristalizando en nuestra jurisprudencia, someramente reseñada. Pero aporta y concreta al establecer con diáfana claridad parámetros de inexcusable respeto empujando a nuevas modulaciones y matizaciones que ya han aparecido en la jurisprudencia laboral (STS -Sala 4ª- 119/2018, de 8 de febrero, que realiza una síntesis clara e íntegramente trasladable al ámbito penal del estado de la cuestión tras ***Barbulescu***).

Acudiendo a la clásica técnica, se habla de la insoslayable necesidad de ponderar los bienes en conflicto. De una parte, el interés del empresario en evitar o descubrir conductas desleales o ilícitas del trabajador. Prevalecerá solo si se atiene a ciertos estándares que han venido a conocerse como el test ***Barbulescu***.

Se enuncian criterios de ponderación relacionados con la *necesidad* y *utilidad* de la medida, la inexistencia de otras vías menos invasivas; la presencia de *sospechasfundadas*... Algunos se configuran como premisas de inexcusable concurrencia. En particular, no cabe un acceso inconsentido al dispositivo de almacenamiento masivo de datos si el trabajador no ha sido advertido de esa posibilidad y/o, además, no ha sido expresamente limitado el empleo de esa herramienta a las tareas exclusivas de sus funciones dentro de la empresa (los usos sociales admiten en algún grado y según los casos, como se ha dicho, el empleo para fines personales, creándose así un terreno abonado para que germine una expectativa fundada de privacidad que no puede ser laminada o pisoteada).

El resto de factores de ponderación entrarán en juego para inclinar la balanza en uno u otro sentido solo si se cuenta con ese presupuesto. En otro caso, habrá vulneración aunque exista necesidad, se use un método poco invasivo, etc...

DÉCIMO.- Esta es la clave que nos permite resolver este asunto. Podrían existir razones fundadas para sospechar y entender que el examen del ordenador era una medida proporcionada para esclarecer la conducta desleal y evaluar los perjuicios. Se buscó, además, una fórmula lo menos invasiva posible. Pero faltaba un *prius* inexcusable.

Si existiese esa expresa advertencia o instrucción en orden a la necesidad de limitar el uso del ordenador a tareas profesionales, (de la que en podría llegar a derivarse una anuencia tácita al control o, al menos, el conocimiento de esa potestad de supervisión) y/o además alguna cláusula conocida por ambas partes autorizando a la empresa a medidas como la aquí llevada a cabo; o, si se hubiese recabado previamente el consentimiento de quien venía usando de forma exclusiva el ordenador (en caso de negativa, nada impedía recabar la autorización necesaria) pocas dudas podrían albergarse sobre la legitimidad de la actuación indagatoria llevada a cabo por la empresa. Pero en las circunstancias en que se llevó a cabo hay que afirmar que el ordenamiento ni consiente, ni consentía en la fecha de los hechos, tal acción intrusiva por ser lesiva de derechos fundamentales.

UNDÉCIMO.- Lo que vicia la prueba es el acceso no legítimo. En esto hay que dar la razón al recurrente.

Es indiferente a esos efectos que luego no aparezcan datos vinculados materialmente a la intimidad; o que todo lo que se examinase careciese de calidad para ser protegido por su enlace directo con actividades delictivas; o incluso que se tratase en su totalidad de información que tuviese derecho a conocer la querellante, como titular del negocio. Las comunicaciones y determinados espacios de privacidad (el domicilio, los aparatos de almacenamiento masivo de datos) se blindan legalmente con murallas que constituyen la materialización de la protección del derecho fundamental, abstracción hecha de que en concreto se identifique una violación material de la intimidad. Hay violación del derecho al secreto de la correspondencia cuando se abre una carta enviada postalmente, aunque luego en la misma solo figuren, v.gr., los resultados conocidos de la última jornada liguera o un inocuo folleto publicitario de un juego de sartenes; o cuando se accede ilegítimamente a un ordenador ajeno y solo aparecen videojuegos infantiles; o se penetra en el domicilio de una persona y allí solo se encuentra el catre donde duerme (o, únicamente, su cadáver); o se intercepta un teléfono y no se llega a conocer ninguna conversación; o tan solo alguna totalmente inofensiva desde el punto de vista de la intimidad (encuesta sobre el funcionamiento del servicio de telefonía, v.gr.).

