

Sr. D. José Carlos Pajares de Frutos
Secretario General del Sindicato FSP/UGT-Ávila

Avda. Portugal, 47, B1
05001 AVILA

Estimado Sr. Pajares de Frutos:

Celebro con satisfacción el interés que demuestra en el conocimiento veraz de los hechos que advierte en su misiva, créame que, siendo como soy consciente de la relevancia de tales hechos y actuaciones, ese interés lo entiendo no sólo justificado, sino que lo comparto plenamente.

Le ruego que me permita, en mi respuesta, seguir el orden de sus interrogantes.

¿Qué delito de suma gravedad se pretende destapar o detectar que justifique este despliegue de medios, que imaginamos no será barato, en medio de una crisis económica como la que sufrimos que ha obligado incluso a eliminar las pagas extra de los trabajadores?

Creo entender que reconoce en su pregunta la existencia de un delito. No se si esa era su intención o si se trata de una argumentación retórica. Resuelvo el dilema afirmando que, efectivamente, nos hallamos ante la comisión, no de un delito, sino de un presunto delito.

Para ser más preciso, el propio auto del Juzgado de Instrucción, de 7 de diciembre de 2012, afirma y reconoce que los hechos investigados son constitutivos de infracción penal. Tales hechos guardan relación con el ataque y difusión de correos injuriosos e infamantes, cuyo contenido, en el hipotético caso de que no los conociera, no tendré inconveniente alguno en facilitarle para su mejor valoración.

Sí deseo participarle ciertas reflexiones sobre los aspectos que me parecen más graves, eludiendo entrar a considerar el tono gratuitamente ofensivo, insidioso, falaz, manipulador, etc. común a todos ellos. En este sentido, uno de los correos resulta particularmente ultrajante contra la dignidad de las mujeres, alegando que la contratación de una mujer por parte de la Diputación, bajo la modalidad de funcionaria eventual, fue realizada por razón de un embarazo. Permítame que, por respeto, en este supuesto particular obvie dar nombres o más detalles.

Otro denominador común de los correos es el de la imputación de negligencias, ilegalidades y abiertas amenazas contra determinados trabajadores de la Diputación, revelando su identidad y cargo que ocupan.

Como ve, me reservo mostrar opinión sobre los ataques que a mi persona, y a la de otros diputados, se hacen en tales libelos; supongo que usted razonará que tales insultos, cobardes y anónimos, van en el sueldo. Me limitaré a invitarle a que haga un sincero ejercicio de reflexión sobre ello.

En cuanto a la gravedad de tales conductas "presuntamente" delictivas, desconozco qué criterio o qué valor les atribuye usted en su fuero interno. El valor del honor, de la propia imagen, la fama, de la verdad, la justicia, la integridad moral (y física, si tomamos en serio las amenazas) de las personas, sería motivo de un interesante debate, pero no se si usted tiene ganas o tiempo para ello. Por el contenido de su pregunta, y su apelación a la crisis económica, intuyo que está más interesado en lo crematístico. Le puedo asegurar que todos los alcaldes de la provincia, y yo lo soy, tienen presente la crisis económica con la misma o mayor preocupación que usted; sin embargo, no eludiré su pregunta sobre el coste "no barato" que considera tendrá el "despliegue de medios". Resulta irónico que, por contraste, el valor de una contratación le va permitir conocer en cuanto tasa usted intangibles tan extraordinariamente importantes: verdad y justicia, honor, imagen, fama, integridad, etc. Como irónico resulta considerar que esta crisis económica, según se afirma en círculos políticos, sociales y académicos, tiene como causa una crisis de valores. Valores como los que esta Diputación pretende defender con su actuación. Permítame que se los repita: verdad y justicia, honor, fama, imagen personal e integridad.

El precio, en cuestión, es equivalente al valor de un contrato menor: 18.000 euros. Permítame que le diga que para este presidente, teniendo en cuenta los valores que pretendo defender, el precio es más que razonable, como también lo sería si hubiera sido sensiblemente más elevado.

