5005/99/def.
WP 18

Grupo de trabajo sobre la protección de las personas por lo que respecta al tratamiento de datos personales

Recomendación 2/99

sobre

la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones

Adoptada el 3 de Mayo de 1999

Recomendación sobre

la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones

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

Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[1],

Considerando del artículo 29 y los apartados 1 y 3 del artículo 30 de la Directiva[2],

Considerando su reglamento interno, y en particular los artículos 12 y 14 de este último,

Ha adoptado la presente recomendación:

El objetivo de la recomendación consiste en recordar la aplicación de las medidas adoptadas a nivel europeo en cuanto a interceptación de las telecomunicaciones, de los principios de protección de los derechos y libertades fundamentales de las personas físicas, y, en particular, de su intimidad y del secreto de la correspondencia.

El ámbito de aplicación de la presente recomendación contempla las interceptaciones en sentido amplio, es decir, la interceptación del contenido de las telecomunicaciones, pero también los datos correspondientes a las telecomunicaciones, y, en particular, posibles medidas preparatorias (tales como el "monitoring" y el "datamining" de los datos de tráfico) que se pudieran prever con el fin de decidir la oportunidad de la interceptación del contenido de la telecomunicación[3]."

A. Alcance de las disposiciones adoptadas a nivel europeo en cuanto a interceptación de las comunicaciones

[1]Directiva 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 DO L 281 de 23.11.1995, p 31.

[2] Los tres miembros que representan respectivamente el Registertilsynet (Dinamarca), la Commission Nationale de l'Informatique et des Libertés (CNIL, Francia) y el Data Protection Register (Reino Unido), no participaron en el voto de esta recomendación, considerando que el asunto tratado no era competencia del grupo. Con todo dan su apoyo, de un modo general, en cuanto al fondo de la recomendación.

[3]Este carácter amplio del concepto de interceptación de las telecomunicaciones corresponde al ámbito de aplicación de la Resolución del Consejo del 17 de enero de 1995 relativa a la interceptación legal de las telecomunicaciones, ya citada (Capítulo A.1.), y al marco general de las disposiciones jurídicas aplicables sobre este tema (véase más adelante, Capítulo B.).

La recomendación se aplica así a la interceptación de las telecomunicaciones no públicas en Internet. Se presta especial atención a la problemática general del tratamiento de datos personales vinculada al desarrollo de la red Internet por el grupo de protección de las personas respecto al tratamiento de los datos personales, en el marco de trabajos realizados en paralelo por el "grupo de trabajo Internet" del grupo.

1. La Resolución del Consejo de 17 de enero de 1995 relativa a la interceptación legal de las telecomunicaciones[4] enumera las condiciones técnicas necesarias para la interceptación de las telecomunicaciones, sin abordar la cuestión de las condiciones en las que deberían tener lugar tales interceptaciones. El texto de la Resolución prevé una obligación por parte los operadores de redes o proveedores de servicios de proporcionar ya descifrados a los «servicios autorizados» los datos interceptados.

   Estos datos abarcan las llamadas telefónicas, móviles o no, los correos electrónicos, los mensajes fax y télex, los flujos de datos Internet, tanto por lo que se refiere al conocimiento del contenido de las telecomunicaciones como de los datos sobre las telecomunicaciones (en particular, los datos de tráfico, pero también todas las señales emitidas por la persona supervisada - apartado 1.4.4. de la Resolución).

   Los datos se refieren a la persona supervisada, a las personas que la llaman y a las personas a quienes ésta llama[5].

   La Resolución prevé también que la localización geográfica de los abonados de servicios móviles constituya un dato al cual deben tener acceso los servicios autorizados [6].

   Esta Resolución de 18 de enero de 1995 está actualmente siendo objeto de una revisión, uno de cuyos principales objetivos es adaptarla a las nuevas tecnologías de la comunicación. El texto en proyecto precisa en particular la aplicación de las medidas de interceptación a las telecomunicaciones por satélite[7].

