

ARTÍCULOS

INSPECCIONES DE COMPETENCIA Y SU CONTROL JUDICIAL: ASPECTOS CONSTITUCIONALES Y PENALES

ALFONSO GUTIÉRREZ y FERNANDO LORENTE
Abogados ()*

Competition inspections and rights of the companies: constitutional, criminal and procedural aspects

Recent dawn raids by the CNC have heated an intense debate on the constitutional and criminal boundaries of antitrust inspections in Spain and their judicial control, in particular regarding entry into business premises and wide access to computers and emails. This article explains the applicable legal rules

Inspecciones de competencia y su control judicial: aspectos constitucionales y penales

La frecuencia e intensidad de las inspecciones domiciliarias de la Comisión Nacional de la Competencia en empresas y asociaciones empresariales de todo tipo ha suscitado un amplio debate sobre los límites constitucionales y penales de dichas inspecciones y su control jurisdiccional, en particular por lo que se refiere a la entrada y registro de dependencias empresariales y el acceso generalizado a los ordenadores y correo electrónico de directivos y empleados. El objetivo de este artículo es exponer las principales reglas aplicables.

1 · CONTROL JUDICIAL DE LA ACTIVIDAD INSPECTORA DE LA CNC

1.1 · La autorización judicial previa de la actuación administrativa inspectora de la CNC

El apartado 1 de la disposición adicional séptima de la Ley de Defensa de la Competencia añade un nuevo párrafo al artículo 8.6 de la Ley de la Jurisdicción Contencioso-Administrativa (en lo sucesivo, «LJCA»). Éste ya atribuía, en su redacción precedente, a los Juzgados de lo Contencioso-Administrativo el conocimiento de las autorizaciones para la entrada en domicilios y restantes lugares cuyo acceso requiera el consentimiento de su titular, siempre que ello proceda para la ejecución forzosa de actos de la Administración pública. Se añade ahora una nueva competencia de dichos Juzgados para autorizar los actos de entrada e inspección de determinados recintos —domicilios, locales, terrenos y medios de transporte— acorda-

da por la CNC siempre que, requiriéndose el consentimiento de su titular, éste se opusiera a su ejecución, o existiese riesgo de tal oposición.

Hay un cierto ámbito de redundancia respecto a lo que la Ley ya disponía. Los actos de inspección son formalmente ordenados por el director de investigación (artículo 40 de la LDC). No existe un personal genéricamente habilitado para practicar cualesquiera inspecciones. La orden o autorización de inspección del director debe referirse a un asunto determinado y tener un objeto y alcance determinados, entre otros fines para permitir un control judicial efectivo. Por tanto, los actos de inspección siempre constituyen la ejecución forzosa del acto del director de investigación que ordena su práctica. La norma no puede implicar un ámbito de vías de hecho legitimado directamente por la intervención judicial.

Sin embargo, la nueva norma tenía en el proyecto —antes de su paso por el Senado— un ámbito funcional más extenso que la preexistente, al referirse no sólo a la entrada en domicilios y lugares de acceso restringido, sino a la restricción de cualesquiera derechos fundamentales eventualmente implícita en la actuación administrativa. Era ésta una solu-

(*) Del Área de Público y Procesal (Competencia) de Uría Menéndez (Madrid).

ción, en nuestra opinión, más correcta técnicamente que la introducida en el Senado y finalmente plasmada en la Ley.

La modificación de la disposición adicional séptima en el Senado ha generado además una cierta antinomia, pues el artículo 40 apartados 2 y 4, que no ha sido modificado correlativamente, sigue exigiendo la autorización judicial con un ámbito distinto al de dicha disposición, y sigue hablando, como aquélla en la versión del proyecto, de los supuestos en que la actuación inspectora «implique restricción de derechos fundamentales». Deberá prevalecer el criterio de la necesaria autorización judicial, más allá de para la entrada y registro, para actos que, como la ocupación o el precinto de correspondencia, incidan en el ámbito del artículo 18 CE, por aplicación, como veremos, directa de éste.

Hubiera sido deseable, en cualquier caso, que la ampliación del ámbito de esta técnica de control judicial *ex ante* se produjera de un modo horizontal o general. Carece de sentido que cada legislación sectorial venga a establecer una competencia judicial *ad hoc* para el control judicial previo en las inspecciones o investigaciones administrativas en su campo. Y existen, desde luego, otras en las que cabe la afectación de derechos fundamentales por la actividad inspectora. La nueva norma procesal podría haber sido concebida de modo horizontal o transversal.

1.2. Actuaciones sujetas a autorización

El artículo 18 CE consagra el ámbito de derechos fundamentales que configuran el respeto de la vida privada y familiar a que se refiere el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales. Las intromisiones en el disfrute de dichos derechos sólo son admisibles (artículo 8.2 CEPDH) si, establecidas por la ley (con un grado suficiente de previsibilidad y garantía), persiguen una de las finalidades legítimas contempladas, con la que son proporcionadas, y resultan necesarias en una sociedad democrática para alcanzarlas¹.

Dicho ámbito es algo más que la pura intimidad personal y familiar a que se refiere el apartado 1 del citado precepto constitucional. Las garantías del

ámbito domiciliario y de las comunicaciones de los apartados 2 y 3 del artículo 18 tienen en el modelo español un carácter autónomo y, como veremos, absoluto.

«El domicilio es inviolable». «Ninguna entrada o registro podrá hacerse en él sin el consentimiento del titular o resolución judicial, salvo en caso de flagrante delito». «Se garantiza —también— el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial», que se ha entendido normalmente referida al ámbito exclusivamente penal.

El Tribunal Constitucional estableció tempranamente, desde la Sentencia 22/1984, de 17 de febrero, que la Administración necesita autorización judicial para entrar en domicilios a efectos de ejecutar actos administrativos, de forma que el artículo 18 CE se muestra como un límite a las facultades administrativas de la llamada autotutela ejecutiva. Sin embargo, dicha autorización judicial no será necesaria cuando la entrada en el domicilio sea para ejecutar, no un acto, sino una sentencia contencioso-administrativa que se hubiera pronunciado sobre aquél, según precisó el Tribunal Constitucional en la Sentencia 160/1991, de 18 de julio, que modifica y matiza la doctrina anterior.

Es pacífico en la jurisprudencia constitucional española que la inviolabilidad del domicilio comprende la del domicilio o ámbito de actuación profesional de las personas jurídicas y, en general, de las empresas. En el ámbito europeo, la cuestión tardó más en dilucidarse, pero está definitivamente despejada desde la Sentencia del Tribunal Europeo de Derechos Humanos (en lo sucesivo «TEDH»), de 16 de abril de 2002, en el asunto Stés Colas y otros contra Francia (demanda 37971/1997)², que,

² El Tribunal recuerda que, de acuerdo con la jurisprudencia, el término «domicilio» tiene una connotación más amplia que la palabra inglesa «home» y puede englobar, por ejemplo, la oficina o el despacho de una persona con una profesión liberal (*vid.* Sentencia Niemietz contra Alemania de 16 de diciembre 1992, serie A núm. 251-B, pg. 34, ap. 30). Ya en el asunto Chappel contra el Reino Unido (TEDH 1989, 6), el Tribunal consideró que un registro efectuado en el domicilio de una persona física, que es a la vez la sede de las oficinas de una sociedad dirigida por ella, constituía una injerencia en el derecho al respeto del domicilio, en el sentido del artículo 8 del Convenio (RCL 1979, 2421; ApNDL 3627) (Sentencia Chappel de 30 de marzo 1989, serie A núm. 152-A, pg. 13, ap. 25 b) y pg. 26, ap. 63.). El Tribunal recuerda que el CEPDH es un instrumento vivo que hay que interpretar a la vista de las condiciones de vida actuales (*Vid., mutatis mutandis*, Sentencia Cossey contra el Reino Unido de 27 septiembre 1990 [TEDH 1990, 22], serie A núm. 184, pg. 14, ap. 35 *in fine*). Tratándose de los derechos reconocidos a las socie-

¹ *Vid.*, por todas, STEDH, de 18 de febrero de 2003 en el asunto Prado Bugallo *c. España*.

en la que denomina interpretación dinámica del CEPDH, considera que «ya es hora de reconocer [...] que los derechos garantizados desde el punto de vista del artículo 8 del Convenio pueden ser interpretados para dar cabida a una sociedad, el derecho al respeto de su sede social, su agencia o sus locales profesionales».

Este reconocimiento, visto a la luz de lo dispuesto sobre respeto del CEPDH en el artículo 6.2 del Tratado de la Unión Europea —y sin olvidar el artículo 7 de la Carta de Derechos Fundamentales de la UE, de redacción similar al artículo 8 CEPDH y que es vinculante por sí mismo tras la entrada en vigor del Tratado de Lisboa— conforma los términos en que debe ser interpretado y aplicado el artículo 20 del Reglamento (CE) 1/2003, en el sentido de que la solicitud de mandamiento judicial a que se refieren sus apartados 7 y 8 debe realizarse siempre que el titular del domicilio no preste su consentimiento a la entrada en el domicilio o al examen de sus comunicaciones.