No se si mi respuesta le satisfará; reconozco que me hubiera facilitado mucho la tarea saber en qué valor tasa su honor, su imagen o su fama, o los de la honorable organización sindical a la que sirve, porque como supongo será conocedor, las personas jurídicas también tienen derecho al honor. Así lo reconoce el TC, en Sentencia de 26 de septiembre de 1995, y consagra la doctrina del Tribunal Supremo; destacando la sentencia de 9 de octubre de 1997, donde el TS manifiesta, de forma taxativa, que el honor, fama o prestigio de una persona jurídica, atacada en su buena fama prestigio u honor tiene acción para su protección, ya que aunque el honor es un valor referido a personas individualmente consideradas, el derecho a su propia estimación no es patrimonio exclusivo de las mismas; y el significado del derecho al honor no puede ni debe excluir de su ámbito de protección a las personas jurídicas, que pueden ver lesionados sus derechos a través de la divulgación de derechos concernientes a su entidad cuando la difame o la haga desmerecer de la consideración ajena.

Le ruego me permita ilustrar un poco más esta idea, sobre el valor que cabe atribuir a la fama y honor de las personas jurídicas, poniendo como ejemplo a su propia organización: UGT; trayendo a colación una sentencia del TS Sala de lo Civil, Sección 1ª, 1160/2008, de 27 de noviembre. En dicha sentencia de Casación, en un procedimiento seguido a instancia de Unión General de Trabajadores (UGT) contra "Central Sindical Independiente de Funcionarios" CSI-CSIF, el TS condenó a ésta última central sindical invocando la doctrina del derecho al honor de las personas jurídicas, considerando sobrepasado el límite de las manifestaciones protegidas por la libertad de expresión, radicado en el menosprecio personal, la vejación injustificada y el insulto. El TS impuso, en este proceso civil, una indemnización de 10.000 euros.

UGT no se arredró por factores tales como las costas procesales en una vía jurisdiccional como la civil, jurisdicción voluntaria, y donde no impera el principio de gratuidad; ni por la incertidumbre de si la indemnización, en el hipotético caso de que se fallase a su favor, sería suficiente para resarcir los costes del procedimiento. UGT optó por apurar todos los escalones del sistema judicial hasta llegar al Tribunal Supremo. Y yo felicito y aplaudo esta determinación, porque obedece a un impulso de salvaguarda de valores superiores.

Es esa misma determinación la que entiendo debe reconocer en la actuación de la Diputación frente a presuntos actos delictivos cometidos contra personas físicas, trabajadores que han visto lesionados derechos fundamentales básicos, y contra la propia Institución que presido.

¿Se ha contratado una empresa de seguridad privada para impulsar una investigación que ya se puso en su momento en conocimiento del juzgado núm. 4 de nuestra provincia?

No, no se ha contratado una empresa de seguridad privada. El contrato, al que entiendo se refiere, vincula a la Diputación Provincial de Ávila con una empresa de seguridad de la información, que no es lo mismo que de seguridad privada, dedicada al desarrollo de soluciones de seguridad informática específica y a medida, consultora de I+D y Seguridad, y con un propósito que se recoge en la propuesta económica presentada por la citada empresa. Los detalles serían los siguientes, sin perjuicio de los cuales le remitiré al propio contenido de la propuesta:

Nombre de la empresa: DRAIMWARE Security Intelligence, S.L.

Objeto de la propuesta económica: Recabar los datos referentes a unos hechos, posiblemente delictivos, ocurridos en fechas anteriores por parte de una/s persona/s indeterminada/s dentro de su corporación. Añadido a todo este trabajo forense y de investigación, se solicita que Drainware desarrolle un informe sobre la seguridad en su red y los posibles cambios que se puedan realizar para mejorarla. Esta mejora será implantada en varias fases, lo que asegurará su implementación. Se llevará a cabo con la máxima pulcritud y confidencialidad, siendo una de las principales peticiones de la Diputación.

