Grupo de trabajo del artículo 29 sobre protección de datos

00451/06/ES
Gt 118

Dictamen 2/2006 del Grupo de trabajo 29 sobre el respeto de la privacidad en relación con la prestación de servicios de cribado de correo electrónico

Aprobado el 21 de febrero de 2006

Este Grupo de trabajo se creó de conformidad con lo dispuesto en el artículo 29 de la Directiva 95/46/CE. Se trata de un organismo europeo de carácter consultivo e independiente de protección de las personas en lo que respecta al tratamiento de datos. Su cometido se describe en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.
Ejerce las funciones de secretaría del Grupo la Dirección C (Justicia Civil, Derechos Fundamentales y Ciudadanía) de la Dirección General de la Comisión Europea «Justicia, Libertad y Seguridad», B-1049 Bruselas, Bélgica, Despacho LX-46 01/43.

Website: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

[1]creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995,

Visto el artículo 29, el artículo 30, apartado 1, letra c), y el artículo 30, apartado 3 de la Directiva mencionada,

Visto su reglamento interno, y en particular sus artículos 12 y 14,

HA ADOPTADO LA PRESENTE DECISIÓN:

I. INTRODUCCIÓN

El Grupo de trabajo 29 es consciente de la expansión de los distintos servicios de comunicación en línea, entre los que se encuentran los servicios de correo electrónico gratuitos de la red y otros servicios afines. Con la expansión de los servicios de comunicación electrónicos han surgido dudas respecto a la protección de la privacidad, en concreto, debido a la práctica actual de inspeccionar las comunicaciones con el fin de eliminar el correo masivo no solicitado («buzonfia») y los virus, así como de detectar un contenido concreto.

El Grupo de trabajo 29 no ignora que la mayoría de los proveedores de Internet, así como los de servicios de correo electrónico («ISPs» y «ESPs»), utilizan filtros para proteger tanto las redes como las máquinas y, con menor frecuencia, para inspeccionar las comunicaciones por motivos comerciales. Sin embargo, el Grupo considera que en algunos casos la utilización de filtros puede ser incompatible con las normas vigentes sobre protección de datos expuestas más adelante. Ello puede deberse, entre otros motivos, a que la aplicación de la normativa a estos nuevos tipos de servicios no es siempre fácil.

El principal objetivo de este documento es servir de guía en el tema de la confidencialidad de las comunicaciones por correo electrónico y, más en concreto, en el del filtrado de las comunicaciones en línea. Se ha planteado, en particular, la cuestión de si cribado de las comunicaciones en el que normalmente participan «ISPs» y «ESPs» con la finalidad de cumplir diversos objetivos constituye una intercepción de las comunicaciones que puede justificarse y de qué manera.

Con esta finalidad, el presente documento examina, entre otras cosas, las disposiciones sobre confidencialidad de las comunicaciones electrónicas previstas en el artículo 5, apartado 1 de la Directiva 2002/58 sobre la privacidad y las comunicaciones electrónicas, así como otras disposiciones pertinentes que forman parte del acervo comunitario y de la normativa nacional de aplicación del mismo.

II. MARCO JURÍDICO PARA LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD EN LAS COMUNICACIONES POR CORREO ELECTRÓNICO

A) Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales

La confidencialidad de las comunicaciones está garantizada de conformidad con los instrumentos internacionales relativos a los derechos humanos, especialmente el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEPDH) y las constituciones de los Estados miembros. Asimismo está garantizada por las dos directivas de la UE que se tratan más adelante.

---

[1] DO L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/index.htm

El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEPDH) establece que toda persona tiene el derecho al respeto de su vida privada y su correspondencia, y define las condiciones en las que podría aceptarse la restricción de estos derechos. El Tribunal Europeo de Derechos Humanos («el Tribunal») ha aplicado el artículo 8 a la comunicación por correo postal en diversas ocasiones.

Se ha considerado que los actos de interceptar, abrir, leer, retrasar la recepción de las cartas, o entorpecer su envío constituyen incumplimientos de lo dispuesto en el artículo 8 del CEPDH[2]. De la casuística de la Comisión y de la jurisprudencia del Tribunal de Derechos Humanos, puede concluirse que si se combinan los conceptos de «vida privada» y «correspondencia» las comunicaciones a través de correo electrónico están protegidas, casi con toda seguridad, por el artículo 8 del CEPDH[3]. Las personas que utilizan el correo electrónico para comunicarse pueden tener una cierta seguridad de que su correspondencia no será inspeccionada por terceros, sean estos del ámbito público o privado.