En España, la protección de la inviolabilidad del domicilio no tiene otros límites que el consentimiento del titular o la autorización judicial³.

Y, obviamente, el consentimiento en cuestión, al que se refiere el artículo 18.2 CE, es un consentimiento libre y no obligado, sin que el ejercicio del derecho fundamental en el sentido de exigir la autorización judicial previa para aquietarse a la entrada domiciliaria pueda constituir, en ningún caso, una infracción del ordenamiento. Cuando el artículo 40.2 LDC señala que las empresas y sus asociaciones están obligadas a someterse a las inspecciones que el director de investigación haya autorizado (*rectius* ordenado) se refiere a los mandamientos del director que sean ejecutorios, y éstos sólo lo son si conllevan entrada y registro domiciliarios, una vez obtenida la autorización judicial. Sólo *iocandi causa* puede entenderse la manifestación, expresada —bien que informalmente— en algún foro, de que la exigencia de autorización judicial podría ser sancionada con base en el artículo 62.1 de la LDC⁴.

En un primer momento, la autorización de las intrusiones administrativas en el domicilio fue atribuida a los jueces de instrucción por el antiguo artículo 37.2 de la Ley Orgánica del Poder Judicial (en lo

dades por el CEPDH, procede subrayar que el Tribunal ya ha reconocido, con base en el artículo 41, el derecho a indemnización por el daño moral sufrido por una sociedad desde el punto de vista del artículo 6.1 del CEPDH (*vid.* Sentencia Comingersoll contra Portugal [GS] núm. 35382/1997, aps. 33 a 35, TEDH 2000-IV, de 6 abril de 2000 [TEDH 2000, 123]). En la prolongación de la interpretación dinámica del CEPDH, el Tribunal considera que ya es hora de reconocer, en determinadas circunstancias, que los derechos garantizados desde el punto de vista del artículo 8 pueden ser interpretados para dar cabida a una sociedad, el derecho al respeto de su sede social, su agencia o sus locales profesionales (*vid.*, *mutatis mutandis*, Sentencia Niemietz contra Alemania anteriormente citada, pg. 34, ap. 30).

³ STC 22/2003, de 10 de febrero: «Los límites que la Constitución española establece al ámbito de la inviolabilidad domiciliaria tienen un carácter rigurosamente taxativo (SSTC 22/1984, de 17 de febrero, FJ 3; 160/1991, de 18 de julio, FJ 8; 126/1995, de 25 de julio, FJ 2; 126/2000, de 29 de mayo, FJ 3), a diferencia de otras regulaciones constitucionales que, aun reconociéndola, se remiten, para las excepciones al respecto, a los casos y a las formas establecidas por la ley (así, el art. 14 de la Constitución italiana), o aceptan la posibilidad de que órganos no judiciales acuerden la entrada forzosa en un domicilio en supuestos de urgencia (así, el art. 13.2 de la Ley Fundamental de Bonn). Por el contrario, en el caso de la Constitución española..., fuera de los supuestos de consentimiento del titular y de flagrancia delictiva, ...se posibilita la entrada o registro domiciliario únicamente sobre la base de una resolución judicial. La garantía judicial aparece así como un mecanismo de orden preventivo, destinado a proteger el derecho, y no —como en otras intervenciones judiciales previstas en la Constitución— a reparar su violación cuando se produzca. La resolución judicial, pues, aparece como el método para decidir, en casos de colisión de valores e intereses constitucionales, si

debe prevalecer el derecho del art. 18.2 CE u otros valores e intereses constitucionalmente protegidos» (STC 160/1991, de 18 de julio, FJ 8). En estrecha conexión con lo anterior hemos declarado que la resolución judicial sólo puede cumplir su función en la medida en que esté motivada, constituyendo la motivación, entonces, parte esencial de la resolución judicial misma (SSTC 126/1995, de 25 de julio, FJ 2; 139/1999, de 22 de julio, FJ 2; en idéntico sentido, SSTC 290/1994, de 27 de octubre, FJ 31; 50/1995, de 23 de febrero, FJ 5; 41/1998, de 24 de febrero, FJ 34; 171/1999, de 27 de septiembre, FJ 10; 8/2000, de 17 de enero, FJ 4). Esa exigencia de motivación constituye la vía de verificación de que la actuación judicial ha operado como «garantía de la excepcionalidad de la injerencia permitida por el art. 18.2 CE y, en todo caso, como garantía de la proporcionalidad de la restricción de todo derecho fundamental» (STC 171/1999, de 27 de septiembre, FJ 10, y citándolas STC 8/2000, de 17 de enero, FJ 4) [...]. «Nuestra jurisprudencia establece, por tanto, como regla general, que, a falta de consentimiento del titular, el acceso al domicilio inviolable se posibilita únicamente sobre la base de una resolución judicial debidamente motivada, en atención al principio de proporcionalidad, y cuyo objeto es preservar y proteger el derecho rodeándolo de una serie de garantías. La exigencia de la garantía judicial decae únicamente en caso de flagrante delito».

⁴ Sobre el carácter nulo y antijurídico de la acción administrativa sancionadora por el ejercicio de derechos fundamentales, en particular el de no contribuir a la propia inculpación (amparado por los artículos 24 CE y 6.º CEPDH) facilitando el acceso a documentos o informaciones —en términos que podrían, incluso, hacer cuestionables los requerimientos imperativos de información de la CNC previstos en la LDC, aunque ésta es cuestión compleja que dejamos sólo apuntada, para desarrollo en otra ocasión—, pueden traerse a colación las Sentencias del TEDH de 25 de febrero de 2003 (Funke c. Francia, parágrafos 41 y 44) y de 24 de julio de 2008 (André y otro c. Francia, parágrafo 41) y la del Tribunal Constitucional 45/1997, de 11 de marzo, y su precedente STC 197/1995 (FJ 7.º), amén de la del TJCE de 18 de octubre de 1989 (Orkem).

sucesivo, «LOPJ»). Desde la LO 6/1998, de 13 de julio, el artículo 91.2 de la LOPJ y el artículo 8 de la LJCA atribuyen la competencia de autorización al orden jurisdiccional contencioso-administrativo, al que con carácter general corresponde el control de juridicidad de la actuación administrativa (artículo 106.1 CE). Ello implica que la autorización incorpora un control efectivo sobre los requisitos de la intromisión para ser compatible con los derechos garantizados por los artículos 18 CE y 8 CEPDH.

La nueva LDC ampliaba en fase de proyecto, antes de su paso por el Senado, el ámbito de ese control a la incidencia o intromisión en otros posibles derechos fundamentales afectados por los actos de inspección de la CNC. En principio, y en teoría, todos los de la sección 1.ª del capítulo II del título I de la Constitución; pero, tal como la LDC ordena las facultades de inspección, los concernidos eran los derechos del artículo 18 CE, en su apartado 3 relativo al derecho al secreto de las comunicaciones, además del de inviolabilidad domiciliaria del apartado 2. Como hemos anticipado antes, la modificación de la disposición adicional séptima en el Senado no puede, sin embargo, eludir el mandato directo del artículo 18.3 CE.

Los supuestos de actos de inspección de la CNC legitimados para incidir sobre los derechos fundamentales están exhaustivamente tasados. No sólo por los términos, no meramente enunciativos, de la relación del artículo 40.2 de la LDC, sino como exigencia del requisito de previsión legal expresa de las intromisiones derivada del artículo 8.2 CEPDH y del artículo 53.1 CE⁵. No pueden realizarse —ni siquiera con autorización judicial— actos de inspección que afecten a los derechos del artículo 18 CE o del artículo 8 CEPDH distintos de los expresamente enumerados en el artículo 40.2 de la LDC, ni éstos podrán extenderse a objetos que, como la correspondencia entre la empresa y sus abogados, afecten a la esencia de otro derecho fundamental, como el de defensa (artículos 24.2 CE y 6.1 CEPDH), de modo que su interferencia, incluso con autorización judicial, venga a vaciar de contenido al referido derecho⁶.

⁵ Dejamos también sólo apuntada —por no abrir más el cúmulo de cuestiones constitucionales implicadas en este trabajo— la posible incidencia del artículo 81.1 CE en la suficiencia de esa legitimación, atendido el carácter de Ley ordinaria, y no orgánica, de la LDC.

⁶ *Vid.* una manifestación de la protección del secreto profesional de los abogados —corolario del derecho de su cliente a la

La Sentencia del TEDH de 24 de septiembre de 2009 (Georgi Yordanov c. Bulgaria) precisa que la intervención de las comunicaciones con el abogado vulnera en sí misma, por el conocimiento implícito en su mera presencia en las actuaciones, el derecho del artículo 8 CEPDH, aunque no llegue a ser utilizada como prueba. Esta doctrina parece no haberse tomado en consideración por la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, en su sentencia dictada sólo seis días más tarde en el RCA n.º 3/2008, en la que, con un criterio a nuestro juicio reduccionista del ámbito protegido, niega relevancia constitucional a aquella intervención y a la presencia de las comunicaciones intervenidas a disposición de la Administración, mientras no sean utilizadas como prueba.