Alcance de la propuesta (proyecto): El alcance consistirá en obtener la mayor información posible de hecho sobre hechos que hayan podido haber ocurrido, mientras respetemos la ley de protección de datos y todas las garantías legales necesarias. El estudio de la red tendrá como misión recabar todos los datos posibles sobre utilización, agujeros de seguridad, y grandes deficiencias. Todo ello con el fin de subsanarlos y obtener unos mínimos niveles de seguridad que permitan el uso de la red y la conexión a Internet de forma segura, evitando en todo lo posible el uso indeseado de la misma.

Con respecto al análisis forense, se realizará de manera escalonada cumpliendo con la legislación vigente y su objetivo será obtener información acerca del uso de alguno o algunos de los equipos de la Diputación para fines posiblemente ilícitos, e identificar el

equipo o equipos desde los que se realizaron estos hechos. Se realizarán diversas técnicas para obtener información acerca del uso de la red y de los correos electrónicos usados para el ilícito. En pro de garantizar el respeto a datos de carácter confidencial y que sean guardadas todas las garantías legales, previa aceptación de la oferta, quedará firmada por ambas partes el documento de confidencialidad que se adjunta como anexo. Como anexo 2 se adjuntan las políticas de seguridad revisadas y adaptadas, las cuales deben de ser comprendidas y aceptadas por todos los usuarios de la red en la Diputación.

Las actuaciones se desarrollan en el marco del deber de colaboración con la Justicia, al existir una actuación judicial, diligencias previas 119/12, seguidas ante el Juzgado de Instrucción núm. 4 de Ávila, en relación con las Diligencias Policiales 2494 de 18 de junio de 2012. Respondiendo a las cuestiones que desde la propia investigación policial son planteadas a la Corporación, para su posterior remisión al Juzgado.

¿A través de qué mecanismo de la Ley de Contratos de las Administraciones Públicas se ha contratado esta empresa?

El "mecanismo" al que hace referencia guarda relación con el expediente de contratación propio de los contratos menores, regulado en el artículo 111 y 138.3 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público. La tramitación del expediente exige la aprobación del gasto y la incorporación de la factura. Los contratos menores podrán adjudicarse directamente a cualquier empresario con capacidad de obrar y que cuente con la habilitación profesional necesaria para realizar la prestación, cumpliendo con las normas establecidas en el [artículo 111](#). Se consideran contratos menores los contratos de importe inferior a 50.000 euros, cuando se trate de contratos de obras, o a 18.000 euros, cuando se trate de otros contratos, sin perjuicio de lo dispuesto en el [artículo 206](#) en relación con las obras, servicios y suministros centralizados en el ámbito estatal.

¿Cuanto les va a costar a los ciudadanos de la provincia de Ávila los servicios de esta empresa?

Esta es una pregunta que, aun siendo formulada con un planteamiento extraordinariamente demagógico, me permite invitarle a que realice otro sano ejercicio de reflexión. ¿Qué costaría a la Diputación de Ávila no contratar los servicios de esta empresa y cubrir una necesidad objetiva en materia de seguridad informática? ¿Qué coste tiene para una Administración Pública no perseguir una conducta delictiva con perjuicio de terceros?

Por si no lo sabía, los hechos investigados que motivaron la actuación judicial, y calificados en el auto del Juzgado de Instrucción como "constitutivos de infracción penal", fueron realizados desde un ordenador de la propia Diputación, justo al inicio de la jornada de trabajo. Más concretamente, desde los ordenadores del Palacio Provincial cuyo acceso a internet se realiza por la IP 194.179.120.42. Este dato, así como la referencia horaria exacta del hecho justo al inicio de la jornada de trabajo, ha sido

acreditado por la investigación policial. Debemos tener bien presente este hecho por varias razones:

Primera y más importante, la Diputación, como Institución, no tolera ni ampara conductas delictivas dentro de su organización, bajo ningún concepto.