El derecho a que se respete la «correspondencia» no comprende sólo la confidencialidad sino también el derecho de enviar y recibir tal correspondencia[4]. Así pues, puede concluirse que una prohibición de alcance general de envío o recepción de correo electrónico infringiría el artículo 8 del CEPDH.

Toda persona que se encuentre sometida a la jurisdicción de uno de los Estados signatarios del CEPDH tiene derecho al respeto de su vida privada y de su correspondencia. Este concepto comprende a todas las partes implicadas en una comunicación. En el asunto de «A *contra* Francia» (1993) el Tribunal sostuvo que la grabación de una conversación telefónica con el consentimiento de una sola parte era una violación del derecho al respeto de la correspondencia de la otra parte implicada en la comunicación.

Con arreglo a lo dispuesto en el CEPDH, los Estados signatarios del mismo pueden interceptar legalmente la correspondencia, comprendidas las comunicaciones electrónicas, o adoptar otras medidas, si es necesario para alcanzar cualquiera de estos objetivos y conformidad con el Convenio Europeo, de acuerdo con la interpretación de las resoluciones del Tribunal Europeo de Derechos Humanos. La interceptación se define como el acceso de un tercero al contenido o los datos de tráfico de comunicaciones privadas entre dos o más personas, incluidos los datos de tráfico relativos al uso de servicios electrónicos de comunicación que constituya una violación del derecho de un individuo a la intimidad y a la confidencialidad de su correspondencia. Estas interceptaciones son inaceptables a menos que cumplan tres criterios fundamentales, de conformidad con el artículo 8, apartado 2 del CEPDH y según la interpretación que el TEDH hace de esta disposición:

«… una base legal, la necesidad de tal medida en una sociedad democrática, y la conformidad con uno de los objetivos legítimos enumerados en el Convenio…»

---

2 En el asunto Niemitz (1992) el Tribunal dictaminó que el correo ya entregado al destinatario está protegido por el artículo 8 del CEPDH. En esta decisión el Tribunal sostuvo asimismo que no sólo se deben proteger las comunicaciones privadas sino también la correspondencia comercial. En los asuntos Klass (1978), Malone (1984) y Huvig (1990) el Tribunal afirmó que las conversaciones telefónicas también están protegidas por el artículo 8. En relación con otras formas de comunicación, cabe destacar el asunto Mersch de la Comisión (1985), en el que la Comisión consideró que la interceptación de cualquier forma de comunicación constituía una infracción del artículo 8.

3 Esta conclusión se apoya en el hecho de que en la mayoría de los Estados miembros se prohíbe la inspección de correos electrónicos y de que tanto a escala internacional como nacional se han creado instancias específicamente destinadas a interceptar las comunicaciones por correo electrónico.

4 Golder (1975), considerando 43: «*El acto* de *impedir a alguien que llegue incluso a iniciar una correspondencia constituye la forma más grave de injerencia (artículo 8, apartado 2) en el ejercicio del derecho al respeto de la correspondencia; no puede concebirse que este supuesto se excluya del ámbito del artículo 8 cuando la mera supervisión se incluye en él de manera indiscutible*» La retención del correo recibido constituirá asimismo injerencia (Schöneberger y Durmaz, 1988)

Sin embargo, en las relaciones privadas el mecanismo más importante de aplicación de los derechos del Convenio es la doctrina de las obligaciones positivas de las Partes Contratantes. Las Partes Contratantes no sólo tienen la obligación de no injerencia sino también la de adoptar medidas activas que garanticen el ejercicio de estos derechos, no sólo en lo que se refiere a los poderes públicos sino también en la esfera de las relaciones de los individuos entre sí. Este deber comprende la obligación de establecer un marco jurídico adecuado para el ejercicio de estos derechos.

El artículo 6, apartado 2 del Tratado de la Unión Europea dispone que la Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales y tal y como resultan de las tradiciones constitucionales comunes a los Estados Miembros como principios generales del Derecho comunitario. Según el artículo 52, apartado 3 de la Carta de los Derechos Fundamentales de la Unión Europea, el sentido y alcance de los derechos contenidos en la Carta serán iguales a los que les confiere el CEPDH. Esta disposición no obstará para que el Derecho de la Unión conceda una protección más extensa.