El párrafo final del artículo 40.2, añadido en el Dictamen de la Comisión del Congreso, requiere «*el previo consentimiento expreso del afectado o, en su defecto, la correspondiente autorización judicial*» sólo para «*el ejercicio de las facultades descritas en las letras a) y e)*». El apartado 4 del mismo precepto, más correctamente, prevé que deba solicitarse la autorización judicial siempre que la inspección ordenada por el director de investigación, a la que se oponga o pueda oponerse el interesado, «*implique restricción de derechos fundamentales*».

No es dudoso que las facultades de acceso y de precinto de locales, o de libros, bienes y documentos de los párrafos a) y e) pueden restringir los derechos fundamentales del artículo 18 CE. Pero también otras facultades del artículo 40.2 de la LDC pueden hallarse en el mismo caso. No se acierta a comprender por qué requiere autorización el precinto de documentos del párrafo e) y no habrían de requerirla la verificación, la copia o la retención hasta durante 10 días de tales documentos, que pueden incluir correspondencia postal o de otro tipo (artículo 18.3 CE), a que se refieren los párrafos b), c) y d). Tales intromisiones en el secreto de las comunicaciones requieren también a nuestro juicio autorización judicial previa.

Por lo demás, lo razonable es que tal autorización se solicite para el conjunto de las facultades del artículo 40.2 de la LDC ejercitables con ocasión de una inspección domiciliaria, aunque su otorgamiento, en su caso, deberá estar especificado como

no autoincriminación— en la citada Sentencia André y otro c. Francia del TEDH, de 24 de julio de 2008.

tal para cada una de ellas en la resolución judicial.

No examinamos, ya que trascienden del objeto de este trabajo, las cuestiones que se plantean en relación con la posible incidencia de los actos de investigación a que se refieren los artículos 39.1 (solicitudes de información) y 40.2 f) (interrogatorio del personal) de la LDC en el ámbito de los derechos del artículo 24.2 CE relativos al procedimiento sancionador, como el de ser informado de la acusación o a no declarar contra sí mismo (*vid.* nota 5). Baste con dejar apuntado que la posible afectación de derechos fundamentales puede impregnar toda la actuación administrativa investigadora de los órganos de la CNC.

Por ello, no cabe dar por buena la limitación de los supuestos sujetos a autorización a unas determinadas modalidades de inspección. Requerirán autorización todas aquellas que impliquen intromisión en, al menos, los derechos garantizados por los artículos 18, 2 y 3 CE y 8 CEPDH.

Finalmente, para excluir la necesidad de autorización no bastará siempre con la no oposición de la empresa o grupo de empresas, como señala el artículo 40.4 de la LDC. El consentimiento relevante, que debe ser expreso —y, por supuesto, libre—, es, como señala el último párrafo del 40.2, el del afectado, es decir, el del titular del derecho fundamental objeto de restricción. Tal será el caso de los empresarios, administradores y otros miembros del personal de las empresas a cuyo domicilio particular se acuerde el acceso conforme a lo facultado por el artículo 40.2 a) de la LDC. Y también el de los empleados cuya correspondencia —incluida la electrónica— sea objeto de examen u ocupación, aunque a reserva, a nuestro juicio, de que en dicha correspondencia actúen en nombre de la empresa, orgánicamente integrados en ella, en cuyo caso el titular de la correspondencia podría entenderse que es aquélla.

La necesidad de distinguir entre la correspondencia electrónica profesional y la personal, que pueden coexistir en el programa de *e-mail* o en el disco duro de un mismo ordenador de la empresa, redundará, a nuestro entender, en la ilicitud de la práctica de copia y traslado para su examen ulterior por parte de los instructores de la Dirección de Investigación toda la correspondencia electrónica de un ordenador, sin abrirla en presencia de los interesados, como exige, en términos trasladables a la acordada y practicada por la Administración, la Ley de Enjuiciamiento Criminal para cualquier intervención de correspondencia.

1.3. Órgano competente

La autorización judicial previa de los actos de inspección que impliquen restricción de derechos fundamentales es competencia objetiva de los Juzgados de lo Contencioso-Administrativo, conforme al artículo 8.6 de la LJCA, no de los Juzgados Centrales de dicho orden, cuya competencia regula el artículo 9 de la LJCA.

Funcionalmente, y aunque la norma legal no lo expresa, conocen en primera instancia, atendido lo dispuesto en el artículo 80.1 de la LJCA. Del recurso de apelación corresponde conocer a la Sala del orden contencioso-administrativo del Tribunal Superior de Justicia de la Comunidad Autónoma de que se trate, conforme al artículo 10.2 de la LJCA.

La competencia territorial podría ofrecer alguna duda, ya que las reglas del artículo 14 de la LJCA están concebidas únicamente para la atribución del conocimiento de recursos contencioso-administrativos. Las reglas segunda y tercera del apartado 1 no comprenden los actos de intromisión domiciliaria o en las comunicaciones, y la regla a), de carácter general, no parece la más adecuada para su adaptación al control judicial previo que nos ocupa.

Parece más razonable una aplicación analógica de la regla tercera, que se refiere a actuaciones que comporten intervención administrativa en la propiedad privada. Serían competentes territorialmente, por tanto, los Juzgados en cuya circunscripción radiquen los domicilios o los instrumentos de comunicación concernidos por los actos objeto de autorización.

1.4. Trámites y alcance del control judicial

Ni la LJCA ni la LDC contienen una regulación procedimental propiamente dicha del trámite para la obtención, o la denegación, de la autorización judicial de los actos de inspección que la requieran. El artículo 40.4 de la LDC se limita a disponer que la autorización judicial debe ser solicitada por el director de investigación de la CNC y que el Juzgado de lo Contencioso-Administrativo resolverá en el plazo máximo de 48 horas. Tampoco existe una regulación normativa directa de los aspectos sustantivos que integrarían el denominado Derecho procesal material.

La brevedad del plazo parece presuponer que no existirá actividad de instrucción procesal ni contra-

dicción. La Ley no la establece —aunque tampoco la excluye—, y parece presuponer también —al referirse al riesgo de oposición— un efecto sorpresa incompatible con aquélla.

Si embargo, se trata de una función propiamente jurisdiccional. El juez de lo Contencioso-Administrativo lleva a cabo una declaración, siquiera sumaria —en el sentido de que se sustenta en una *cognitio* limitada y no produce efecto de cosa juzgada—, de carácter jurídico. Pronuncia la adecuación a Derecho de la intromisión acordada por el director de investigación en el ámbito de los derechos fundamentales.

Respecto de la autorización que en su día regulaba el artículo 87.2 de la LOPJ, el Tribunal Constitucional había considerado que el juez que autoriza la entrada domiciliaria no debía actuar con automatismo formal, pero tampoco debía —recordemos que era un juez de instrucción penal— entrar a conocer y revisar la legalidad intrínseca del acto que se ejecutaba. Actúa como garante del derecho fundamental concernido y verifica la apariencia de legalidad del acto y la necesidad y proporcionalidad de la medida para su ejecución (Sentencia 78/1992, de 19 de mayo).

Esta aproximación debe completarse una vez que la autorización se atribuye al orden contencioso-administrativo, competente para el control de legalidad de la actuación administrativa (ex artículo 106.1 CE), y que se refiere específicamente por la LDC a actos de trámite, como los de inspección, en los que aquel control se identifica propiamente con la garantía del derecho fundamental que se restringe. El juez debe, por tanto, valorar la efectiva previsión legal de la intromisión cuya autorización se solicita; su proporcionalidad o adecuación objetiva de su alcance con la investigación en que se incardina; y su necesidad, en suma, en una sociedad democrática para alcanzar el fin legítimo (la investigación de las infracciones) al que se dirige, como exige el artículo 8.2 CEPDH.