Segunda, con independencia de que la naturaleza antijurídica del hecho merezca o no reproche penal, siempre que se constata un daño a terceros que no deba ser asumido por estos, la responsabilidad de las Administraciones Públicas está informada por un principio de responsabilidad objetiva. Esto supone que la Diputación se puede ver obligada a responder del daño causado frente a terceros siempre que el daño que se le imputa, ya sea por un funcionamiento normal o anormal de los servicios, sea efectivo, evaluable económicamente e individualizado y que exista relación de causalidad. Como bien sabrá la responsabilidad de las Administraciones Públicas cubre tanto los daños físicos, como morales.

Sin ánimo de eludir la respuesta, le ruego que me evite la demagogia de tener que escribir el dato exacto. Como muy bien habrá podido deducir, el coste de los servicios de la empresa para los ciudadanos, que centra su interés, puede ser calculado mediante la sencilla división de los 18.000 euros del contrato menor entre el número de habitantes de la Provincia.

¿Se han tomado las precauciones imprescindibles para que cada trabajador tenga una clave exclusiva de su ordenador que no pueda ser utilizada por otros usuarios informáticos, etc. o como nos aseguran en la Diputación siempre ha existido la práctica de que varios trabajadores conozcan las claves de más de un ordenador y los informáticos accedan sin previo aviso de su usuario habitual a cualquier ordenador?

Cada empleado de la Diputación tiene asignada su propia contraseña individual para poder acceder a su ordenador. Es evidente que el uso que cada empleado haga de esa contraseña es de su exclusiva responsabilidad. Soy plenamente consciente que en esta materia no se ha estado actuando con la debida diligencia, siendo esta una de las razones que han motivado la aprobación de una serie de directrices para mejorar nuestra seguridad informática, advirtiendo también, con cierta y sorprendente contestación y fuerte crítica por parte del sindicato que usted representa, quien ha visto en estas directrices un pretendido ejercicio de autoritarismo sobre los empleados, sin considerar que las mismas previenen los peligros derivados de una posible suplantación de usuarios, amenaza de la que usted muestra una lógica preocupación.

Sobre la afirmación de que los informáticos acceden sin previo aviso de su usuario habitual a cualquier ordenador, debo contestarle mi sorpresa por tamaña afirmación y no pudiendo imaginar de quién o dónde ha obtenido dicha información. No se si entiende que en la pregunta que me formula está lanzando una gravísima acusación contra los empleados del departamento de informática de esta Diputación; por ello le rogaría que, o bien aporta elementos de prueba más tangibles y consistentes que sus palabras, o bien le invito a que reconsidere la conveniencia de formular esta pregunta.

Sin perjuicio de lo anterior, me permito asegurarle que los accesos telemáticos o remotos a los equipos han estado siempre prohibidos en esta casa. No consta ni existe ninguna autorización expresa para realizar tales operaciones. Cualquier acceso de estas características sería considerado como una violación de la seguridad informática. Si se constataste un intento de acceso de estas características, y se demostrase su existencia, sería perseguible como delito informático sin ningún género de dudas y el responsable o responsables, ya sean personal de la casa o ajenos a ella, perseguidos legalmente.

Indicarle, por último, que todos los accesos de los empleados del departamento de informática se realizan a petición expresa del usuario, quien debe aceptar la operación de acceso. Le ruego que para más detalle de estas operaciones consulte directamente con el departamento de informática de la Diputación provincial.

Le recuerdo que la figura del administrador del sistema, en cualquier sistema, en el desempeño de sus labores, supone necesariamente gestionar las contraseñas de todos los integrantes de la entidad. Es por tanto una figura íntegra y que recibe la confianza de la gestión de las mismas, al igual que el resto de integrantes del equipo de informáticos.

En línea con lo anterior le informo que, según el punto tres del documento de VIGILANCIA Y CONTROL DE LAS COMUNICACIONES ELECTRÓNICAS EN EL LUGAR DE TRABAJO EN EL MARCO DE LA DIRECTIVA 95/46/CE del Parlamento Europeo, los administradores de sistemas están sometidos a una obligación estricta de secreto profesional respecto a la información confidencial a la que se pueda acceder.