B) Disposiciones específicas sobre la confidencialidad de las comunicaciones por correo electrónico

Como se mencionó anteriormente, la confidencialidad de las comunicaciones está además garantizada por dos directivas de la UE. A la hora de tratar el tema de la confidencialidad de las comunicaciones, las disposiciones de estas directivas deben interpretarse en conjunción con el CEPDH y con la jurisprudencia del Tribunal de Derechos Humanos antes citada.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo 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 («Directiva de protección de datos») presenta un marco legal horizontal para la protección de los derechos individuales de protección de datos. Por lo que se refiere al tratamiento de datos personales, la Directiva de protección de datos alude al derecho al respeto de la vida privada reconocido en el artículo 8 del CEPDH[5]. También se reconoce el derecho a recibir o comunicar informaciones, como parte de la libertad de expresión, garantizada en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[6]. Por otra parte, con arreglo al considerando 47, la persona de quien procede un mensaje de correo electrónico que contenga datos personales será considerada responsable del tratamiento de los datos personales, mientras que las personas que ofrezcan el servicio de correo electrónico serán normalmente consideradas responsables del tratamiento de los datos personales complementarios necesarios para el funcionamiento del servicio.

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (en adelante, Directiva sobre la privacidad y las comunicaciones electrónicas) concierne al tratamiento de datos personales en conexión con la prestación de servicios de comunicaciones electrónicas disponibles al público en la Comunidad. Las disposiciones de esta Directiva pormenorizan y complementan la Directiva de protección de datos. El artículo 5 de la Directiva sobre la privacidad y las comunicaciones electrónicas protege en particular la confidencialidad de las comunicaciones, con el texto siguiente:

---

[5] Considerando 10: *Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario.*

[6] Considerando 37: *Considerando que para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.*

«…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. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo…»

Por otra parte, el artículo 4 de la misma Directiva establece que *«El proveedor de un servicio público de telecomunicación deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de telecomunicación por lo que respecta a la seguridad de la red».*

También hay que mencionar la Directiva sobre comercio electrónico, en particular las disposiciones relativas a la responsabilidad de los proveedores de servicios Internet o correo electrónico con arreglo a las cuales los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisión. Esta obligación constituiría una violación de la libertad de información así como de la confidencialidad de la correspondencia (artículo 15 de la Directiva sobre comercio electrónico[7]).

III. ANÁLISIS DEL CONTENIDO DE CORREO ELECTRÓNICO

A la luz de esta base legal se plantea la cuestión de si el análisis de las comunicaciones en el que normalmente participan los ISPs o ESPs con objetivos diversos es compatible con el Derecho de la UE.

La mayoría de ISPs y ESPs analiza los correos electrónicos. Lo hacen de manera rutinaria con fines tan diversos como el filtrado de correo masivo no solicitado («buzonfia»), la detección de virus, la búsqueda y la corrección ortográfica, el reenvío de mensajes, la auto-respuesta, la señalización con banderas de mensajes urgentes, la conversión de correos electrónicos entrantes en mensajes de texto de móvil, el salvado automático, el almacenamiento en carpetas, o la conversión de URL en conexiones clickables.

Más adelante revisaremos el marco legal que regula la criba realizada con los siguientes fines: (A) a detección del virus, (B) filtrar buzonfia y (C) detectar un contenido concreto.

A) El cribado de correos electrónicos con fines de detección de virus

El control antivirus consiste en el proceso de comprobar ficheros para averiguar si contienen virus conocidos. En algunos casos, al control antivirus sigue la limpieza, que es el proceso de eliminar del fichero el virus detectado para que pueda utilizarse con seguridad. Por regla general, el control de virus se realiza cuando el correo electrónico llega por primera vez a los servidores de correo de los proveedores. La mayor parte de los proveedores incluyen el control antivirus entre los servicios que ofrecen con objeto de protegerse ellos mismos y de proteger a los usuarios. En la mayoría de los casos, los usuarios no pueden desconectar el control, que es automático y constituye parte del servicio.

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.