2. Las reflexiones del grupo de trabajo se refieren al ámbito de aplicación de las medidas previstas por la Resolución del Consejo de 17 de enero de 1995. Una versión no publicada del documento antes citado y posterior a éste («declaración de intenciones» con fecha de 25 de octubre de 1995) prevé que los signatarios del texto puedan ponerse en contacto, por lo que se refiere a las especificaciones en cuanto a interceptación de las telecomunicaciones, con el director del «Federal Bureau of Investigation» de los Estados Unidos. El texto prevé por otro lado que, con el consentimiento de los «participantes», otros Estados puedan participar en el intercambio de información, en la revisión y en la actualización de las especificaciones.

   El grupo observa, por una parte, que el estatuto jurídico de este texto - en particular su firma efectiva por los países implicados - no queda claro y que no constituye, en el sentido de la jurisprudencia citada del Tribunal Europeo de Derechos Humanos , una medida accesible al ciudadano al no ser objeto de publicación alguna. Por otra parte, este texto confirma la voluntad de desarrollar medidas técnicas de interceptación de las

---

[4]DO C329 de 14.11.1996.

[5]Artículo 1.4 del Anexo de la Resolución del Consejo de 17 de enero de 1995.

[6]Artículo 1.5, ibid.

[7]Documento 10951/1/98, Enfopol 98 Rev 1 (http://www.heise.de/tp/deutsch/special/enfo/6332/1.htm). Parece que una versión aún más reciente ha recibido el acuerdo del grupo de trabajo sobre cooperación policial del Consejo y que se ha transmitido al Parlamento Europeo para que éste pueda adoptarlo o modificarlo. Se prevé al parecer que el Consejo adopte la nueva Resolución los días 27-28 de mayo de 1999 (véase "Datenschutz-Berater", 15.02.99, p 5, que hace referencia a una versión no pública de 20.01.99). La comisión jurídica del Parlamento europeo recomendó a la comisión sobre libertades públicas (coordinador) rechazar el proyecto de revisión de la recomendación del Consejo tal como se propone en ENFOPOL 98, entre otras cosas por razones de protección de la intimidad y por la entrada en vigor inminente del Tratado de Amsterdam (véase informe Florio). La comisión de libertades públicas no siguió este dictamen y propondrá al Pleno que apruebe ENFOPOL 98 sobre la base del informe Schmid. El Parlamento Europeo debería tomar una decisión a principios de mayo.

telecomunicaciones en concertación con Estados no sujetos a las exigencias del Convenio Europeo de Derechos Humanos y de las Directivas 95/46/CE y 97/66/CE.

3. El grupo constata que el texto de la Resolución del Consejo pretende resolver cuestiones técnicas relativas a las modalidades de interceptación de las comunicaciones, sin poner en causa las disposiciones nacionales que regulan las escuchas desde el punto de vista jurídico. Resulta, sin embargo, que algunas medidas previstas por la Resolución y destinadas a ampliar las posibilidades de interceptación de las comunicaciones están en contradicción con las disposiciones nacionales, más protectoras, de ciertos países de la Unión Europea (en particular: apartado 1.4, comunicación de los datos correspondientes a las llamadas, incluidas las llamadas de los usuarios móviles, sin tomar en consideración los servicios anónimos y pagados por adelantado actualmente disponibles; apartado 1.5, localización geográfica de los usuarios móviles; apartado 5.1, prohibición a los operadores de revelar a posteriori las interceptaciones realizadas).

4. Si bien la Resolución del Consejo se inscribe en un objetivo «de protección de los intereses nacionales, de seguridad nacional e investigación de crímenes graves», el grupo desea llamar la atención sobre los riesgos de deriva por lo que respecta a los objetivos de las escuchas, riesgos que se verían aumentados por una extensión a un número creciente de países - exteriores algunos a la Unión Europea - de las técnicas de interceptación y descifrado de las telecomunicaciones.

   Una resolución oficial del Parlamento Europeo de 16 de septiembre de 1998 sobre las relaciones transatlánticas[8], «considera que la importancia creciente de la red Internet, de las telecomunicaciones a escala mundial, en general, pero sobre todo del sistema ECHELON, así como los riesgos de su utilización abusiva, exigen la adopción de medidas de protección de las informaciones económicas y de un cifrado eficaz.»