El juez debe, pues, denegar la autorización cuando no concurren todos esos requisitos, respecto de los que el director de investigación que solicita la autorización tiene la carga de acreditarlos. Eso supone que la solicitud de autorización, para prosperar, debería ser fundada y documentada, y expresar los hechos que se investigan, su carácter supuestamente infractor, la relación existente entre ellos y el objeto del acto de inspección restrictivo de derechos fundamentales y la necesidad consiguiente de éstos. No puede ser una mera petición formal o

ritual. En palabras de la Sentencia de la Sala de lo Contencioso-administrativo del Tribunal Superior de Justicia de Cataluña, de 11 de octubre de 2007, en la apelación 56/2007 (FJ 7.º):

«ha de haber indicios de la comisión del ilícito que se persigue y los ha de haber también de obtener mediante la entrada y registro el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa. Y, aun con tales indicios, faltará en todo caso el carácter necesario de la intervención cuando constituya «la primera medida de investigación pues el juicio de necesidad, esto es, el carácter imprescindible de la medida como parte esencial del juicio de proporcionalidad, requiere ponderar la eventual existencia de medios alternativos de investigación» (SSTC 184/2003 y 146/2006). Es más, según esta STC 145/2006, han de expresarse los indicios existentes de que se ha cometido un ilícito; no bastando la mera sospecha de que se ha cometido, ni que se pretenda satisfacer la necesidad genérica de prevenir o descubrir delitos o ilícitos o se quieran despejar las sospechas sin base objetiva que surjan en la mente de los encargados de la investigación, de manera que la decisión judicial debe exteriorizar las razones fácticas y jurídicas que justifiquen la concurrencia del presupuesto habilitante de la intervención, como lo son la imputación de un ilícito y los datos o hechos objetivos que puedan considerarse indicios en la posible existencia. Es indispensable la precisión de los indicios, como un prius lógico de los también obligados juicios sobre la adecuación, la necesidad y la proporcionalidad de la medida, requiriendo su apoyo en datos objetivos»⁷.

El Juzgado, que no tiene un procedimiento específico que tramitar, puede, sin embargo, tras examinar la documentación presentada, recabar su complemento, o explicaciones o justificaciones adicionales, y, en casos límite en que lo estime necesario, oír contradictoriamente al titular de los

⁷ Como señala el auto del Juzgado de lo Contencioso-Administrativo n.º 12 de los de Barcelona, de 31 de enero de 2008, desestimatorio de una autorización de entrada solicitada en nombre de la Dirección de Investigación de la CNC, «es preciso que la Administración motive de forma particular las razones que tiene para entender que la autorización sorpresiva es indispensable, motivación que no se aporta en el caso que nos ocupa, en el que bien entendido que con los pocos datos aportados se deduce que lo que hay que investigar es si hay un reparto material de mercados entre la afectada y otra empresa, circunstancia que probablemente se pretende comprobar a partir de las licitaciones a que concurren una y otra, y si esto es así no se aprecia riesgo de desaparición de tal documentación que en todo caso consta en las Administraciones licitadoras. En definitiva, no se ha aportado una motivación que justifique la no audiencia de la afectada».

derechos a restringir. Dado el carácter sumario del proceso y su objeto, la contradicción no es una regla exigible, pero tampoco puede entenderse que está necesariamente excluida. Puede tener sentido en algunos casos, como alternativa a la denegación directa de la autorización⁸.

No cabe ocultar, sin embargo, que el TEDH se ha pronunciado en contra de la compatibilidad de las inspecciones domiciliarias de la Administración con el derecho a la tutela judicial efectiva garantizado por el artículo 6 del Convenio, aun autorizadas por resolución judicial —y en un marco de las máximas garantías de control directo por el juez del desarrollo de la inspección, como es el establecido en Francia por el artículo L. 16B del *Livre des Procédures Fiscales*—, cuando en el procedimiento que conduce a dicha autorización «*la persona concernida por el registro proyectado —que ignora en esta fase la existencia de un procedimiento en su contra— no tenga la oportunidad de hacerse oír*»; ya que, a falta de dicha posibilidad de contradicción, «*no se puede considerar que la instancia en la que el juez examina la solicitud de autorización sea conforme con el artículo 6.1*». Así se expresa paladinamente en la Sentencia, de 21 de febrero de 2008, en el asunto *Ravon y otros c. Francia* (vid. parágrafos 28 y 30), cuya doctrina se reitera en la de 16 de octubre del mismo año (*Maschino c. Francia*)⁹.

⁸ En el ámbito de las autorizaciones de entrada para la ejecución forzosa de actos administrativos, las Salas de lo Contencioso-Administrativo de los Tribunales Superiores habían considerado que era preceptiva la audiencia del titular del domicilio con carácter previo a la decisión judicial de autorización, salvo que la demora pueda conllevar «*daño irreparable para el interés público*» (vid., entre otras, STSJ Madrid, de 27 de marzo de 2001. RCA 2001/732). La pérdida del efecto sorpresa de la inspección puede integrar, a nuestro juicio, el supuesto de daño irreparable al interés público.

⁹ No es de recibo, a nuestro juicio, la tesis apuntada por la CNC en alguna resolución, según la cual la trascendencia y peculiaridad de la defensa de la competencia que tiene encomendada determinarían una menor exigencia de garantías en sus intromisiones en los derechos garantizados por los artículos 18, 2 y 3 CE y 8 del CEPDH, que en los de la inspección tributaria. En materia de injerencia en los derechos fundamentales no caben distinciones no expresamente establecidos por la Ley (artículo 53.1 CE). Y tampoco cabe compartir, en términos de razonabilidad, la razón dada para ello en algún caso por la CNC —en materia fiscal, supuestamente, no habría nada que ocultar, como sí ocurriría, como supuesta peculiaridad, en materia de competencia—, que parte del olvido de que lo que se busca en las inspecciones tributarias no son los documentos que acreditan la declaración o el pago de las deudas tributarias, sino los que reflejen la existencia de hechos imposables, o de la magnitud de sus bases, ocultados a la Hacienda Pública, exactamente en los mismos términos que se predicán de los documentos indiciarios de comportamientos infractores en materia de competencia.

En relación con lo anterior, el plazo de 48 horas del artículo 40.4 de la LDC no tiene carácter preclusivo, ni, por supuesto, su transcurso sin que haya recaído resolución judicial implica autorización tácita o por silencio, inexistente en el ámbito de la Jurisdicción. Si es necesaria una instrucción complementaria de la solicitud, por deficiencia en la motivación de la inicialmente presentada, o si fuera preciso dar audiencia al titular del domicilio o de las comunicaciones concernidos, será normal un lapso temporal mayor. La alternativa, si se insistiera en la preclusión, sería, simplemente, la caducidad del trámite y la inexistencia, ya que no la denegación, de la autorización.

La resolución del juez deberá ser motivada, normalmente en forma de auto, por referencia a las circunstancias específicas del caso y no en términos rutinarios o estereotipados, que podrían conllevar la nulidad de la autorización y de la propia inspección.

La resolución del juez no tiene que ser, necesariamente, una mera denegación o una autorización pura y simple del acto de inspección. Puede también imponer determinados requisitos para que su práctica no resulte desproporcionada, como la limitación del ámbito de la documentación o correspondencia a examinar o copiar. Por ejemplo, pero no exclusivamente, para excluir el examen o copia de la correspondencia del empresario con sus abogados ordenada al ejercicio del derecho de defensa.

No estimamos que quepa un trámite de oposición del interesado, no oído previamente, a la autorización otorgada y, en su caso, ejecutada. La decisión judicial es, en ese sentido, definitiva, y su impugnación debería seguir el cauce de los recursos procesales. Sin embargo, como hemos apuntado, el pronunciamiento judicial de autorización —del juez o de la Sala de apelación— no produce a nuestro juicio —por su sumariedad y ausencia de contradicción— efecto de cosa juzgada y, por consiguiente, la nulidad del acto de inspección autorizado, y, por extensión, la de la resolución que recaiga en el procedimiento sancionador basada en aquél podrá ser planteada en el procedimiento administrativo y en el ulterior recurso contencioso-administrativo contra la resolución que le ponga fin. En éste podrá cuestionarse el acierto de la decisión autorizadora y los presupuestos ofrecidos por el director de investigación para solicitarla. En suma, la revisión de la validez del acto de inspección en cuestión, desde la perspectiva de los dere-

chos fundamentales restringidos, formará parte del control de legalidad de la resolución que ponga fin al procedimiento, ejercida por el Tribunal contencioso-administrativo que conozca de su impugnación.

En segunda instancia, serán de aplicación las normas de procedimiento de la sección 2.^a del capítulo III del título IV de la LJCA. Y, en lo sustantivo, vale, en los mismos términos que para la primera instancia, lo anteriormente expuesto sobre el alcance del control previo que se ejercita. Ahora bien, con la peculiaridad de que, concedida, en su caso, la autorización en primera instancia y ejecutada la inspección domiciliaria —desde cuya ejecución, en la que se habrá notificado el auto de autorización, correría el plazo de recurso para el titular—, el objeto del proceso de apelación será el control de la validez (o nulidad) de la propia autorización y, por consiguiente, de la inspección autorizada.

1.5. El control ex post en vía de recurso

Nos referimos, finalmente, en este punto, no al cuestionamiento de la validez de la inspección domiciliaria que pueda llevarse a cabo con ocasión del recurso contencioso-administrativo interpuesto contra la Resolución definitiva de la CNC que ponga fin al expediente en que aquélla se haya practicado, al que ya hemos hecho referencia, sino a la impugnación autónoma de las vías de hecho en que pueda incurrir la actuación inspectora.

