Datuak Babesteko
Euskal Bulegoa

Agencia Vasca de
Protección de Datos

CN15-014

DICTAMEN QUE SE EMITE EN RELACIÓN CON LA CONSULTA PLANTEADA

Solicitante: Departamento de […]

Consulta planteada Habilitación para filtrado de correo electrónico con fines de seguridad para detección y reacción ante ciberamenazas

ANTECEDENTES

Primero. Con fecha 20 de agosto de 2015 tiene entrada en esta Agencia Vasca de Protección de Datos un correo electrónico procedente del Responsable de Sistemas de Información del Departamento de […], por el que se plantea consulta en relación al asunto de referencia.

Segundo. La consulta tiene su origen en una reciente oleada de correos electrónicos que se han recibido en diferentes buzones de la Red […] del Departamento […], conteniendo determinado tipo de virus ("Cryptolocker"), que también se han recibido en la Red Corporativa Administrativa del Gobierno Vasco.

Los responsables de la Red […] han diseñado diferentes medidas preventivas y correctivas para evitar y mitigar los efectos de dicho ataque, que deben complementar las soluciones que proporcionan los "antivirus" habituales. Dichas medidas implican filtrar los buzones de correo de los usuarios para identificar los correos sospechosos, mover dichos mensajes a un área de "cuarentena" y, en su caso, eliminar las amenazas identificadas.

Por parte de los administradores técnicos se han planteado si existe habilitación para realizar dicho filtrado y supresión de correos, y si ello supondría una intromisión en la privacidad de los usuarios de los buzones de correo.

Tercero. El artículo 17 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, en su apartado n) atribuye a la Agencia Vasca de Protección de Datos la siguiente función:

> *"Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta Ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de esta Ley".*

Corresponde a esta Agencia Vasca de Protección de Datos, en virtud de la normativa más arriba citada, la emisión del informe en respuesta a la consulta formulada.

CONSIDERACIONES

I – CORREO ELECTRÓNICO Y CONTROL DE LA ACTIVIDAD LABORAL

El correo electrónico, como forma de comunicación que es, goza de la protección constitucional que le otorga el artículo 18.3 de la Constitución española:

> *"Artículo 18*
>
> *(…) 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".*

Sin embargo, en el marco de las relaciones laborales, el Estatuto de los Trabajadores reconoce a los empleadores una facultad de supervisión sobre la actividad los empleados y los medios que utilizan, tal como se recoge en su artículo 20.3:

> *"Artículo 20. Dirección y control de la actividad laboral.*
>
> *(…) 3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso. (…)".*

Dicha facultad de control de la actividad laboral no es absoluta, y así lo ha establecido el Tribunal Supremo en una Sentencia de 26 de septiembre de 2007 (STS 6128/2007 - ECLI:ES:TS:2007:6128)[1], dictada en un Recurso para Unificación de Doctrina, puesto que debe existir, y existe, un cierto "margen de tolerancia" en el uso personal de los medios facilitados por el empleador y, por tanto, una "expectativa de privacidad" que hay que respetar:

> *"(…) CUARTO.- El control del uso del ordenador facilitado al trabajador por el empresario no se regula por el artículo 18 del Estatuto de los Trabajadores , sino por el artículo 20.3 del Estatuto de los Trabajadores y a este precepto hay que estar con las matizaciones que a continuación han de realizarse. (…).*
>
> *En este punto es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio.*
>
> *Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar*

[1] Disponible en http://www.poderjudicial.es/search/documento/TS/326542/Despido/20071018

la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos".

Sobre la cuestión del tratamiento del correo electrónico dentro del ámbito laboral también se han pronunciado las Autoridades de Protección de Datos, tanto la Agencia Española de Protección de Datos, como el "Grupo de Trabajo del Artículo 29"[2] (en adelante, Art29WP) en varios de sus documentos de trabajo, entre los que pueden destacarse los siguientes:

- Opinión 8/2001 (WP48)[3] sobre el tratamiento de datos personales en el contexto laboral
- Documento de trabajo de 29-05-2002 (WP55)[4] relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo
- Dictamen 2/2006 (WP118)[5] sobre el respeto de la privacidad en relación con la prestación de servicios de cribado de correo electrónico

El primero de los documentos citados (WP48) analiza el marco legal, tanto europeo como de cada país, y establece principios generales que deben guiar el tratamiento de los datos personales de los empleados. Resulta de especial interés la consideración de que la obtención del consentimiento ***no es*** el instrumento más adecuado para legitimar el tratamiento de datos en el ámbito laboral:

«Si un empresario debe tratar datos personales como consecuencia inevitable y necesaria de la relación laboral, actuará de forma engañosa si intenta legitimar este tratamiento a través del consentimiento. El recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello.»