Esa muralla solo cede en virtud del consentimiento del afectado (actual o anticipado, v. gr. ha dejado las llaves de su domicilio al vecino o al portero de la finca) o de autorización judicial.

La evaluación de si ha existido vulneración ha de realizarse mediante un juicio *ex ante*: no depende de que efectivamente se hayan obtenido elementos sensibles desde el punto de vista de la privacidad. Y se protege aunque *ex post* se compruebe que solo se han descubierto comunicaciones o efectos a los que debía tener acceso el promotor de la intromisión: que se invada el ordenador usado por una persona y se descubra que solo contiene fotos de quien accede ilegítimamente a él; o que se entre sin autorización en el domicilio del supuesto ladrón para recuperar el móvil sustraído con un método -llamadas al número específico para localizarlo- que va a permitir acceder en exclusiva al efecto que es de titularidad del invasor, no convierte en legítima la intromisión.

La valoración de la legitimidad de la actuación inicial (acceso al ordenador que usaba el querellado) no puede hacerse más que mediante un juicio *ex ante*. A esos efectos es indiferente que solo se hayan buscado elementos que tuvieran relación con la actividad mercantil de la empresa o que se haya eludido cuidadosamente adentrarse en cualquier archivo o comunicación en la que se percibiese el más mínimo aroma

de vinculación con la intimidad o la privacidad. Esto, que solo es posible dilucidar en un juicio *ex post,* no cambia ni puede cambiar la valoración que se hace *ex ante.*

¿Se puede entrar en un domicilio particular sin consentimiento del titular ni autorización judicial cuando se sabe no ocupado en ese momento y con el único fin de recuperar un efecto robado tiempo antes que está a la vista? No. Sin matices.

¿Se puede acceder a un dispositivo de almacenamiento masivo usado por un empleado con la firme y decidida finalidad de acceder en exclusiva a los archivos relacionados con la empresa? En principio no. Tan solo cuando haya precedido un consentimiento expreso o derivado implícita e inequívocamente del compromiso asumido previamente por el trabajador, será legítima esa actuación. El empleo de una herramienta de filtrado del tipo búsqueda "ciega" no legitima por sí sola la injerencia (vid. voto particular STC 23/2018; la sentencia mayoritaria no aborda esa cuestión).

Limitar los perjuicios de la intromisión a lo estrictamente necesario consiguiendo no afectar a elementos ajenos a la empresa o relacionados con la intimidad del usuario no sirve para revertir en legítima la intromisión *ab initio* ilegítima. Ha de ser una valoración apriorística y no a expensas de los concretos contenidos obtenidos. La ilegitimidad no deriva del contenido obtenido, ni de la forma de acceso más o menos intrusiva, sino del mismo acceso inconsentido y no advertido previamente.

DUODÉCIMO.- Tampoco se debe reputar decisiva a estos efectos la difícil cuestión de dilucidar si todos los *mails* examinados habían sido ya recepcionados o tuvieron que abrirse algunos antes de que hubiese accedido a ellos el acusado. Aparte de las dificultades -casi imposibilidad- de determinarlo, no es dato al que aquí haya que otorgar relevancia decisoria. No puede descartarse la presencia de correos sin abrir. Y tampoco en estos casos -registro de dispositivos de almacenamiento masivo de datos- ese elemento accesorio puede convertirse en la piedra de toque que traiga la solución. No se atiene a parámetros de lógica esa distinción. Adquiere pleno sentido en los procesos de comunicación postales (interceptación antes de que se cierre el proceso de comunicación o una vez agotado éste: la carta ya abierta que se guarda en un bolsillo es diferente -muy diferente- a la carta que se abre antes de llegar a su destinatario); pero esos moldes no son trasladables sin más a las comunicaciones vía telemática o telefónica.