«También es admisible el recurso contra la inactividad de la Administración y contra sus actuaciones materiales que constituyan vía de hecho», en los términos establecidos en la Ley (artículo 25.2 de la LJCA).

En materia de aplicación de la LDC, las vías de hecho son concebibles, especialmente, en el ámbito de las actividades inspectoras o de investigación, cuando se adopten medidas sobre la esfera jurídica de los interesados (por ejemplo, la ocupación de la correspondencia o la intervención de las comunicaciones mantenidas con los abogados en ejercicio del derecho de defensa) sin un acto que las acuerde o sin la autorización judicial cuando, en defecto de consentimiento del interesado, ésta sea preceptiva o incluso cuando la actuación inspectora trascienda de lo estrictamente autorizado. Este último caso —extralimitación de la actuación inspectora respecto al ámbito material del mandato del director de investigación o de la autorización judicial— es el

apreciado en la Sentencia de 30 de septiembre de 2009, de la Sección Sexta de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, en el RCA n.º 3/2008.

En caso de producirse cualquiera de las mencionadas vías de hecho, el interesado podrá formular requerimiento a la Dirección de Investigación, como Administración actuante, intimando su cesación. Si dicha intimación, que no resulta así un presupuesto procesal necesario, no hubiere sido formulada o no fuere atendida dentro de los diez días siguientes a la presentación del requerimiento, podrá deducir directamente recurso contencioso-administrativo (artículo 30 de la LJCA). En este recurso, el demandante podrá pretender que se declare contraria a Derecho la actuación material de que se trate, que se ordene el cese de la actuación y que se adopten, en su caso, las demás medidas adecuadas para el pleno restablecimiento de la situación jurídica conculcada, entre ellas la nulidad de las actuaciones basadas en el resultado de la vía de hecho y la indemnización de los daños y perjuicios cuando proceda (artículos 32.2 y 31.2 de la LJCA).

El recurso contencioso-administrativo podrá ser, bien el ordinario, bien el procedimiento de amparo judicial de las libertades y derechos, previsto en el artículo 53.2 CE y regulado en el orden contencioso administrativo en los artículos 114 al 22 (capítulo I del título V) de la LJCA. La Sentencia de la AN de 30 de septiembre de 2009, antes mencionada, incurre a este respecto, a nuestro juicio, en una errónea confusión entre el aspecto sustantivo de la existencia o no de vulneración de derechos fundamentales y el cauce instrumental de la actuación administrativa en que aquélla se produce, al calificar la existencia de vía de hecho como cuestión de legalidad ordinaria (FJ 1.º, *in fine*).

La vía de hecho, si incide, limitándolo fuera del ámbito del título habilitante para ello (el mandato administrativo consentido o la autorización judicial, en el caso del derecho del artículo 18.2 CE, cuya extralimitación parece inherente a la vía de hecho en este caso), en el goce de un derecho fundamental, podrá dar lugar a una vulneración de éste y ser controlada en el procedimiento del capítulo I del título V de la LJCA.

En el recurso, o previamente, podrá pedirse como medida cautelar inmediata *inaudita parte*, ex artículo 135 de la LJCA, la suspensión de la práctica de la inspección. Y en estos casos de vía de hecho la regla es, de conformidad con el artículo 136 de la misma Ley, la adopción de la medida cautelar.

2. EL ACCESO A LOS ORDENADORES

Una cuestión de especial trascendencia práctica durante las inspecciones domiciliarias realizadas por las autoridades de competencia consiste en el acceso a los ordenadores de directivos y empleados y, en particular, a sus cuentas de correo electrónico. La rapidez con que el *e-mail* permite enviar, recibir y almacenar documentación, así como la facilidad para buscar correos por palabras clave o fechas de envío o recepción, explican que las autoridades siempre procedan a su revisión y, con frecuencia, a copiar archivos informáticos en él contenidos.

Ciertamente, los ordenadores y sistemas de *e-mail* están, como regla general, sometidos a los poderes de inspección de las autoridades en la medida en que se hallen en las dependencias de la empresa investigada y se haya permitido (de forma voluntaria o con autorización judicial) la entrada y acceso a dichas dependencias. Esto es, al igual que no existen diferencias relevantes durante una inspección entre los diferentes «formatos» (físico o digital) de un documento, tampoco las hay entre los soportes o sistemas de almacenamiento de tales documentos (armarios, cajones, carpetas físicas, ordenadores o servidores). A primera vista, por tanto, no cabría diferenciar a los presentes efectos entre un archivador físico de papeles y un ordenador personal.

Sin embargo, los ordenadores presentan algunas características propias que los diferencian del resto de objetos ubicados en las dependencias empresariales y que les sitúan en una posición especial durante una inspección:

- El ordenador es la puerta de acceso a los sistemas de correo electrónico, que constituyen una modalidad de telecomunicaciones (comparable al correo postal ordinario y a las conversaciones telefónicas), cuyo secreto e inviolabilidad goza de protección constitucional y penal frente a la autoridad administrativa.
- Con frecuencia, los empleados y directivos de una empresa almacenan en los ordenadores que utilizan información de naturaleza privada o personal (incluyendo no sólo correos electrónicos, sino archivos gráficos o audiovisuales) que quedaría al descubierto ante los inspectores.
- Al tratarse de archivos informáticos o digitales, la información contenida en un ordenador puede ser copiada por la autoridad de forma masiva y rápida. Esto es, la facilidad de búsqueda y copia de los archivos digitales fomenta su aprehensión «en bloque» por parte de la autoridad (y su almacenamiento en unidades lógicas para su posterior examen), lo que disuade del análisis individualizado de cada documento a efectos de determinar si es o no relevante para el objeto de la inspección.

Procede por tanto examinar de forma separada los principales problemas jurídicos que plantea el acceso a los ordenadores y correos electrónicos durante las inspecciones de competencia. Sin duda, los más relevantes son los relativos al secreto de las comunicaciones, cuya inviolabilidad garantiza la Constitución Española, y al delito de descubrimiento y revelación de secretos por funcionario público, tipificado en el artículo 198 del Código Penal.

2.1. El secreto de las comunicaciones

El artículo 18.3 CE dispone:

«Se garantiza el secreto de las comunicaciones, y en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

La jurisprudencia del Tribunal Constitucional permite incluir con seguridad al correo electrónico en la protección del artículo 18.3. En efecto, la Sentencia de 3 de abril de 2002¹⁰ admite expresamente la extensión del derecho fundamental del secreto de las comunicaciones a los «nuevos ámbitos» relacionados con los «avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática», en inequívoca referencia al correo electrónico. Nótese en este sentido que el artículo 18.3 CE emplea los términos «en especial» al referirse a «las comunicaciones postales, telegráficas y telefónicas», lo que evidencia el carácter meramente ejemplificativo (y no exhaustivo) de los canales de comunicación mencionados por la norma. Por otra parte, la inclusión del correo electrónico en la garantía del secreto de las comunicaciones queda además confirmada por la legislación

¹⁰ STC núm. 70/2002, de 3 de abril.

comunitaria¹¹ y española¹² y asumida por la doctrina especializada¹³.

Una vez sentada la inclusión general del *e-mail* en el artículo 18.3 CE, se suscita la cuestión del ámbito objetivo de la protección constitucional o, en otros términos, determinar qué correos electrónicos (si todos o solamente algunos) están amparados por el secreto de las comunicaciones. En particular, conviene examinar la situación jurídica de los *e-mail* de contenido «profesional» o empresarial (i.e., los que no revelan aspectos privados o personales de los interlocutores), los ya recibidos pero aún no abiertos por su destinatario, los ya abiertos por el destinatario y archivados en el ordenador (p.ej., en el programa de correo electrónico o en el disco duro) y los impresos en papel y archivados en carpetas, cajones, etc.

En este punto, resulta útil recordar los contornos básicos del artículo 18.3 CE tal y como los ha definido el propio Tribunal Constitucional en sus principales sentencias en la materia¹⁴:

- El secreto de las comunicaciones no sólo protege la libertad del proceso de la comunicación, sino también el contenido de la

comunicación y otros aspectos, como la identidad de los interlocutores. El artículo 18.3 prohíbe, por tanto, la interceptación en sentido estricto (i.e., la aprehensión física del soporte del mensaje —con conocimiento o no de dicho mensaje— o la captación del proceso de comunicación), pero también «el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo). Por ello, no resulta aceptable lo sostenido por el Abogado del Estado en sus alegaciones en el sentido de que el artículo 18.3 de la Constitución protege sólo el proceso de comunicación y no el mensaje, en caso de que éste se materialice en algún objeto físico» (STC 114/1984, FD 7.º). El objeto de la protección constitucional no es sólo el proceso de comunicación (p.ej., la llamada telefónica mientras se produce, el traslado de la correspondencia desde el remitente hasta el destinatario, el envío telemático de correos electrónicos, etc.), sino el propio mensaje comunicado.