---

7 Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

Efectivamente, dado que la distribución de correos electrónicos afectados por virus puede cerrar el sistema de los proveedores de servicios de correo electrónico (además de dañar otros documentos y programas informáticos almacenados en la terminal del usuario final), y por ello perjudicar la transmisión de ulteriores comunicaciones de correo electrónico, el Grupo de trabajo 29 considera que la ejecución del cribado es una medida de seguridad dirigida a proteger el sistema del responsable del tratamiento de datos (proveedor de servicios de correo electrónico) que, como ya se ha subrayado, es una obligación vinculante para los proveedores de servicios de comunicaciones electrónicas, en aplicación del artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas.

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.

Además, el Grupo de trabajo 29 estima que cuando los proveedores de correo electrónico instalan filtros puede considerarse que están protegiendo la ejecución del contrato de servicio suscrito con sus clientes, que esperan recibir y enviar correos con un cierto grado de seguridad. En consecuencia, el tratamiento de datos al que proceden los proveedores cuando instalan sistemas de filtrado puede legitimarse asimismo con arreglo al artículo 7, letra b de la Directiva de protección de datos, que prevé el tratamiento de los mismos si *«es necesario para la ejecución de un contrato en el que el interesado sea parte»*.

Dado que, de acuerdo con lo anteriormente expuesto, el filtrado de virus se justificaría para preservar la seguridad de los servicios, de conformidad con el artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas y por ser necesario para la mera ejecución del contrato, de conformidad con el artículo 7 b de la Directiva de protección de datos, 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.

Debería faciliatarse asimismo información sobre el cribado (véase la sección específica, *infra*)

B) El cribado de correos electrónicos para filtrar buzonfia («*spam*»)[8]

Los ISPs y ESPs utilizan diversas técnicas para evitar que los correos electrónicos no deseados (no siempre de carácter comercial), es decir, la buzonfia, lleguen a sus destinatarios.

Una de ellos consiste en la utilización del llamado establecimiento de lista negra, mediante el que se incluyen en una lista negra de direcciones IP (protocolo de Internet) de determinados servidores así como rangos de IP asignados a ciertos ISPs[9]. Este documento no se ocupa con más detalle del establecimiento de lista negra.

El filtrado de buzonfia se ha convertido de hecho en una práctica necesaria. Si los servicios de correo electrónico no utilizaran el filtrado con este fin, aumentaría progresivamente el porcentaje de buzonfia que se recibe en los buzones de entrada y los sistemas serían probablemente muy lentos e ineficaces, malográndose así la utilidad del correo electrónico para sus usuarios. Esta situación obviamente no satisfaría a los consumidores y reduciría las posibilidades de proporcionar un servicio de correo electrónico fiable y digno de confianza.

Si bien la buzonfia no parece constituir en sí misma una amenaza para la seguridad de los servicios de los ESPs, sino más bien para el funcionamiento de la red en general y el servicio de correo electrónico en particular, puede sin embargo anular la capacidad de los ESPs para proporcionar el servicio de correo electrónico. El Grupo de trabajo 29 considera que el artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas, que exige a los proveedores de correo electrónico adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, se refiere a la seguridad de los servicios ESP y de la red en sí, pero también al funcionamiento general de los servicios de correo electrónico y de la red. La seguridad del ESP es un problema en la medida en que afecta al servicio que ofrece, por ello, el Grupo de trabajo 29 estima que el artículo 4 podría también aplicarse a esta situación. Dicho de otra forma, que las amenazas que hacen peligrar el funcionamiento general del correo electrónico y de los servicios de red pueden justificar que los ISPs y ESPs realicen filtrados con el fin de combatir la buzonfia. Si se tienen en cuenta los efectos que la buzonfia produce, incluso cuando el emisor distribuye sólo poca información al día, pero a un inmenso número de destinatarios, se refuerzan los argumentos en favor de la aplicación del artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas, porque incluso en estos casos, el envío de un número limitado de correos podría bloquear el tráfico de Internet y perjudicar gravemente la fiabilidad, seguridad y eficacia los servicios de correo electrónico en general. Además, por los mismos motivos, el Grupo de trabajo 29 considera asimismo que este filtrado estaría legitimado por el artículo 7, letra, b) de la Directiva de protección de datos, ya que el filtrado para combatir la buzonfia es necesario para que el proveedor de correo electrónico pueda ejecutar correctamente el contrato del que es parte el afectado por los datos, es decir, el destinatario.