Como hemos visto, la jurisprudencia ha situado la clave de la legitimidad de la injerencia empresarial en la ausencia de toda expectativa de confidencialidad por parte del trabajador que sufre la intromisión que puede basarse en una cláusula contractual o en una advertencia del empresario o en la legítima instrucción expresa de limitar el uso del dispositivo a fines laborales. La existencia de un precepto incorporado al convenio del sector donde se prohíbe el uso personal de los instrumentos informáticos, la suscripción de una cláusula que reserva al empresario esa facultad o, en fin, la comunicación, por uno u otro medio, del uso de mecanismos tecnológicos de fiscalización, difuminan el espacio de exclusión del trabajador.

Ninguno de esos presupuestos legitimadores aparece aquí.

DÉCIMO TERCERO.- Sentada esa primera conclusión -se produjo la violación, quizás bienintencionada, y derivada de no extremar el máximo de diligencia o las precauciones exigibles ante una materia muy sensible y una situación normativa y jurisprudencial de cierta incertidumbre; pero, a fin de cuentas, violación de derechos fundamentales-, el siguiente paso ha de ser contestar a este interrogante: ¿qué consecuencia hay que anudar a ello?

La contestación reclama descender dos peldaños. Primero, delimitar si tal actuación queda afectada por la prohibición contenida en el art. 11.1 LOPJ. En caso afirmativo, determinar si la supresión de las pruebas que han de ser invalidadas (en este caso los correos electrónicos o archivos extraídos de ese ordenador, así como las pruebas vinculadas a esa de una forma tan directa y jurídicamente relevante que pueda hablarse de una *conexión de antijuricidad)* nos arrastra a un vacío probatorio o, si, por el contrario, existen pruebas convalidables por ser desconectables o por emanar de fuentes independientes.

En el primer nivel -aplicabilidad del art. 11.1 LOPJ- dos cuestiones podrían despertar alguna duda: la actuación ilegítima corre a cargo de un particular y no de los poderes públicos; y, por otra parte, éste se enfrentaba a una situación normativa, si no confusa, al menos no cristalina, en el momento de la injerencia. La penuria normativa y los zigzagueos jurisprudenciales podrían haber hecho creer a la empresa que esa modalidad investigadora en defensa de sus intereses y ejercida de forma comedida se ajustaba al ordenamiento.

Estamos ante temas de inequívoco alcance constitucional. Las pautas a las que ha de guardar fidelidad este Tribunal, no solo como tributo debido a la seguridad jurídica, sino especialmente por respeto al principio de legalidad - art. 5.1 LOPJ- son las consagradas y reiteradas por el Tribunal Constitucional, máximo intérprete de la norma suprema del ordenamiento. A impulsos de sus resoluciones en materia de amparo se ha apuntado el anclaje constitucional de la exclusión de la prueba obtenida con violación de derechos fundamentales; y

se han pergeñado las excepciones que legítimamente pueden y deben admitirse. Entre esas excepciones se encuentran la falta de conexión de antijuridicidad cuando se trata de prueba refleja; o la buena fe del agente.

En el origen del discurso sobre la inutilizabilidad de la prueba obtenida con violación de derechos se situaba una finalidad disuasoria y profiláctica: una protección eficaz de los derechos fundamentales exige esa drástica medida. La mejor garantía para proteger los derechos fundamentales, y soslayar los riesgos de que el celo investigatorio acabe ignorándolos, es negar todo valor a las pruebas que se alcancen vulnerando esos derechos. Así, el Estado, el agente de la autoridad y también el particular, percibe nítidamente la inutilidad de esa actuación y se estimula el escrupuloso cumplimiento de todas las garantías por quienes toman parte en una investigación.

Puestos en la balanza los valores enfrentados, merece la pena sacrificar la eventual "injusticia" que representa no castigar a ciertos culpables para dotar de mayor efectividad a la protección de los derechos fundamentales. La hipotética sanción por la violación de esos derechos fundamentales de todos puede no ser suficientemente disuasoria. Empíricamente es comprobable que el rechazo absoluto del valor probatorio de los elementos así obtenidos es una medida más eficaz en la tutela de los derechos fundamentales y ahuyenta en mayor grado la tentación de actuaciones ilegales.