El segundo de los documentos citados (WP55), establece las principales directrices aplicables acerca de la legitimación del tratamiento de los datos de los trabajadores, en

[2] Órgano con carácter consultivo e independiente creado por el artículo 29 de la *Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Su misión es, en particular, examinar todas las cuestiones relativas a la aplicación de las medidas nacionales adoptadas en virtud de la Directiva sobre protección de datos con el fin de contribuir a su aplicación uniforme.

[3] Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[4] Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_es.pdf

[5] Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp118_es.pdf

especial cuando implica un control del correo electrónico y la vigilancia del acceso a internet.

Este documento establece que el tratamiento de datos debe legitimarse únicamente en la ***satisfacción del interés legítimo del responsable del tratamiento, en circunstancias limitadas, excepcionales y concretas***, combinado con una estricta aplicación del ***principio de transparencia***, que se concreta en proporcionar suficiente ***información*** al interesado y garantizar el derecho de ***acceso*** a los datos que hayan sido tratados.

Estas directrices han sido recogidas por la Agencia Española de Protección de Datos, la cual se ha pronunciado sobre esta cuestión en numerosas ocasiones[6] y cuya doctrina ha plasmado en la Guía *'La protección de datos en las relaciones laborales',* (2009)[7], que puede resumirse en:

- *La legitimación para el tratamiento deriva de la existencia de la relación laboral y, por tanto, de acuerdo con el art. 6.2 LOPD,* ***no se requiere del consentimiento***
- *A la hora de decidir adoptar una medida de control que comporte un tratamiento de datos personales debe aplicarse el* ***principio de proporcionalidad****.*
- *Debe existir una finalidad que, en este caso, no puede ser otra que la establecida por el art. 20.3 ET de «****verificar el cumplimiento*** *por el trabajador de sus obligaciones y deberes laborales».*
- *Los datos que se obtengan y almacenen deberán ser exactos y puestos al día y* ***no podrán conservarse más tiempo del necesario****. Se recomienda a los empleadores fijar un plazo de conservación.*
- *Debe cumplirse con el deber de* ***información a los trabajadores****. Este deber resulta particularmente relevante cuando se trate de controles sobre el uso de Internet y/o del correo electrónico.*
- *En este caso es muy recomendable que la información a los trabajadores sea clara en lo que respecta a la* ***política de la empresa*** *en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales. Así como que incluya la finalidad de la vigilancia, y cuando pueda repercutir sobre medios que el trabajador utiliza normalmente una información sobre las medidas de vigilancia adoptadas.*

II – FILTRADO DEL CORREO ELECTRÓNICO Y SEGURIDAD

Como ya se ha apuntado, el Documento de Trabajo de 2002 (WP55) establece que el tratamiento de datos debe legitimarse únicamente en la ***satisfacción del interés legítimo del responsable del tratamiento, en circunstancias limitadas, excepcionales y concretas***. Pues bien, precisamente la necesidad de ***garantizar la seguridad*** es la

[6] Véanse los informes AEPD 247/2008, 417/2009 y 615/2009
[7] Guía disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales2.pdf

circunstancia limitada, excepcional y concreta a que se hace referencia en dicho documento de trabajo:

"3.1.1. NECESIDAD

(…)Sólo en circunstancias excepcionales se considerará necesaria la vigilancia del correo electrónico o de la utilización de Internet de un trabajador. Podría resultar necesario controlar el correo electrónico de un trabajador para obtener una confirmación o una prueba de determinados actos del mismo. En este tipo de actos se incluiría la actividad delictiva de un trabajador que obligara al empleador a defender sus intereses, por ejemplo, cuando es responsable subsidiario de los actos del trabajador. ***Estas actividades de vigilancia incluirían también la detección de virus y, en general, cualquier actividad realizada por el empleador para garantizar la seguridad del sistema****."*

(…)