   Estas consideraciones ponen de relieve los riesgos vinculados a una interceptación de las telecomunicaciones que sobrepase el marco estricto de las cuestiones de seguridad nacional – e incluso el marco del "tercer pilar" de la Unión Europea. Plantean asimismo la cuestión de su legitimidad, en particular, a la luz de las obligaciones que se derivan de los textos de derecho comunitario en cuanto a protección de los derechos y libertades fundamentales de las personas físicas, y, en particular, de su intimidad.

5. El grupo destaca finalmente que la entrada en vigor del Tratado de Amsterdam implicará un cambio de base jurídica a nivel europeo por lo que se refiere a las medidas de interceptación de las telecomunicaciones. La competencia actual del Consejo para elaborar el texto de la Resolución, basada en el apartado 9 del artículo K.1 y en el apartado 2 del artículo K.3 del Tratado relativos a la cooperación policial y judicial, se convertirá en una competencia de iniciativa de la Comisión Europea sobre la base del apartado 2 del nuevo artículo K.6.

B. Cuadro jurídico general

[8]Sesión plenaria, parte II, B4-0803, 0805, 0806 y 0809/98.

6. El grupo recuerda que cada interceptación de telecomunicación, entendida como el conocimiento de una tercera parte del contenido y/o de los datos asociados a las telecomunicaciones privadas entre dos o varios corresponsales, en particular los datos de tráfico vinculados a la utilización de los servicios de telecomunicación, constituye una violación del derecho a la intimidad de los individuos y del secreto de la correspondencia. Sólo puede por lo tanto admitirse una interceptación si responde a tres requisitos fundamentales, de acuerdo con el apartado 2 del artículo 8 del Convenio Europeo de Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950[9], y de la interpretación reservada a esta disposición por el Tribunal Europeo de Derechos Humanos: un fundamento jurídico, la necesidad de tal medida en una sociedad democrática y la conformidad con uno de los objetivos legítimos enumerados en el Convenio[10].

   El fundamento jurídico deberá definir precisamente los límites y modalidades de su ejercicio, por medio de normas claras y detalladas, necesarias sobre todo debido al perfeccionamiento continuo de los medios técnicos utilizables[11]. Este texto legal debe ser accesible al público para que el ciudadano pueda prever las consecuencias de su comportamiento[12].

   En este contexto jurídico debe prohibirse la vigilancia exploratoria o general de las telecomunicaciones a gran escala[13].

7. En la Unión Europea, la Directiva 95/46/CE[14] consagra el principio de la protección del derecho a la intimidad inscrito en los sistemas jurídicos de Estados miembros. Esta

[9]Conviene destacar que las garantías fundamentales reconocidas por el Consejo de Europa en cuanto a interceptación de las comunicaciones generan obligaciones a cargo de los Estados independientemente de las distinciones que existan en la Unión Europea en función del carácter comunitario o intergubernamental de los ámbitos abordados.

[10]El Convenio n° 108 del Consejo de Europa prevé también que sólo se tolerará una medida de injerencia cuando constituya una medida necesaria en una sociedad democrática para la protección de los intereses nacionales enumerados en el apartado 2 de su artículo 9 (se tendrá en cuenta que los intereses nacionales enumerados en el Convenio 108 y en el Convenio de Protección de Derechos Humanos no son exactamente iguales), y cuando esté estrictamente definida respecto a esta finalidad.

[11]Véanse a este respecto, más adelante, las obligaciones previstas por el artículo 4 de la recomendación n° 4 del Consejo de Europa sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, respecto, en particular, a los servicios telefónicos, de 7 de febrero de 1995

[12]Sentencias Huvig y Kruslin contra Francia de 25 de abril de 1990, serie A n° 176 A y B, p 15 y s.

[13]Véanse, en particular, las sentencias Klass, de 6 de septiembre de 1978, serie A n° 28, p 23 y s, y Malone, de 2 de agosto de 1984, serie A n° 82, p 30 y s.

La sentencia Klass, así como la sentencia Leander de 25 de febrero de 1987, hacen hincapié en la necesidad de "garantías suficientes contra los abusos, ya que un sistema de vigilancia secreta destinado a proteger la seguridad nacional crea el riesgo de minar, o incluso de destruir, la democracia pretendiendo defenderla" (Sentencia Leander, serie A n° 116, p 14 y s).