Tras la teoría de la prueba ilícita late como en tantas materias en el mundo del derecho una ponderación de valores en conflicto. Ante la disyuntiva entre el derecho del Estado a sancionar al autor de un delito y la **eficaz** protección de los derechos fundamentales se opta por esto último: es un valor preferible frente a la sanción en todo caso y a toda costa de todos los responsables penales. Es una decisión de política criminal, no ya correcta, sino muy acertada.

En algunos sistemas (como el norteamericano: decisiones de la Corte Suprema, Stone v. Powell, 1976; U.S. v. León, 1984; III v. Krull, 1987), la regla se vincula indisimuladamente a la contención de comportamientos inadecuados de los agentes estatales. En nuestro ordenamiento no es pacífica esa afirmación. Se habla más de protección objetiva de los derechos fundamentales.

Pero sea cual sea la plataforma de la que se parta no puede hacerse abstracción de las circunstancias que rodean la infracción.

DÉCIMO CUARTO.- Nos enfrentamos aquí a una ilicitud atribuible no a órganos del Estado, sino a particulares. Este dato tiene relevancia; mucha si se asume como punto de partida el fundamento preventivo de la teoría de la prueba ilícita.

No hay duda de la eficacia de los derechos fundamentales entre particulares (*drittewirkung*), aunque no se puede desconocer que su construcción teórica y su fortificación legal y práctica ha surgido y crecido sobre todo en tensión frente a los poderes estatales. Por definición algunos derechos fundamentales solo son oponibles al poder estatal (derecho a no confesarse culpable -con algún matiz-, y en general, derecho a un proceso con todas las garantías). Es verdad que el art. 11.1 LOPJ no introduce distinción alguna en este sentido. La inutilizabilidad de la prueba obtenida con violación de derechos se predica de todos los casos y de todos los procesos, más allá de que el agente infractor sea estatal o un particular. También en el proceso civil (vid. art. 287 LEC) o en el laboral rige la previsión.

Admitido eso, no puede ocultarse que por tradición, por teleología, por ponderación de derechos fundamentales en tensión y por sus finalidades, el juego de esa norma, de máxima intensidad cuando la violación proviene de un agente estatal, consiente más modulaciones en el caso de particulares (son frecuentes en el derecho comparado las regulaciones de esta materia que dejan al margen las actuaciones de particulares: U.S.A., Francia, Holanda, México, Bélgica con matices).

Por eso la jurisprudencia reciente ha admitido que en el caso de particulares estamos en un terreno más permeable a excepciones (SSTS 87/2017, de 19 de abril ó 116/2017, de 23 de febrero).

En las relaciones entre particulares, las exigencias de la doctrina de la prueba ilícita son más débiles porque las necesidades de protección y la potencialidad de agresión son en principio menores. Normalmente basta con las sanciones penales o, en su caso, las reacciones desde el ordenamiento privado.

Desde esa óptica, por ejemplo, cuando no se constata en la actuación del particular la finalidad de **obtener** pruebas para hacerlas valer en un proceso judicial puede eludirse la tajante sanción del art. 11.1 LOPJ en cuanto no está presente la finalidad a que obedece la norma (STS 116/2017, de 23 de febrero).

Pero en otros casos, rige el mandato del art. 11.1 LOPJ.

En este supuesto hay que apresurarse, además, a advertir en la relación empresario-empleado existe un matiz diferencial que introduce algún desequilibrio y no permite hablar de plena horizontalidad.

La flexibilidad interpretativa, no puede llegar al punto de traicionar la dicción del art. 11.1 LOPJ.

La empresa realizó esas indagaciones con el propósito de hacer valer como prueba, en su caso, los datos recabados en un proceso judicial. Eso impide escapar del ámbito de art. 11.1 LOPJ.