"3.1.3. TRANSPARENCIA

(…)Los trabajadores deben ser informados de manera completa sobre las circunstancias particulares que pueden justificar esta medida excepcional; así como del alcance y el ámbito de aplicación de este control. Esta información debería incluir:

> *(…) 2.- Los motivos y finalidad de la vigilancia, en su caso. Cuando el empleador autorice a los trabajadores a utilizar los sistemas de comunicación de la empresa con fines personales, las comunicaciones privadas podrán supervisarse en circunstancias muy limitadas, p. ej.,* ***para garantizar la seguridad del sistema informático (detección de virus)****."*

(…)

"3.1.4. LEGITIMIDAD

(…)En realidad, a menos que la legislación nacional las autorice específicamente previendo garantías adecuadas, las actividades de vigilancia destinadas directamente al tratamiento de datos delicados relativos a los trabajadores no son legítimas de conformidad con la Directiva 95/46/CE ni tampoco aceptables. No obstante, tampoco parece aceptable impedir o complicar en exceso las actividades de vigilancia (que, en muchos casos ***no sólo son legales, sino también deseables, como las que tienen por objeto directamente garantizar la seguridad del sistema****) por el mero hecho de que sea inevitable el tratamiento de información delicada."*

(…)

"3.1.5. PROPORCIONALIDAD

(…)El principio de proporcionalidad excluye por lo tanto el control general de los mensajes electrónicos y de la utilización de Internet de todo el personal, ***salvo si resulta necesario para garantizar la seguridad del sistema****. Si existe una solución que implique una intromisión menor en la vida privada de los trabajadores y que permita lograr el objetivo perseguido, el empleador debería considerar su aplicación (por ejemplo, debería evitar los sistemas que efectúan una vigilancia automática y continua)."*

(…)

"3.1.7. SEGURIDAD

Este principio obliga al empleador a aplicar las medidas técnicas y organizativas adecuadas para proteger todos los datos personales en su poder de toda intromisión exterior. Incluye también el derecho del empleador a ***proteger su sistema contra los virus y puede implicar el análisis automatizado de los mensajes electrónicos*** *y de los datos relativos al tráfico en la red.*

El Grupo de Trabajo opina que, dada la importancia de garantizar la seguridad del sistema, ***la apertura automatizada de los mensajes electrónicos no debe considerarse una violación del derecho del trabajador a la vida privada, siempre y cuando existan garantías adecuadas****. Por ejemplo, los empleadores pueden ahora utilizar tecnologías que responden a sus intereses en términos de seguridad, pero que no violan el derecho de los trabajadores a la vida privada.*

El Grupo de Trabajo «Artículo 29» llama la atención sobre el papel del administrador del sistema, un trabajador cuyas responsabilidades en materia de protección de datos son importantes. Es fundamental que el administrador del sistema, así como cualquier persona que tenga acceso a datos personales de los trabajadores durante las operaciones de control, esté sometido a una ***obligación estricta de secreto profesional respecto a la información confidencial a la que pueda acceder****".*

En definitiva, este documento constituye un marco de referencia suficientemente claro, en cuanto a los tratamientos permitidos y las limitaciones y garantías a establecer cuando del tratamiento sistemático del correo electrónico por parte del proveedor del servicio por razones de seguridad, y su lectura completa, que se recomienda, contribuirá a aclarar otros aspectos más amplios que los que se han planteado en esta consulta.

Finalmente, el Dictamen 2/2006 (WP118) sobre el respeto de la privacidad en relación con la prestación de servicios de cribado de correo electrónico analiza los tratamientos que realizan los prestadores de servicios de internet (ISPs), y en particular de servicios de correo electrónico (ESP), consistentes en aplicar proceso automatizados de monitorización y filtrado ("cribado") de los correos que entran o salen de sus servidores, con diferentes finalidades.

Las finalidades que se contemplan en el Dictamen son las siguientes:

- (A) Detección del virus,
- (B) filtrar "spam" (correo basura)
- (C) detectar contenidos concretos

Respecto del filtrado de correos electrónicos con el fin de detectar virus, el citado Dictamen dice lo siguiente:

"El control antivirus consiste en el proceso de comprobar ficheros para averiguar si contienen virus conocidos. (…).