---

8 El documento del OECD titulado «Anti Spam Regulations» (Normas sobre *Buzonfia*) elaborado por la «*TaskForce Spam*» (Grupo de trabajo sobre *Buzonfia*) en marzo de 2005 (DSTI/CP/ICCP/SPAM(2005)1 describe *buzonfia («spam»)* de la siguiente forma: «*El término* buzonfia *se emplea comúnmente en los medios de comunicación internacionales y en los comunicados políticos emitidos por diversos países, sin embargo no hay una definición acuñada del mismo. Aunque en términos generales se habla de los mismos fenómenos, cada país define* buzonfia *de la manera más adecuada a su entorno local. Para desarrollar una política antibuzonfia es esencial que el concepto de* buzonfia *se comprenda y se defina claramente, y la práctica de la* buzonfia (*el* «spamming»*) se distinga de la práctica legítima.»*

9 Utilizando esta técnica, el proveedor de correo electrónico no realiza filtrados, simplemente bloquea (es decir, rechaza) los correos procedentes de servidores o rangos de IP incluidos en la lista negra, sin cribar su contenido. Si bien esta práctica de incluir en la lista negra es en principio menos intrusiva que el filtrado de contenido, puede poner en cuestión de la libertad de palabra y de expresión así como del derecho a la libertad de enviar y recibir correspondencia, reconocido en el artículo 8 del CEPDH, interpretado a fondo por el Tribunal.

Por otro lado, el Grupo de trabajo 29 manifiesta su preocupación por el hecho de que el filtrado a veces da lugar a «falsos positivos», es decir, que mensajes legítimos «deseados» no se distribuyen por consideralos buzonfia. El Grupo de trabajo 29 estima que la acción de filtrar y retener correo supuestamente indeseado puede constituir no sólo una invasión de la libertad de expresión sino también, una infracción del artículo 10 del CEPDH y una injerencia en las comunicaciones privadas[10].

A la luz del anteriormente mencionado, sin perjuicio de la aplicación del artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas, y para preservar el principio de libertad de comunicación, reconocido en el artículo 10 del CEPDH así como la confidencialidad de las comunicaciones prevista en el artículo 5 de la Directiva sobre la privacidad y las comunicaciones electrónicas y recogida asimismo en el artículo 8 del CEPDH, el Grupo de trabajo 29 anima encarecidamente a los proveedores de correo electrónico a que tengan en cuenta las siguientes recomendaciones, cuyo objetivo principal es que los destinatarios de correos electrónicos puedan controlar las comunicaciones que se dirigen ante todo a ellos:

(a) el Grupo de trabajo 29 anima a utilizar la práctica que consiste en ofrecer a los abonados la posibilidad descartar el análisis de sus correos electrónicos a efectos de detección de buzonfia, la de comprobar los correos considerados buzonfia para determinar si lo son en realidad y la de decidir qué «tipo» de buzonfia debe eliminarse mediante filtrado. Además, el Grupo de trabajo 29 acoge asimismo con satisfacción la práctica de algunos ESPs que posibilitan a sus abonados que vuelvan a permitir el análisis de sus correos electrónicos con el objetivo de filtrar buzonfia;

(b) el Grupo de trabajo 29 es también favorable al desarrollo de sistemas de filtrado que los usuarios finales pueden instalar o configurar en su terminal, en servidores de terceros o en el servidor del proveedor de correo electrónico y que les permiten controlar lo que desean y no desean recibir, con la finalidad añadida de reducir los costes inherentes a la descarga del correo electrónico no solicitado, según recuerda el considerando 44 de la Directiva 2002/58. El Grupo de trabajo 29 saluda asimismo los trabajos de investigación de otras herramientas para combatir la buzonfia de forma menos intrusiva para la privacidad.

Por otra parte, el Grupo de trabajo 29 recuerda a los proveedores de servicios de correo electrónico que analizan correos con el fin de detectar buzonfia la obligación, prevista en el artículo 10 de la Directiva de protección de datos, de informar a los abonados de sus prácticas en relación con la buzonfia de manera clara e inequívoca, tal como se detalla en sección IV del presente dictamen. Los proveedores de correo electrónico deben garantizar también la confidencialidad de los correos filtrados, que no deberían ser utilizados para ningún otro fin.