DÉCIMO QUINTO.- Con anclaje en la tesis partidaria de la finalidad profiláctica, se ha sostenido que para tachar a una prueba de *ilícita*, debe exigirse, usando un paralelismo penal, una conducta antijurídica y culpable (aunque sea simple negligencia). No sería "ilícita" a estos efectos la acción, ni por tanto la prueba, cuando se ha actuado de buena fe, con la convicción de que la conducta se ajustaba al ordenamiento y sin indiligencia, indiferencia o desidia reprobables. Desde esa premisa se conformó lo que se llamó la excepción de la *buena fe* se viene aplicando por el Tribunal Supremo americano; alguna vez, precisamente, con motivo de pronunciamientos jurisprudenciales: no podía exigirse a unos agentes que se apartasen de lo establecido en una ley que posteriormente fue declarada inconstitucional por la Justicia. Las actuaciones realizadas al abrigo de tal ley, antes de su expulsión del ordenamiento jurídico, eran válidas en cuanto existía buena fe.

La STC 22/2003, de 10 de febrero abrió paso en nuestro ordenamiento a esa excepción *"La inconstitucionalidad de la entrada y registro obedece, en este caso, pura y exclusivamente, a un déficit en el estado de la interpretación del Ordenamiento que no cabe proyectar sobre la actuación de los órganos encargados de la investigación imponiendo, a modo de sanción, la invalidez de una prueba, como el hallazgo de una pistola que, por sí misma, no materializa en este caso, lesión alguna del derecho fundamental (vid. STC 49/1999, de 5 de abril , FJ 5) y que, obviamente, dada la situación existente en el caso concreto, se hubiera podido obtener de modo lícito si se hubiera tenido conciencia de la necesidad del mandamiento judicial.* ***En casos como el presente, en que el origen de la vulneración se halla en la insuficiente definición de la interpretación del Ordenamiento, en que se actúa por los órganos investigadores en la creencia sólidamente fundada de estar respetando la Constitución y en que, además, la actuación respetuosa del derecho fundamental hubiera conducido sin lugar a dudas al mismo resultado, la exclusión de la prueba se revela como un remedio impertinente y excesivo que, por lo tanto, es preciso rechazar. ... no cabe hablar de que se haya vulnerado el derecho a un proceso con todas las garantías pues, en este caso, la vulneración del derecho a la inviolabilidad del domicilio es, por decirlo de algún modo, un mero accidente.*** ".

Sin embargo, en el caso presente, a la vista de la jurisprudencia existente y predominante en el momento de la actuación empresarial cuya licitud fiscalizamos ahora, se podía y debía haber extremado la cautela: no existiendo advertencia de que el ordenador había de ser usado exclusivamente para los fines de la empresa y no constando al empleado que la empresa se reservaba la potestad de su examen, por mucho que se utilizasen métodos informáticos especialmente poco invasivos y selectivos, constituía un cierto atrevimiento (una indiligencia), no recabar antes el consentimiento del titular o, en su defecto, la autoridad judicial. Regía ya un cuerpo de doctrina jurisprudencial que alertaba sobradamente sobre la dudosa legalidad de esa actuación. Algo de osadía se aprecia en la iniciativa adoptada por la empresa.

La prueba no es rescatable; no puede utilizarse.

DÉCIMO SEXTO- Como explica la STS 299/2013, de 27 de febrero, cuando se declara la nulidad de actos de prueba (lo que, lleva aparejada su invalorabilidad o inutilizabilidad), como hacemos ahora hay que explorar cuál es la solución pertinente, (por todas STC 208/2007, de 24 de septiembre, 135/2011, de 12 de septiembre, y 144/2012, de 2 de julio).

a) Si la prueba indebidamente valorada por ser nula o ilícita era prescindible y puede asegurarse sin temor a equivocaciones que, suprimida, el pronunciamiento de condena no pierde sustento y hubiese sido el mismo se impondrá mantener la condena. Alguna argumentación subsidiaria de la acusación particular discurre por esta senda.

b) Si la prueba anulada se revelaba como esencial, de forma que el fallo condenatorio al borrar esa prueba pierde todo o, al menos, su principal apoyo, habrá que proceder directamente a la absolución por aplicación de la presunción de inocencia. Es esto lo que viene a impetrar en casación el acusado.

c) Solo cuando el marco probatorio sea lo suficientemente complejo como para no poder deducirse de forma indubitada qué influjo pudo tener la prueba anulada, es decir si era o no decisiva para fundamentar la convicción o se limitaba a corroborar lo que ya podía considerarse acreditado por otros elementos, habrá que reenviar la causa al Tribunal *a quo,* para que dicte una nueva sentencia sin contar con esa prueba que se considera vulneradora de derechos fundamentales o para celebrar un nuevo juicio (si se atisba pérdida de la imparcialidad en el Tribunal o el modelo de proceso -jurado- no consiente otra alternativa).