- La protección al mensaje se extiende a cualquier tipo de «comunicación» entre personas (conversaciones, informaciones, datos, imágenes, etc.) y al soporte físico en que la comunicación se materializa (carta, telegrama, mensaje de correo electrónico, CD, DVD, cinta de vídeo, etc.). Sin embargo, es necesario que el mensaje y su soporte físico se envíen a través de conductos o continentes (sobre cerrado, paquete postal, etc.) utilizados habitualmente para transportar correspondencia y no para el tráfico de mercancías (STC 281/2006, FD 3.º).
- El derecho tiene carácter formal, «en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado» (STC 114/1984, FD 7.º). El secreto de las comunicaciones tiene un carácter autónomo frente a la protección de la intimidad personal y familiar: ampara a cualquier tipo de comunicación, personal o profesional.
- El artículo 18.3 CE garantiza la impenetrabilidad de las comunicaciones frente a cualquier tercero (público o privado) a la comunicación. Se trata por tanto de un derecho con eficacia *erga omnes*, tanto Administración pública como empresarios. Por el con-

¹¹ Vid. artículo 5 de la Directiva 2002/5/CE, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas): «Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público».

¹² Vid. artículo 33 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones: «Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias».

¹³ Vid., por ejemplo, P. L. Murillo de la Cueva, «Notas sobre el derecho fundamental al secreto de las comunicaciones», en *Constitución, estado de las autonomías y justicia constitucional (Libro homenaje al profesor Gumersindo Trujillo)*, Valencia, 2005, págs. 661 y ss. I. Marín Alonso, *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Valencia, 2004, págs. 126 y ss. J.J. Fernández Rodríguez, *Secreto e intervención de las comunicaciones en Internet*, Madrid, 2004, p. 95. A. Elvira Perales, *Derecho al secreto de las comunicaciones*, Madrid, 2007. A. Ortega Jiménez y J.A. González Martínez, «Protección de datos, secreto de las comunicaciones, utilización del correo electrónico por los trabajadores y control empresarial», *Diario La Ley*, número 7188, de 3 de junio de 2009.

¹⁴ Vid. SSTC 114/84, de 29 de noviembre, 70/2002, de 3 de abril, 137/2002, de 3 de junio, y 281/2006, de 9 de octubre.

trario, los interlocutores de la comunicación (remitente y destinatario(s) del *e-mail*) no soportan ninguna obligación bajo el artículo 18.3 CE, por lo que pueden comunicar o reenviar el mensaje a terceros (e incluso hacerlo público) sin vulnerar el secreto de las comunicaciones¹⁵.

- Sólo gozan de la protección del artículo 18.3 CE las comunicaciones consideradas secretas o reservadas por quienes las realizan. Por ello, las comunicaciones realizadas a través de canales abiertos de comunicación (conversaciones presenciales, tarjeta postal sin sobre, paquetes postales transparentes o con interior visible, etc.) excluyen el secreto y, por tanto, la protección del precepto¹⁶.
- Como corolario de lo anterior, la revelación voluntaria a la autoridad administrativa del contenido de la comunicación por el titular del derecho hace innecesaria la autorización judicial.

Se pueden extraer ya algunas consecuencias claras en relación con la protección que proporciona el artículo 18.3 CE a los correos electrónicos accesibles desde ordenadores o servidores inspeccionados por las autoridades de competencia. La primera es que los *e-mail* que prueben una infracción por la empresa de las normas de defensa de la competencia (los que precisamente busca la autoridad inspectora) están amparados por el artículo 18.3 CE en la misma medida que los correos de índole personal o íntima del remitente o del destinatario¹⁷. La

segunda es que la inviolabilidad de las comunicaciones de los empleados y directivos se alza no sólo frente a los funcionarios que realizan la inspección, sino también frente a la propia empresa obligada a tolerarla y a colaborar con la autoridad inspectora. Ello supone que la autoridad inspectora no podría lícitamente requerir a la empresa para que le entregara los correos de sus empleados (en lugar de obtenerlos ella misma en los ordenadores o servidores correspondientes), pues la empresa también está obligada por el artículo 18.3 CE.

De especial interés para el asunto que nos ocupa es determinar el *alcance temporal* de la protección y, en concreto, si el artículo 18.3 CE continúa desplegando sus efectos una vez que el correo electrónico ha sido efectivamente recibido por su destinatario o abierto por él¹⁸. No hay duda de que el precepto sigue siendo de aplicación mientras que el destinatario aún no haya abierto o leído el *e-mail*, con independencia de que la entrega del correo electrónico a su destinatario (la aparición del mensaje en la bandeja de entrada de la cuenta de correo) ya se haya consumado. Recuérdese que la inviolabilidad se proyecta no sólo al proceso de comunicación *stricto sensu* (el proceso telemático de envío y recepción del correo), sino también al propio contenido u objeto de la comunicación (el mensaje de *e-mail* propiamente dicho). El Tribunal Constitucional ha señalado expresamente que la «apertura de la correspondencia ajena guardada por su destinatario» vulnera el artículo 18.3 CE (STC 114/1984), lo que necesariamente presupone que el mensaje ha sido ya recibido¹⁹. Por consiguiente, los correos electrónicos aún no leídos o abiertos por su destinatario (normalmente identificados por el programa de *e-mail* en negrita o con un color de letra diferenciado) están directamente protegidos por el artículo 18.3 CE, de manera que ni los inspectores de competencia ni la propia empresa

¹⁵ En su caso, podría tratarse de una conducta contraria al artículo 18.1 CE, que protege la intimidad.

¹⁶ *Vid.* STC 281/2006. La doctrina admite unánimemente que los correos electrónicos no circulan por canales abiertos, sino cerrados (de forma similar a una conversación telefónica), por lo que están amparados por el secreto de las comunicaciones.

¹⁷ Nótese no obstante que, en caso de correos electrónicos de naturaleza «profesional» o empresarial, el titular del derecho al secreto de las comunicaciones garantizado constitucionalmente será por lo general la propia empresa y no el empleado o directivo que envía o recibe el correo, al presumirse que en este tipo de comunicaciones los empleados o directivos actúan en nombre de la empresa y no por cuenta propia. Como señala la doctrina, no hay inconveniente alguno en reconocer la titularidad del derecho al secreto de las comunicaciones también a las personas jurídicas (*vid.*, por ejemplo, P. L. Murillo de la Cueva, «Notas sobre el derecho fundamental al secreto de las comunicaciones», cit.). La única diferencia sería, pues, formal: quien debería invocar el artículo 18.3 CE ante los funcionarios de la autoridad de competencia para proteger el secreto de los correos electrónicos «profesionales» no sería el usuario del

ordenador o de la cuenta de correo, sino un representante de la empresa investigada.

¹⁸ En efecto, las inspecciones de las autoridades de competencia no se basan en la «intercepción» de correos electrónicos durante el proceso de su envío y recepción, sino en el simple acceso (mediante la entrada en las cuentas de *e-mail* accesibles a través de ordenadores personales y servidores) a los correos ya recibidos o enviados.

¹⁹ En realidad, el proceso de «comunicación» amparado por el artículo 18.3 no termina hasta que el destinatario del correo procede a su apertura y lectura, pues hasta ese momento no ha podido conocer lo que desea comunicarle el remitente. Por lo demás, es delicado identificar apertura y lectura, que no siempre tienen que ser simultáneas.

podrán acceder a ellos, salvo que cuenten con autorización judicial.

Más dudosa resulta para algunas opiniones la respuesta cuando el destinatario ya ha abierto o leído el correo electrónico. Por un lado, es indudable la concepción finalista del derecho fundamental alumbrada por el Tribunal Constitucional en su Sentencia 114/1984 (citada invariablemente en la doctrina constitucional posterior), que extiende la protección no sólo a la «comunicación», sino también al «mensaje», y condena como vulneración del secreto «la apertura de la correspondencia guardada por su destinatario»²⁰ porque el artículo 18.3 CE prohíbe el «conocimiento antijurídico de lo comunicado». Pero por otro lado, algunas sentencias posteriores han señalado que la protección del artículo 18.3 CE no puede exceder de la duración del propio proceso de comunicación, resultando así el precepto inaplicable a los supuestos en que se accede al mensaje antes de iniciarse la comunicación²¹ o tras su finalización («La protección del secreto de las comunicaciones alcanza el 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», STC 70/2002, FJ 9)²². Algunos pronunciamientos judiciales sostienen directamente que las cartas guardadas fuera del sobre (o incluso guardadas dentro de un sobre ya abierto) carecen de la protección del artículo 18.3 CE²³.

20 Haciendo recaer por tanto la vulneración del derecho fundamental no en conocer una comunicación antes de que lo haga su destinatario, sino en la «apertura» de la correspondencia recibida y guardada (sin excluir que esa correspondencia ya hubiera sido abierta y leída por el destinatario).