Tras la contratación de la empresa DRAIMWARE, tal y como está recogido en la política de seguridad recientemente aprobada, dentro del apartado de responsabilidades de los usuarios:

“...el usuario es responsable de proteger y mantener la confidencialidad de la información perteneciente o confiada a la Diputación y deberá contribuir de manera activa al secreto de la misma.”

“El usuario se hace responsable de sus contraseñas y bajo ninguna circunstancia debe divulgarlas o cederlas al resto de usuarios. Las contraseñas de usuario serán robustas y difícilmente adivinables por terceros no autorizados, proporcionadas directamente por el Departamento de Informática.”

De igual manera, desde la citada empresa, se ha realizado la recomendación de la instalación del directorio activo o LDAP. Con esta tecnología se impide el acceso y el conocimiento de las contraseñas de los usuarios pues deben de ser cambiadas por ellos mismos. Pueden sin embargo resetear la clave debiendo comunicarse a los usuarios.

Por otra parte y como se ha venido constatando debido a los ataques sufridos desde dentro de la Diputación y para la preventiva fuga de información y mal uso de los medios suministrados, se implementará un sistema DLP (Data Loss Prevention) unido a un sistema integral contra APT (Advanced Persistent Threats) que posibilitará a la

entidad de una protección y una adecuación a las nuevas amenazas y tecnologías de un modo innovador y ejemplar.

Los datos confidenciales generados serán publicados a la AEPD para que se garantice el uso correcto de todo el flujo y los derechos tanto de los usuarios como de la entidad.

¿Cómo se va a garantizar la cadena de custodia, siendo una empresa privada la que está realizando la clonación de los discos duros?

La cadena de custodia es uno de los pasos de la investigación muy importante y que se traduce en la recolección, manejo, preservación y almacenamiento de los elementos materiales de prueba que luego de haberse sometido a un examen especial van a constituir medios de prueba, para finalmente ser sometido al contradictorio y sean consideradas como pruebas.

La Cadena de Custodia se inicia con el aseguramiento, inmovilización o recojo de las evidencias, durante las primeras actuaciones o incorporados en el curso de la Investigación preparatoria; y, concluye con la disposición o resolución que establezca su destino final. Asimismo se ha considerado elaborar un formato de cadena de custodia, donde las evidencias se registraran en éste mediante una descripción minuciosa y detallada de las técnicas utilizadas en el recojo y pericias que se dispongan.

Requisitos:

- .- Identidad de las personas actuantes
- .- Fecha y lugar donde se efectúa la adquisición de datos.
- .- En caso de que alguna persona presencie la adquisición, se identificará en el acta y se le invitará a firmarla.

En el caso de evidencias digitales, la cadena de custodia queda acreditada por la firma digital obtenida de las evidencias, quedando firmada y protegida con un sello logarítmico (Logaritmo de cálculo Hash SHA-1 ó 256) que permite que, en caso de la modificación de un solo bit de información, la firma cambie completamente desvirtuando la evidencia.

Es por tanto necesario adjuntar documento anexo con relación de las evidencias obtenidas y su firma digital correspondiente.

¿Cómo se va a preservar el derecho a la privacidad de los trabajadores sin vulnerar derechos fundamentales, cuando durante los últimos años, la práctica habitual en la Diputación no incluía ninguna directiva de uso de los ordenadores, que prohibiera acceder por ejemplo a correos electrónicos personales?

El estudio forense de las evidencias obtenidas se limitará, repito, se limitará, exclusivamente a la localización de diversas claves textuales extraídas de documentos relacionados con la investigación en curso por esta Diputación, quedando sin embargo a diligencia de ésta, como es su deber, el hecho de solicitar a la Autoridad Judicial ampliación de las actuaciones en el caso de que los resultados de ésta búsqueda descubra un uso ilegal o delictivo de otra índole.