El Tribunal observa en la sentencia Klass (apartados 50 y s) que la valoración de la existencia de garantías adecuadas y suficientes contra los abusos depende de todas las circunstancias de la causa. Considera en la sentencia en cuestión que las medidas de vigilancia previstas por la legislación alemana no autorizan la vigilancia exploratoria o general y no infringen el artículo 8 del Convenio europeo de protección de los derechos humanos. Las garantías previstas por la ley alemana son las siguientes: sólo pueden efectuarse medidas de vigilancia cuando ciertos indicios permitan sospechar que alguien proyecta realizar, realiza o ha realizado infracciones graves; sólo pueden prescribirse si el esclarecimiento de los hechos por otros medios está llamado al fracaso o presenta considerables obstáculos; incluso en ese caso la vigilancia sólo podrá referirse a la persona del sospechoso o a las personas presuntamente en contacto con éste.

Directiva precisa los principios contenidos en el Convenio Europeo de Protección de los Derechos Humanos de 4 de noviembre de 1950 y en el Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales. La Directiva 97/66/CE[15] concreta las disposiciones de esta Directiva y precisa la obligación de los Estados miembros de proteger el secreto de las comunicaciones por medio de normativas nacionales que garanticen la confidencialidad de las comunicaciones efectuadas a través de redes públicas de telecomunicaciones o de servicios de telecomunicaciones accesibles al público.

Según el apartado 1 del artículo 13 de la Directiva 95/46/CE, un Estado miembro puede adoptar medidas legislativas destinadas a limitar el alcance de determinadas obligaciones (por ejemplo acerca de la recogida de datos) y determinados derechos (por ejemplo el derecho a ser informado en caso de recogida de datos) previstos por la Directiva[16]. Estas excepciones se enumeran taxativamente: la limitación debe constituir una medida necesaria para proteger los intereses públicos enunciados de manera exhaustiva en las letras a) a g) de este artículo, tales como la seguridad del Estado, la defensa, la seguridad pública o la prevención, investigación, detección y represión de infracciones penales.

En el apartado 1 del artículo 14, la Directiva 97/66/CE precisa también que los Estados miembros sólo pueden restringir la obligación de confidencialidad de las comunicaciones a través de redes públicas cuando tal medida constituya una medida necesaria para salvaguardar la seguridad del Estado, la defensa, la seguridad pública, la prevención, investigación, detección y represión de infracciones penales.

C. Obligaciones de los operadores y de los proveedores de servicios de telecomunicación

8. Hay que hacer hincapié en el hecho de que las obligaciones de seguridad y confidencialidad de los datos a las que se somete a los operadores de telecomunicaciones, a los proveedores de servicios y a los Estados miembros, respectivamente sobre la base de los apartados 1 y 2 del artículo 17 de la Directiva 95/46 y sobre la base de los artículos 4, 5 y 6 de la Directiva 97/66/CE, constituyen el principio y no la excepción.

   El grupo recuerda que estas obligaciones se imponen también de manera general a los operadores con arreglo al artículo 7 del Convenio del Consejo de Europa n° 108 para la protección de las personas respecto al tratamiento de los datos personales, de 28 de enero de 1981, y del artículo 4 de la Recomendación n°4 del Consejo de Europa sobre protección

[14]Se deberá tener en cuenta que el artículo 3 de la Directiva 95/46/CE excluye de su ámbito de aplicación los tratamientos de datos personales en el ejercicio de actividades no incluidas en el ámbito de aplicación del Derecho comunitario, y los tratamientos cuyo objeto sea la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado relativas a ámbitos de derecho penal. La mayoría de los Estados miembros que transponen esta Directiva no han establecido sin embargo hasta ahora, en sus leyes nacionales, una distinción según la cual esta ley no se aplicaría a las materias no cubiertas por el Derecho comunitario.