21 [La protección comienza] «una vez iniciado el proceso de comunicación» (STC 281/2006, de 9 de octubre FJ 3); «no se produjo ninguna interferencia en el proceso de comunicación (el paquete postal se interceptó y abrió antes de depositarse en las oficinas postales para su remisión al destinatario)» (STC 137/2002, de 3 de junio, FJ 3).

22 «La vulneración de este derecho requiere dicha interferencia en el proceso de comunicación»; «el derecho fundamental protege el secreto de las comunicaciones frente a cualquier clase de interceptación en el proceso de comunicación» (STC 281/2006, FJ 3).

23 Vid., por su claridad, AAP Girona de 5 de julio de 1999. Nótese, no obstante, que la denegación de la protección del artículo 18.3 CE a las cartas guardadas en «sobre abierto» podía deberse tanto a que el proceso de comunicación ya había expirado (al haber sido leída la carta por el destinatario) como simplemente a que la apertura del sobre por parte del destinatario revela una voluntad implícita de que el mensaje deje de ser secreto (de forma similar a las comunicaciones por canales abiertos, vid. *supra*).

La aplicación al correo electrónico de la doctrina según la cual el amparo del artículo 18.3 CE expira con la propia comunicación llevaría necesariamente a concluir que los *e-mail* ya leídos por su destinatario se encuentran extramuros del precepto, con independencia de dónde se almacenen. Sin embargo, el criterio de la apertura por el destinatario del sobre de la correspondencia guardada permite distinguir entre las copias impresas de los correos recibidos o enviados y los *e-mail* no impresos ya leídos por su destinatario y guardados en el ordenador personal (bien en la aplicación de correo electrónico, bien en carpetas del disco duro). En el primer caso, las copias impresas son asimilables a una carta tradicional fuera de su sobre (o guardada dentro de un sobre abierto), puesto que en ambos casos se infiere la voluntad de su remitente o destinatario de remover la barrera física que preservaba el mensaje del conocimiento ajeno y, por tanto, de renunciar a su carácter secreto o reservado²⁴. Pero en el segundo (*e-mail* archivados en el ordenador) cabe observar que —a diferencia del correo tradicional— el correo electrónico no se guarda en un sobre físico que lo oculte de los demás, sino que se envía y recibe de ordenador a ordenador. Los equipos informáticos —y las cuentas de correo cuyo acceso permiten— hacen así las veces del sobre en el correo tradicional, esto es, son los elementos físicos que preservan la opacidad de los mensajes respecto a cualquier tercero distinto de los usuarios de los ordenadores remitente o receptor²⁵. Al ser el ordenador personal el «sobre» del correo electrónico, el archivo del mensaje en el propio ordenador (sin impresión ni almacenamiento «en papel») no puede equivaler a la apertura del sobre postal: antes al contrario, revela justamente la voluntad del destinatario de mantener el mensaje dentro del continente en que lo recibió y de no renunciar a su carácter reservado *erga omnes*, como suele evidenciar la necesidad de utilizar una contraseña personal secreta para acceder a la información contenida en el ordenador.

Pero, además y en cualquier caso, la protección del proceso de comunicación no excluye la de su resultado, sino que, como la naturaleza de las cosas

24 Salvo que la copia impresa del mensaje haya sido archivada por el destinatario de forma específicamente dirigida a impedir su conocimiento por cualquier otro tercero, por ejemplo en el interior de un cajón del escritorio.

25 Nótese que algún autor ha sostenido recientemente que los correos electrónicos abiertos y almacenados no están protegidos por el artículo 18.3 CE. Vid. J.J. Fernández Rodríguez, *Secreto e intervención de las comunicaciones en Internet*, p. 95.

implica, está al servicio de ésta. Como recuerda la STC 281/2006, «a través de la protección del proceso de comunicación se garantiza a su vez el carácter reservado de lo comunicado sin levantar su secreto, de forma que es objeto de este derecho la confidencialidad tanto del proceso de comunicación mismo como del contenido de lo comunicado» (FJ 3).

Esta conclusión se ve apoyada a nuestro juicio por la doctrina constitucional. El secreto de las comunicaciones engloba no sólo el propio proceso de comunicación y el mensaje comunicado, sino también ciertos datos externos de la comunicación, tales como la identidad subjetiva de los interlocutores²⁶ y el momento, duración o destino de las llamadas telefónicas²⁷, lo que incluye en particular el listado de llamadas telefónicas realizadas²⁸. A este respecto, el Tribunal Constitucional ha confirmado que la protección del artículo 18.3 CE opera «con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso [el de comunicación]», pues los citados datos se refieren a un momento en el que el proceso de comunicación aún estaba teniendo lugar²⁹. La aplicación de este principio a las comunicaciones vía correo electrónico revela que las bandejas de entrada y salida de la aplicación de *e-mail* muestran algunos de esos elementos (identidad de los interlocutores y momento en que se produjo la comunicación), de forma similar a un listado de llamadas ya realizadas.

En suma, y en nuestra opinión, las autoridades de defensa de la competencia necesitan inexcusablemente autorización judicial para abrir, leer y copiar correos electrónicos (con cualquier contenido) que figuren como «no leídos» en la bandeja de entrada de las cuentas de *e-mail* a las que accedan. En cuanto a los correos identificados como «leídos» o «abiertos» por el programa de correo electrónico, y que se hallen guardados en el ordenador del remitente o destinatario, creemos que una obligada lectura garantista del precepto constitucional exige igualmente autorización judicial para abrirlos, leerlos o copiarlos, en la medida en que las aplicaciones de correo electrónico empleadas para su apertura y archivo muestran el resultado de la comunicación y datos externos de ésta, expresamente incluidos en el ámbito protector del artículo

18.3 por la doctrina constitucional. Por el contrario, el artículo 18.3 CE no será de aplicación a las copias impresas de los correos electrónicos (excepto aquéllas archivadas por el destinatario del mensaje específicamente para ocultarlas a la vista de terceros), por lo que no será necesaria la autorización judicial para su lectura y copia.

La muy reciente y ya citada sentencia de la Audiencia Nacional de 30 de septiembre de 2009 (que examina la inspección de la CNC en la sede de una asociación empresarial) no ha analizado en detalle el artículo 18.3 CE en materia de incautación de correos electrónicos por las autoridades de defensa de la competencia. La Sala no considera vulnerado el derecho fundamental en la medida en que «la Administración actuante no dirigió su actuación a la aprehensión de los documentos privados de los empleados ni de sus correos, lo que ocurrió es que, al copiar el contenido de los discos duros de los ordenadores, también copió documentos personales de los empleados» (FJ 4.º), lo que parece considerar a contrario que si la autoridad hubiese examinado y copiado directamente desde Outlook u otra aplicación de *e-mail* entonces sí habría podido existir una infracción del secreto de las comunicaciones (pues, en tal caso, la actuación habría ido directamente dirigida a apoderarse de correos electrónicos)³⁰.

Queda finalmente referirse a las características de la autorización judicial exigida expresamente por el artículo 18.3 CE para acceder a los correos electrónicos amparados por el secreto de las comunicaciones. Una pacífica jurisprudencia del Tribunal Constitucional³¹ requiere una estricta aplicación del principio de proporcionalidad, tanto desde el punto de vista material (la autorización judicial sólo es admisible en caso de que los hechos investigados sean suficientemente graves, pues de otra manera no podría justificarse una restricción de un derecho fundamental)³² como desde el punto de vista formal o procedimental (la autorización judicial no

²⁶ STC 114/1984.

²⁷ STC 123/2002, de 20 de mayo.

²⁸ STC 123/2002.

²⁹ FJ 6.º.

³⁰ No puede considerarse relevante la reiterada mención de la sentencia al carácter «personal» o «privado» de los correos: como señala la jurisprudencia constitucional, el artículo 18.3 CE comprende tanto los mensajes privados como los profesionales.

³¹ Vid. STC 104/2006, de 3 de abril de 2006.

³² Es altamente discutible que una conducta sin trascendencia penal (p.ej., vulneración de las normas de defensa de la competencia) pueda revestir una gravedad suficiente como para justificar la intervención judicial en un derecho fundamental. Vid., en general, STC 104/2006, que implícitamente asume que la intervención de las comunicaciones sólo procede en caso de investigación de hechos delictivos.

puede ser genérica, sino que ha de contener «los datos relativos al marco espacial —líneas telefónicas delimitadas—, temporal —plazos—, objetivo —hechos delictivos investigados— y subjetivo —personas conectadas con los hechos delictivos [...]»³³. Las autorizaciones que suelen expedir los Juzgados de lo Contencioso-Administrativo a solicitud de las autoridades de defensa de la competencia no cubrirían, en nuestra opinión, muchas de las inspecciones de correos electrónicos realizadas en el marco de las investigaciones domiciliarias.

3. DESCUBRIMIENTO DE SECRETOS

El artículo 197 del Código Penal dispone lo siguiente:

«1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales [...], será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».