Todo este marco forense queda contractualmente ligado a una estricta Política de Confidencialidad hecha pública entre la Diputación de Ávila y la empresa Drainware Systems SL. Acuerdo de Confidencialidad aprobado por acuerdo de la Junta de Gobierno de 21 de enero de 2013.

El procedimiento utilizado para obtener pruebas relevantes de los dispositivos electrónicos involucrados (discos duros) en la investigación, es el denominado de “búsquedas ciegas”. La jurisprudencia ha reconocido que dicho procedimiento salvaguarda plenamente los derechos fundamentales de las personas afectadas por la investigación.

El procedimiento de búsquedas ciegas se realiza mediante la selección de unas palabras clave facilitadas a los investigadores en relación con el caso. El resultado de las búsquedas ciegas permite descartar cualquier archivo o contenido que no guarde relación estricta con el caso, de modo que el procedimiento utilizado no supone acceso a información o datos de carácter personal, quedando salvaguardados los derechos fundamentales a la intimidad o al secreto en la comunicaciones. El resultado del computer forensic tras la fase de búsquedas ciegas se traduce en un informe técnico-pericial que pueda ser utilizado como medio de prueba ante el Juzgado.

En el caso concreto del tratamiento de las evidencias obtenidas de la adquisición de información del análisis forense, el equipo de auditores cumplirá con las mejores prácticas del sector y las herramientas pertinentes que permitan el estricto cumplimiento de secreto profesional en cuanto a la información confidencial almacenada en los volcados de disco.

Todo este marco forense queda contractualmente ligado a una estricta Política de Confidencialidad hecha pública entre la Diputación de Ávila y la empresa Drainware Systems S.L.

Para mejorar el nivel de seguridad de la Diputación, se realizará la integración y parametrización de una plataforma de seguridad de última generación. Dicha plataforma contará con 2 módulos:

Data Loss Prevention: permitirá analizar la información con la que trabaja la Diputación a diario para identificar posibles comportamientos de fuga de información sensible.

Advanced Persistent Threats: para ofrecer las mejores garantías, solo permitirá la ejecución de las aplicaciones más vulnerables (como pueden ser Internet Explorer, Acrobat Reader, Adobe Flash ó Oracle Java) dentro de una sandbox para evitar intentos

de ataques dirigidos de tipo APT (Advanced Persistent Threats). Este tipo de ataque son de la misma naturaleza, que los descubiertos recientemente, que tenían como origen China y por objeto la recopilación de información sensible alrededor del mundo mediante el despliegue de malware equipado en muchos casos de exploits que abusan vulnerabilidades de tipo 0day. Entre las técnicas empleadas se encuentra la detección en memoria en tiempo de ejecución de: rastros de nopsled, heap spray, técnica rop, ... de malware no categorizado por los motores antivirus. La compañía Drainware tiene experiencia en esta área y ha desarrollado recientemente y con éxito una integración a medida con una entidad pública que estaba siendo atacada desde fuera de España.

¿Qué garantía tenemos de que no se va a responsabilizar a un trabajador de algo que se haya hecho desde su ordenador, sin tener la absoluta seguridad de que haya sido él el que lo ha hecho?

Como usted bien sabe, vivimos en un Estado de Derecho. No se muy bien que quiere decir cuando exige tales "garantías". Le ruego que analice detenidamente su pregunta, si lo hace, se dará cuenta de que formulándola en tales términos usted presupone que la actuación de la Justicia (en la vertiente judicial de este asunto) o administrativa (en la vertiente disciplinaria) está sometida a una arbitrariedad intolerable e incompatible con los principios informadores del Estado de Derecho. Tengo bien presente que todas las actuaciones que se lleven a cabo desde la Diputación estarán enmarcadas en el más escrupuloso cumplimiento de la legalidad, y en defensa del interés general. La garantía es la Ley, nadie está por encima de ella.

¿Se van a investigar todos los ordenadores de la Diputación, incluyendo políticos, cargos de confianza y el suyo propio o las pesquisas solo se circunscribe a los trabajadores y por tanto se les toma a estos como presuntos culpables de algún delito?