A la hora de valorar los fundamentos jurídicos que legitiman esta práctica, el Grupo de trabajo 29 opina que la introducción y el uso de filtros por parte de proveedores de correo electrónico con el objetivo de detectar el virus podría justificarse por la obligación de adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, según lo previsto en el artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas citada anteriormente.

(…)

El Grupo de trabajo 29 considera que la utilización de filtros con los fines establecidos en el artículo 4 puede ser compatible con el artículo 5 de la Directiva sobre la privacidad y las comunicaciones electrónicas.

El Grupo de trabajo 29 desea hacer hincapié en que las medidas mencionadas anteriormente deben respetar los principios generales de Derecho comunitario.

(…)

Dado que, de acuerdo con lo anteriormente expuesto, el filtrado de virus se justificaría para preservar la seguridad de los servicios (…), sin perjuicio de la confidencialidad de la comunicación, el Grupo de trabajo 29 recuerda la necesidad de que los proveedores de correo electrónico se atengan al cumplimiento de los siguientes puntos:

(a) el contenido de los correos y los anexos debe mantenerse secreto y no revelarse a ninguna persona que no sea(n) el (los) destinatario(s);

(b) si se detecta un virus, los programas informáticos instalados deben ofrecer suficientes garantías de confidencialidad;

(c) cuando se realice un control antivirus que suponga un análisis de contenidos, debería realizarse de forma automática y sólo con ese fin, es decir, el contenido no debe analizarse con cualquier otro propósito".

Nótese que, en este caso, se trata del tratamiento que haría no el empleador respecto del correo que proporciona a sus empleados, sino los "prestadores de servicios" que incluyan un correo electrónico como parte del servicio. No existe, en este caso, la habilitación para el tratamiento basado en la relación laboral a que se ha hecho referencia anteriormente (artículo 20.3 del Estatuto de los Trabajadores).

Sin embargo, los razonamientos empleados en este caso también son de igual aplicación puesto que, de alguna forma, el empleador está también actuando como proveedor del servicio de correo, y pueden generalizarse para otros incidentes o ciberamenazas que, no constituyendo "virus" específicamente, constituyan una amenaza para la organización o sus empleados (fraudes por "ingeniería social", suplantación de identidad, secuestro de datos y equipos, denegación de servicio, etc).

Nuevamente, se debe llamar la atención sobre el criterio del "Grupo del Artículo 29" en el Documento de Trabajo de 2002 (WP55):

"El Grupo de Trabajo opina que, dada la importancia de garantizar la seguridad del sistema, la apertura automatizada de los mensajes electrónicos no debe considerarse una violación del derecho del trabajador a la vida privada, ***siempre y cuando existan garantías adecuadas****".*

Precisamente, una de las garantías que el "Grupo del Artículo 29" identificaba como adecuadas reside en el papel del Administrador del Sistema (o, en terminología del Reglamento RD-1720/2007, el Responsable de Seguridad):

"El Grupo de Trabajo «Artículo 29» llama la atención sobre el papel del administrador del sistema, un trabajador cuyas responsabilidades en materia de protección de datos son importantes. Es fundamental que el administrador del sistema, así como cualquier persona que tenga acceso a datos personales de los trabajadores durante las operaciones de control, esté sometido a una ***obligación estricta de secreto profesional respecto a la información confidencial a la que pueda acceder****".*

En definitiva: el tratamiento del correo electrónico, con el fin de preservar la seguridad, debe ser efectuado bajo el control del Responsable de Seguridad de la Organización y por profesionales sometidos al secreto profesional, a fin de preservar la garantía de confidencialidad del tratamiento.

No se analizan los otros casos cubiertos por el Dictamen 2/2006 (WP118), como son el filtrado del correo basura o “spam” ni el filtrado de contenidos concretos, por exceder el alcance de este dictamen.

CONCLUSIONES

Primero. El filtrado de correo electrónico con fines de seguridad para detección y reacción ante ciberamenazas, efectuado con garantías de confidencialidad por los administradores de la seguridad del sistema, no supone una violación de las expectativas de privacidad de los empleados.

Segundo. Debe cumplirse con el principio de transparencia, informando a los empleados tanto de forma previa y general de la existencia de la supervisión, como concretamente a posteriori, cuando se haya actuado ante una incidencia o amenaza que les afecte.

Vitoria-Gasteiz, a 4 de setiembre de 2015