En los casos en los que faltan elementos para llegar a una conclusión clara en uno u otro sentido, solo en esos, se deja abierta la cuestión para que de nuevo el órgano de la instancia adopte una nueva decisión sin contar con ese medio probatorio.

DÉCIMO SÉPTIMO.- En el presente caso la supresión de los resultados de ese análisis inconsentido del disco duro del ordenador usado por el recurrente no nos conduce a un desierto probatorio. En algún pasaje de la sentencia se desliza esa idea: algunos de los hechos determinantes de la condena se derivan de prueba documental (contabilidad) que no tiene por qué estar vinculada a los hallazgos en el dispositivo (fuente independiente). A ello alude en su dictamen de impugnación la acusación particular.

El propio dictamen pericial inicial parece distinguir diferentes fuentes de conocimiento: algunas (documentación de la empresa) se antojan separables del escrutinio del ordenador.

Se observa igualmente que existen otras pruebas diferentes -también de carácter personal- a las que no necesariamente ha de extenderse el efecto invalidante, bien por poder estimarse que se ha roto la conexión de antijuricidad según la doctrina de nuestro Tribunal Constitucional -juicio éste que corresponde efectuar en primer lugar al Tribunal que presencia toda la prueba-, bien por poder aplicarse alguna de las diferentes modulaciones que matizan la doctrina de los *frutos del árbol envenenado* (v. gr., descubrimiento inevitable; nexo causal atenuado...: aparte de la jurisprudencia constitucional y de esta Sala, -por todas STC 81/1998, de 2 de abril o SSTS 228/2017, de 3 de abril y 811/2012, de 30 de octubre- vid. SSTEDH , Asunto *Prada,* de 3 de marzo de 2016 ; de 1 de junio de 2010 *asunto Gäfgen;* o de 22 de mayo de 2018 , asunto *Svetina* .

No estamos en condiciones en casación, al margen, por tanto, de toda inmediación, ni de dilucidar esas cuestiones, ni, una vez discriminado el material probatorio inservible de aquél que puede fundar una sentencia, ponderar si puede considerarse destruida la presunción de inocencia. Eso obliga a reenviar la causa al Tribunal *a quo* para un nuevo enjuiciamiento que, partiendo de esa premisa ahora afirmada -el examen del ordenador vulneró derechos fundamentales- determine qué pruebas no están afectadas por esa realidad y si las mismas pueden apoyar o no un pronunciamiento de culpabilidad.

DÉCIMO OCTAVO.- El primer motivo del recurso denuncia una cuestión procesal: se habría dictado condena por hechos introducidos tardíamente durante la instrucción (apartado cuarto del escrito de acusación: los recogidos al final del *factum* y fechados entre el 17 de marzo de 2011 y el 6 de junio siguiente (actos de insolvencia). Se denuncia que:

a) No se oyó en declaración al acusado sobre esos hechos.

b) No son mencionados en el auto de acomodación previsto en el art. 779.5.4ª LECrim: (folios 1207 y ss)

c) No fueron objeto de apertura del juicio oral. La fijación de fianza se limitó a los tres primeros apartados del escrito de acusación.

Sobre esa triple base concluye la defensa que no era posible la condena. Faltarían los presupuestos necesarios para una acusación válida.

La defensa protestó por tal irregularidad en sucesivos momentos.

Cuestiona el recurrente en su escrito de contestación a las impugnaciones la postura adoptada por la representación del Ministerio Público que no es congruente con la mantenida en la instancia. Si ante la Audiencia se opuso a la petición de la acusación particular que reclamaba el enjuiciamiento de esos hechos no abarcados por el auto de transformación; ahora, sin embargo, defiende la sentencia que en ese punto no le dio la razón y se inclinó por la tesis de la acusación no pública.