El Computer Forensic se llevará a efecto conforme la metodología recogida en la resolución de 8 de febrero de 2013. Eso incluye y afecta, potencialmente y según el devenir del propio análisis, a todos los equipos informáticos existentes en el Palacio Provincial que acceden a Internet por la IP 194.179.120.42

Intervención policial y toma de huellas dactilares.

Si bien usted no formula ninguna pregunta sobre este particular, el hecho de que lo mencione en su carta, las dudas que parece mostrar sobre estos acontecimientos y la gravedad que personalmente le atribuyo a esta cuestión, me animan a que aborde el tema con el exclusivo ánimo de informarle.

Lamentablemente, debo confirmarle que efectivamente fue requerida la presencia policial en el Palacio Provincial. La razón que motivó su presencia y posterior investigación guarda relación con un desagradable y grave suceso que se produjo el viernes, 14 de febrero, mientras el personal de la empresa DRAIMWARE realizaba sus

trabajos de adquisición de datos en los ordenadores del Departamento del Boletín Oficial de la Provincia. Así, en determinados momentos de los que existe constancia documental, se produjeron varios cortes de luz que interrumpieron y obligaron a reiniciar los trabajos, provocando además el daño de uno de los discos de trabajo de la citada empresa.

Existen fundadas sospechas de que los cortes de luz no fueron accidentales, sino intencionados, lo que constituiría un acto deliberado de sabotaje. Dado que se cuenta con múltiples evidencias, al quedar precintada tras el último corte de luz la caja de mandos desde la que, supuestamente y según informes de los electricistas de la Diputación, se debían realizar los cortes (dadas las características de los mismos) el cotejo de huellas resultó muy valioso. Otra evidencia fundamental ha sido obtenida de las cámaras de seguridad, cuyas imágenes fueron visionadas por la policía y obran en su poder para lo que pueda disponer la autoridad judicial.

He dejado para el final responder a su escrito de solicitudes:

- a) Se nos tenga por personado en el expediente de contratación.
- b) Se nos de vista de todo el expediente conforme a la legislación vigente.

Debo recordarle que los expedientes de contratación no son expedientes contradictorios. No existe un derecho subjetivo que pueda invocar como interesado para "personarse" en el mismo.

Debo recordarle también que si algo caracteriza al contrato menor es precisamente su carácter esencialmente informal. La regulación de los contratos menores obedece, desde un punto de vista finalista o teleológico, al objetivo de la simplificación del procedimiento jurídico administrativo de contratación. En los contratos menores no existe propiamente un expediente de contratación, sino que los únicos trámites del contrato menor serían: la aprobación del gasto y la incorporación de la factura. De tal modo que, en cuanto sea presentada la factura por la empresa, estaré muy gustoso de remitirle la copia oportuna.

Sin otro particular, atentamente le saluda,

EL PRESIDENTE,

Fdo.: Agustín González González

CLAVES

1º.- Hemos comprobado una conducta delictiva dentro de la casa, estamos obligados a actuar.

2º.- Sr. Frutos, en su carta muestra preocupación por todo el colectivo de empleados de Diputación, independientemente de su filiación sindical, lo cual es loable. Evidentemente no conozco la sindicación de los empleados que sufrieron estos ataques

anónimos, pero le ruego que considere la conveniencia de dirigirse a ellos y trasladarles su apoyo y el de su organización sindical.

3º.- Condena sin paliativos de estas prácticas delictivas o cuasidelictivas. debemos entender que en política, acción sindical y cualquier otro orden de la vida, no todo vale.

4º.- Tiene alguna propuesta que hacer o que desee sugerir a esta Institución para acometer esta crisis.

5º.- (confidencial) Se han recibido correos postales anónimos delatando posibles responsables entre los cuales me consta se hallan afiliados suyos. Sepa que esta Institución ha hecho oídos sordos a todas esas acusaciones.