[10] Tal y como reconoció el Tribunal en el asunto Schöneberger y Durmaz (1988).

C) El cribado de correos electrónicos con objeto de detectar un contenido concreto

El Grupo de trabajo 29 señala que algunos proveedores de correo electrónico se reservan el derecho de cribar e incluso retirar un contenido concreto[11], por ejemplo, material supuestamente ilegal o no deseado por el destinatario, usuario de este servicio. La técnica utilizada para este tipo de cribado es muy similar a la que se emplea para la detección virus y de buzonfia.

A diferencia del cribado para detectar virus, el que se realiza para detectar un contenido concreto, incluso si se considera supuesto material ilegal, no puede considerarse una medida técnica y de gestión necesaria para preservar la seguridad de los servicios de correo electrónico, como prevé el artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas. El proveedor de servicios de correo electrónico no se enfrenta a la amenaza de que las comunicaciones se vean perjudicadas e interrumpidas debido al contenido de los correos. Por ello, el cribado con el fin de detectar este material no está legitimado por la necesidad de preservar la seguridad del servicio. Al Grupo de trabajo 29 le preocupa asimismo que, utilizando este tipo de filtrado, los proveedores se conviertan en censores de la correspondencia privada por correo electrónico, bloqueando por ejemplo, comunicaciones cuyo contenido sea perfectamente legal, poniendo en cuestión la libertad de palabra, de expresión y de información. El Grupo de trabajo 29 querría subrayar que los proveedores de servicios no tienen ninguna obligación general de supervisar contenidos concretos o supuestamente perjudiciales, sino que, como se expone más adelante, este es un servicio que puede ofrecerse como valor añadido.

En consecuencia, el Grupo de trabajo 29 llega a la conclusión de que, de conformidad con el artículo 5, apartado 1 de la Directiva sobre la privacidad y las comunicaciones electrónicas, queda prohibido a los proveedores de correo electrónico el filtrado, almacenamiento u otros tipos de intervención en las comunicaciones y los datos de tráfico asociados a ellas con el fin de detectar un contenido concreto sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo, con arreglo a lo dispuesto en el artículo 15 de la Directiva sobre la privacidad y las comunicaciones electrónicas, aplicado por la legislación de los Estados miembros.

---

[11] Véase TOS (Términos del Servicio) de Yahoo!: *«Yahoo! no pre-selecciona el Contenido, sin embargo, Yahoo y sus designatarios o representantes tienen el derecho, pero no la obligación, a su plena discreción de preseleccionar, rechazar o remover cualquier Contenido que esté disponible por medio del Servicio. Sin limitación de lo anterior, Yahoo y sus designatarios o representantes tendrán el derecho de remover cualquier Contenido que viole los TOS. Usted conviene que debe evaluar y que acepta mediante su registro, todos aquellos riesgos asociados con el uso de cualquier Contenido, incluyendo su confianza en la veracidad, integridad o uso de dicho Contenido. En este respecto, usted acepta que no podrá depender de ningún Contenido creado por Yahoo o sometido a Yahoo, incluyendo, sin limitación, aquella información contenida en los Boletines de Mensajes, Yahoo! Clubs, y en todas las demás partes del Servicio. Usted acepta y conviene en que Yahoo puede conservar y/o revelar el Contenido si así le es requerido por ley o si de buena fe considera que dicha reserva o revelación es necesaria para: (a) cumplir con procesos legales; (b) hace valer los TOS; (c) responder a quejas de que algún Contenido viola los derechos de terceras personas; o (d) proteger los derechos, propiedad, o seguridad personal de Yahoo, sus usuarios y el público en general».*

IV. OBLIGACIÓN DE INFORMAR

Además de lo dispuesto en el artículo 5 del de la Directiva sobre la privacidad y las comunicaciones electrónicas, el tratamiento de datos personales con el fin de conocer el contenido o los datos de tráfico asociados a comunicaciones privadas debe cumplir también los diversos requisitos previstos en la Directiva de protección de datos.

Entre otras cosas, la Directiva de protección de datos impone la obligación de informar a los ciudadanos sobre el tratamiento de sus datos personales. En particular, el artículo 10 *«información del interesado»* obliga a los responsables del tratamiento a comunicar a la persona de quien se recaben los datos que le conciernen determinada información, incluida la identidad del responsable del tratamiento de los datos, así como los fines del tratamiento del que van a ser objeto los datos. Por otra parte, el artículo 6, apartado 1, letra a) de la Directiva de protección de datos establece que los datos deben ser tratados de manera leal y lícita, lo que refuerza la obligación de los responsables del tratamiento de observar una total transparencia cuando manejan datos personales.