No tiene razón el recurrente en esa objeción. El Fiscal no está atado por el principio de sujeción a los propios actos (art. 94 del Reglamento Orgánico del Ministerio Fiscal de 1969). Es esa una consecuencia derivada de su ubicación institucional y de las misiones que le atribuye el art. 124 CE. No es obstáculo para su petición que no sea armónica con su posición procesal en la instancia (por todas STS 504/2017, de 3 de julio).

No se ha actuado correctamente desde el punto de vista procesal. Ante la introducción de un grupo diferenciado de hechos con cierta relevancia (aunque penalmente fuesen enmarcables en el único delito continuado por el que finalmente se condena), devenía imperativa una nueva toma de declaración al acusado.

Puede matizarse que en el caso de un delito continuado, como éste, no siempre será ello imprescindible -pensemos en la aparición de otro pasaporte falsificado en una causa en la que se investiga una falsificación masiva de ese tipo de documentos-. Pero resulta insoslayable cuando los hechos nuevos suponen una relevante ampliación fáctica del contenido del único delito continuado y gozan de autonomía o entidad propias. Eso sucede aquí.

Era asimismo exigible que en el auto de acomodación al procedimiento abreviado se incorporasen esos hechos. El auto guarda silencio sobre ellos, seguramente de manera inercial y no como fruto de una decisión consciente y reflexiva del Instructor. Pero era obligada su mención para permitir en su caso que la defensa pudiese recurrir y reclamar el sobreseimiento parcial respecto de esos hechos. En todo caso la falta de

inclusión no puede interpretarse como un inexistente sobreseimiento tácito, inexistente (STS 239/2014, de 1 de abril). Otro entendimiento supondría privar a la acusación, de la posibilidad de recurrir por la exclusión de un material fáctico que había introducido de forma correcta en el proceso, pasando a integrarse en el objeto procesal que se va delimitando progresivamente.

El auto de apertura del juicio oral tampoco se ajusta estrictamente a lo ideal. Pero no puede afirmarse como interpreta el recurrente que no se abriese el juicio oral por tales hechos. El sobreseimiento exige una resolución expresa: no caben sobreseimientos tácitos. Estando tales hechos relatados y calificados en el escrito de la acusación particular y no excluyéndose en el auto de apertura del juicio oral, no se puede decir que fueron expulsados mediante un sobreseimiento implícito (STS 513/2017, de 19 de junio). En absoluto, por más que la fianza -también seguramente cuantificada de forma inercial- sugiera que solo se están contemplando los tres grupos de operaciones objeto de querella inicial.

Ahora bien, no toda irregularidad procesal ha de dar lugar a la nulidad. Solo aquéllas que producen **efectiva indefensión.**

El recurrente optó por tratar de extraer rendimiento de esa irregularidad procesal. Es una decisión estratégica legítima, aunque encerraba algún peligro. Dilapidó las posibilidades reales de que gozaba para erradicar la supuesta indefensión: no solo renunció a proponer prueba (con una salvedad) sobre esos nuevos hechos (que conocía perfectamente: aparecieron en la instrucción -escrito de 26 de junio de 2013- y se relatan en el acta de acusación de la entidad querellante); sino que también se reservó toda explicación guardando silencio sobre esos hechos. Podía haberlos justificado en el acto del juicio oral. Ha preferido hacer pivotar su defensa frente a esa acusación sobre ese argumento procesal: tenía que haber sido oído sobre ellos en fase de instrucción.

Estamos ante un delito continuado (¿no podrían haber aparecido esos hechos y motivar una modificación del escrito de acusación en el mismo acto del juicio oral sin perjuicio de lo establecido en el art. 746.6?). Esa realidad introduce modulaciones en la forma en que debe abordase tal cuestión. Era obligado, en todo caso, conocimiento conjunto y acumulado de todos lo hechos al poder tratarse de un solo delito desde el punto de vista jurídico (anterior art. 300 LECrim).