El artículo 198 CP contempla un tipo agravado del delito anterior en caso de que lo cometa un funcionario público:

El objeto tutelado por el artículo 197 CP (y por tanto, también el 198 que se remite a él) es la intimidad personal: así lo ha aclarado el Tribunal Supremo respecto al artículo 197.1³⁴ y lo señala la propia norma en el caso del artículo 197.2 («datos reservados de carácter personal o familiar»). Ello permite excluir de la protección penal los datos e informaciones de índole profesional o empresarial (p.ej., los e-mail buscados por los inspectores de competencia). Sin embargo, esto no significa que

no pueda cometerse una vulneración del artículo 198 CP si, durante la búsqueda de los e-mail empresariales incriminatorios, los funcionarios tienen acceso o se apoderan de datos personales o privados de los empleados o directivos de la empresa inspeccionada. Este hecho se producirá con mayor probabilidad si los funcionarios realizan un copiado masivo de archivos (por ejemplo, mediante la utilización de palabras o criterios de búsqueda eminentemente genéricos) sin una revisión o lectura de los documentos preseleccionados antes de su copia³⁵.

Entrando ya en el examen del tipo penal, puede excluirse con seguridad la aplicación del artículo 197.1, que requiere un elemento intencional específico («para descubrir los secretos o vulnerar la intimidad de otro») que no concurrirá como es lógico en las inspecciones de competencia. Sin embargo, el artículo 197.2 CP no exige dicho elemento intencional específico. El Tribunal Supremo ha sostenido³⁶ que la expresión «en perjuicio de tercero» que integra el tipo penal no requiere una intencionalidad específica de perjudicar al titular de los datos, de forma que el dolo «no tiene que ser el único ni el prioritario móvil de la acción»³⁷. Por ello, el elemento intencional implícito en los términos «en perjuicio de tercero» se vería satisfecho si el sujeto activo penetra en los archivos o sistemas informáticos sin adoptar todas las cautelas y medidas necesarias y razonables para no acceder ni apoderarse de los datos privados protegidos por el tipo penal. Así, el mero acceso a un listado de correos electrónicos (y, en concreto, la apertura de la aplicación de correo electrónico Outlook) ha sido considerado suscep-

³⁵ La conducta típica se produce tan pronto como el funcionario «accede» a los datos personales («esto es, tan pronto lo conoce y tiene a su disposición», STS 234/1999) o se «apodera» de ellos (p.ej., la copia en dispositivos lógicos). Además, basta con acceder a los datos almacenados en archivos o sistemas informáticos, sin necesidad de acceder también a esos sistemas o archivos (SAP de Barcelona de 10 de marzo de 2006).

³⁶ STS 234/1999, de 18 de febrero, y STS 1461/2001, de 11 de julio.

³⁷ En terminología penal, «estamos pues ante un delito doloso pero no ante un delito de tendencia» (STS 234/1999, FJ 2.º). En la STS 725/2004, de 11 de junio, el Tribunal Supremo aclaró que el dolo requerido consistía en el simple conocimiento de los elementos del tipo objetivo (vid. FJ 11.º). Por su parte, los tribunales penales han precisado el alcance del dolo requerido por el tipo: dolo eventual (SAP Huelva de 16 de junio de 2006), «que al sujeto se represente la posibilidad de que cualquier persona pudiera resultar afectada por la utilización de los datos, sin exigir un ánimo específico de perjudicar a tercero» (SAP Palma de Mallorca de 11 de febrero de 2009) o el dolo indirecto o de segundo grado (SAP Vizcaya de 28 de mayo de 2007).

³³ STC 104/2006, FJ 2.º.

³⁴ STS 666/2006, de 19 de junio, y STS 358/2007, de 30 de abril.

tible de vulnerar el artículo 197.2 CP incluso sin necesidad de abrir ningún mensaje de tipo personal, con tal de que la cuenta de correo efectivamente almacenara algún *e-mail* de tipo privado o personal³⁸.

En este punto debe destacarse que, en una reciente sentencia de 3 de febrero de 2009³⁹, el Tribunal Supremo ha rebajado aún más la necesidad de la concurrencia del dolo, al recordar que la condición «*en perjuicio de tercero*» sólo se exige para algunas de las conductas prohibidas por el artículo 197.2 CP (el apoderamiento, utilización, alteración o modificación de los datos), pero *no para el mero acceso a ellos*.

En cuanto a los concretos datos personales protegidos por el artículo 197.2 CP, el Tribunal Supremo ha sostenido que serán los pertenecientes «*al reducto de los que, normalmente, se pretende no trasciendan fuera de la esfera en que se desenvuelve la privacidad de la persona y de su núcleo familiar*»⁴⁰ o, en términos más sintéticos, todos los datos automatizados no públicos⁴¹. La jurisprudencia contempla un amplio muestrario de datos tutelados: incidencias de la vida laboral de los trabajadores, historiales clínicos, saldo de cuentas bancarias, listados de llamadas telefónicas, número de teléfono móvil, domicilio particular, situación patrimonial de una persona física, etc. Sin embargo, debe tratarse de datos

«*registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado*», como, por ejemplo, los almacenados en un ordenador personal o en una cuenta de correo electrónico⁴². No obstante, el Tribunal Supremo ha matizado que la perfección del tipo requiere que el ordenador sea un lugar idóneo para el archivo o almacenamiento de datos personales del titular, lo que no sería el caso de los ordenadores adscritos a una Administración Pública o de los ordenadores de uso compartido por varias personas⁴³.

Queda por último referirse al requisito de la «ausencia de autorización». Es evidente que el legislador se refiere a la autorización del titular del dato personal automatizado⁴⁴ (*in casu*, el empleado o directivo cuyo ordenador es inspeccionado por las autoridades), pero debe entenderse que también una autorización judicial excluiría la tipicidad de la conducta del funcionario. No obstante, y en coherencia con la especial protección que el legislador ha querido dispensar a los datos personales automatizados, la referida autorización judicial debería satisfacer un mínimo de especificidad e indicar —al menos— la identidad de las personas cuyos ordenadores podrán inspeccionarse, así como autorizar específicamente a los funcionarios de la autoridad de competencia a acceder a las cuentas de correo electrónico y demás sistemas o archivos informáticos susceptibles de incorporar datos personales protegidos por el artículo 197.2 CP. Por el contrario, es igualmente evidente que una eventual autorización de la empresa investigada no sería suficiente para excluir el tipo penal, toda vez que ésta no es responsable ni titular de los datos personales de sus empleados almacenados en los ordenadores y sistemas informáticos investigados⁴⁵.

38 «Por lo tanto, los acusados al acceder a estos archivos, asumieron con dolo eventual, o por mejor decir de indiferencia, [...] que con su proceder podrían vulnerar la legalidad penal, en tanto que el sistema de correo electrónico es un archivo, soporte o fichero que contiene datos, bases de datos e información que pueden ser reservados de carácter personal o familiar de otro. Como consecuencia de lo anterior, podemos asentar que en los acusados al abrir el sistema Outlook Express, concurría el elemento subjetivo de volición requerido, en su forma de dolo eventual, siendo suficiente situarse en una posición de indiferencia respecto del contenido posible de la aplicación Outlook Express, y sin representación, ni posibilidad de acometer ningún acto de averiguación para poder prever el alcance de su conducta. No existió dolo directo [...] pero sí hubo un dolo eventual al conocer los autores que con su acción creaban un peligro no permitido y cercano para el bien jurídico protegido, ejecutando a pesar de todo los actos queridos, bien porque el resultado les era indiferente o bien porque, considerándolo probable, lo aceptaron, aun cuando no lo pretendieran directamente. En palabras del Tribunal Supremo, la intención no va entonces referida al resultado sino a la conducta, y a aquella se une la aceptación del resultado probable o la indiferencia sobre su producción, de modo que éste se imputa a título de dolo eventual» (SAP Huelva de 16 de junio de 2006). En idéntico sentido, vid. SAP Barcelona de 18 de enero de 2008.

39 STS 123/2009, FJ 4.º.

40 STS 234/1999, de 18 de febrero.

41 STS 1461/2001, de 11 de julio (FJ 3.º, 5).

42 «Y como también se analizó, el sistema de correo Outlook Express participa de la naturaleza de fichero o soporte de datos en tanto que conserva además de los mensajes concretos, listados de mensajes enviados o recibidos, libreta de direcciones, etc. [...] (SAP Huelva de 16 de junio de 2006). Nótese que lo protegido por el artículo 197.2 CP es el dato o información personal, y no el propio correo electrónico en sí mismo, que goza de protección específica en el artículo 197.1 CP (vid. SAP Barcelona de 18 de enero de 2008).

43 Vid. STS 358/2007, de 30 de abril.

44 Vid. STS 1461/2001, de 11 de julio.

45 Vid. SAP Madrid de 15 de abril de 1999, en la que se considera que la autorización otorgada por quien es legalmente responsable de la custodia de los datos personales automatizados excluiría el tipo penal.