Por lo que se refiere al filtrado con fines de detección de virus y buzonfia, el Grupo de trabajo 29 considera adecuado que la información de los abonados sea parte de las condiciones contractuales del servicio que ofrecen los ESPs.

Además de todo lo anterior, los ESPs deben atenerse también a lo dispuesto en el artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas, que obliga a los proveedores de un servicio de comunicaciones electrónicos disponibles para el público a informar a los abonados sobre un riesgo particular de violación de la seguridad de la red. Cuando el riesgo quede fuera del ámbito de las medidas que deberá tomar el proveedor del servicio, este deberá informar a sus usuarios y abonados de las posibles soluciones que existen para proteger la seguridad de sus comunicaciones.

V. OTROS SERVICIOS RELACIONADOS CON EL CORREO ELECTRÓNICO

El Grupo de trabajo 29 destaca el desarrollo de un nuevo tipo de productos y servicios informáticos como el llamado «did they read it?» («¿Lo han leído?») cuyo objetivo es detectar la apertura del correo electrónico.

Estos servicios permiten a sus abonados saber si un correo enviado (a) ha sido leído por el (los) destinatario(s), (b) cuándo se leyó, (c) cuantas veces se leyó (o por lo menos se abrió), (d) si se envió a otras personas posteriormente y (e) a qué servidor, con datos sobre su localización. Finalmente, permite también saber qué tipo de navegador de la red y sistema operativo utiliza el destinatario de los correos.

El tratamiento de datos se realiza de forma secreta, es decir, no se facilita información alguna sobre el mismo a los destinatarios del correo electrónico de los que se recuperan los datos. Además, los destinatarios de correo electrónico carecen de la posibilidad de aceptar o rechazar la recuperación de la información descrita anteriormente. En suma, a diferencia de sistemas clásicos de correo electrónico de confirmación, con estos nuevos productos el destinatario de los correos no puede aceptar o rechazar que la información de confirmación se transmita a los usuarios de programas informáticos para su tratamiento.

El Grupo de trabajo 29 expresa su más firme oposición a este tratamiento porque se registran y transmiten sin el consentimiento inequívoco del interesado datos personales sobre sus actividades. Este tratamiento, realizado en secreto, es contrario a los principios de lealtad y transparencia en la recogida de datos personales, establecidos en el artículo 10 de la Directiva de la protección de los datos.

Para llevar a cabo el tratamiento de datos que consiste en recuperar del destinatario de un correo la información que revela si aquel lo ha leído y cuándo y si lo ha enviado a terceros, es necesario el consentimiento inequívoco del interesado. No existe ningún otro fundamento que lo justifique legalmente. Por tanto, el tratamiento secreto de datos contraviene el principio de protección de datos que requiere un consentimiento otorgado inequívocamente, previsto en el artículo 7 de la Directiva de protección de datos.

VI. CONCLUSIÓN

Ante las dudas existentes relacionadas con la compatibilidad del filtrado de las comunicaciones de correo electrónico y la solicitud de asesoramiento de las partes interesadas, el Grupo de trabajo consideró que sería de utilidad publicar el presente dictamen.

El Grupo de trabajo 29 desea animar a los proveedores de servicios de correo electrónico a que lleven a cabo la prestación de sus servicios teniendo en cuenta las directrices y recomendaciones de este dictamen. Además, siguiendo su objetivo de promover tecnología que incorpore los requisitos necesarios de protección de datos y de respeto a la privacidad en la creación de infraestructura y de sistemas de información, incluidas las terminales, el Grupo de trabajo 29 desearía animar a los responsables de desarrollo de programas informáticos de correo electrónico a concebir y desarrollar sistemas que respeten la privacidad, de forma que el tratamiento de datos personales quede reducido al mínimo posible, limitándolo a lo que resulte imprescindible y proporcionado para lograr los objetivos del tratamiento.

Hecho en Bruselas, el 21 de febrero de 2006.

Por el Grupo de trabajo

El Presidente
Peter Schaar