Por otra parte, parece, y en eso se apoya tanto la sentencia como las partes recurridas, que la indefensión producida si ha llegado a tener consecuencias es precisamente como consecuencia de esa decisión estratégica de la defensa: renunciar a defenderse para no *blanquear* el defecto procesal detectado. Su declaración en el acto del juicio oral, y la aportación de las pruebas que tuviese por pertinentes para desmontar esa acusación a través de sus conclusiones provisionales hubiesen disipado todo atisbo de indefensión. De hecho resalta la sentencia con tino que llegó a proponer una prueba encaminada precisamente a desvirtuar esa acusación, prueba que se practicó. En otro contexto quizás serían refrendables los argumentos de la Audiencia.

Pero en trance de solventar este motivo, siendo así que la sentencia va a ser necesariamente anulada como consecuencia de la declaración de inutilizabilidad de algunos medios de prueba, hay que contemplar sin excesiva rigidez este segundo motivo. No ha sido correcta la secuencia procesal ni respetuosa con los derechos del acusado. Siendo cierto que ha tenido ocasión de neutralizar las condiciones de indefensión generadas con una actuación mínimamente diligente, no puede exigírsele renunciar a esa forma de defensa articulada.

Se va a estimar por ello el motivo para que se desvanezca incluso la apariencia de indefensión. La nulidad se extenderá por ello a lo actuado a partir del auto de acomodación en el que debían haberse mencionado los hechos introducidos previa toma de declaración sobre ellos al investigado. De esa forma éste se encontrará en condiciones de proponer en la fase de investigación diligencias de prueba que podrán ser consideradas necesarios o no. Culminada la fase de instrucción deberá proseguir el procedimiento resolviéndose en la forma prevista en el art. 779 LECrim respecto de todos los hechos introducidos.

Lo que no es dable, como pretende el recurrente, es deducir de una irregularidad en la tramitación del procedimiento una causa de exención de la responsabilidad criminal. El defecto señalado no lleva a la absolución, sino a la reposición de las actuaciones al momento en que se produjo para su subsanación y continuación y nueva terminación de la causa con arreglo a derecho.

El art. 240.2 LOPJ no supone un óbice para declarar la nulidad con ese alcance. La naturaleza de la queja lleva implícita esa petición, y, además, en definitiva todo motivo de casación supone necesariamente una solicitud de anulación ("casar" la sentencia) sin perjuicio de que en ocasiones esa anulación se vea sucedida por otra sentencia (segunda sentencia) zanjando el fondo. No es dable aquí por tales razones dictar esa segunda sentencia. La tarea de la Sala de casación queda culminada con la primera sentencia y el reenvío de la causa al órgano de origen para reponerla al momento indicado y culminarle con arreglo a derecho (STS 299/2013, de 27 de febrero).

DÉCIMO NOVENO.- Habiéndose estimado parcialmente el recurso, las costas habrán de declararse de oficio

F A L L O

Por todo lo expuesto, en nombre del Rey y por la autoridad que le confiere la Constitución, esta sala ha decidido

1.- ESTIMARparcialmente el recurso de casación interpuesto por **Maximiliano ,** contra sentencia nº 23/2017 dictada el 1 de junio de 2017 por la Sección Primera de la Audiencia Provincial de Vizcaya en causa seguida contra el recurrente por un delito de administración desleal, **por estimación de los motivos primero y segundo** de su recurso; y en su virtud **casamos y anulamos la sentencia** en los términos expuestos, retrotrayéndose las actuaciones al momento indicado para que se tramiten y concluyan con arreglo a derecho.

2.- Declarar de oficio las costas de este recurso.

Comuníquese esta resolución al Tribunal Sentenciador a los efectos procedentes, con devolución de la causa que en su día remitió, interesándole acuse de recibo.

Notifíquese esta resolución a las partes haciéndoles saber que contra la misma no cabe recurso e insértese en la colección legislativa.

Así se acuerda y firma.

Andres Martinez Arrieta Luciano Varela Castro Alberto Jorge Barreiro

Antonio del Moral Garcia Andres Palomo Del Arco