Hay que añadir que, a partir del momento en que se aplica en el marco de la Directiva un tratamiento de datos (por ejemplo, la lista de las llamadas registradas para facturación por un operador), pero que en una segunda fase es objeto de un tratamiento consistente en una interceptación de estos datos, deben aplicarse las disposiciones de Derecho comunitario. La Directiva 95/46/CE prevé a este respecto una serie de garantías que deben respetarse en el marco de estas interceptaciones, y que se exponen a continuación.

[15]Directiva de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, DO L 24 de 30 de enero de 1998, p.1.

[16]Previstos en el apartado 1 del artículo 6 - principios relativos a la calidad de los datos, en el artículo 10, en el apartado 1 del artículo 11 - información a la persona en cuestión, y en los artículos 12 - derecho de acceso y 21 - publicidad de los tratamientos.

de datos personales en el ámbito de los servicios de telecomunicaciones, de 7 de febrero de 1995[17], que tiene en cuenta, en particular, a los servicios telefónicos.

9. Estas obligaciones implican, por una parte, que los operadores de telecomunicación y los proveedores de servicios sólo pueden tratar los datos relativos al tráfico y a la facturación de las telecomunicaciones cumpliendo determinadas condiciones: a partir del principio de que los datos referentes al tráfico relativos a abonados y usuarios deben borrarse o tornarse anónimos en cuanto termina la comunicación, se deduce que las finalidades para las cuales pueden tratarse los datos, la duración de su posible conservación, así como el acceso a dichos datos están estrictamente limitados[18].

10. Por otra parte, los operadores de telecomunicaciones y los proveedores de servicios de telecomunicaciones deben adoptar las medidas necesarias con el fin de hacer técnicamente difíciles o imposibles, según el estado actual de la técnica, la interceptación de las telecomunicaciones por instancias no autorizadas por la ley.

    El grupo destaca a este respecto que la aplicación de medios eficaces de interceptación de las comunicaciones con fines legítimos, utilizando precisamente las técnicas más avanzadas, no debe tener por consecuencia reducir el nivel general de confidencialidad de las comunicaciones y de protección de la intimidad de las personas.

    Estas obligaciones toman un sentido particular cuando las telecomunicaciones entre personas situadas en el territorio de los Estados miembros transiten o puedan transitar por el exterior del territorio europeo, en particular en la utilización de satélites o de Internet.

11. En la medida en que sea de aplicación la Directiva 95/46/CE, el hecho de hacer accesibles tales telecomunicaciones en el exterior de la Unión Europea podría por otra parte constituir una violación de su artículo 25, dado que los organismos extranjeros que interceptan los datos no necesariamente pueden pretender garantizar un nivel adecuado de protección.

---

[17] "4.1. No deberían comunicarse los datos personales recogidos y tratados por los concesionarios de red o los proveedores de servicios, a menos que el abonado interesado haya dado por escrito su consentimiento claro y explícito y que la información comunicada no permita identificar a los abonados llamados.

El abonado puede retirar su consentimiento en cualquier momento pero no con efecto retroactivo.

4.2. Los datos personales recogidos y tratados por los concesionarios de red o los proveedores de servicios pueden comunicarse a las autoridades públicas si esta comunicación está prevista por la ley y constituye una medida necesaria, en una sociedad democrática:

a. para la protección de la seguridad del Estado, la seguridad pública, los intereses monetarios del Estado o la represión de las infracciones penales;
b. para la protección de la persona en cuestión y los derechos y libertades de otros.

4.3. En caso de comunicación de datos personales a autoridades públicas, el derecho interno debería regular:

a. el ejercicio de los derechos de acceso y rectificación por parte de la persona interesada;
b. las condiciones en las cuales las autoridades públicas competentes tendrán derecho a negarse a dar información a la persona interesada o a diferirla;
c. la conservación o destrucción de estos datos."

[18] Véanse en particular las obligaciones del artículo 6 de la Directiva 97/66/CE.
Estas obligaciones plantean algunos interrogantes en cuanto a las prácticas que se desarrollan actualmente entre los prestadores de servicios de telecomunicación y que consisten en un examen general y previo de los datos de tráfico de los suscriptores, con objeto de identificar el comportamiento sospechoso de algunos abonados – y eventualmente permitir la interceptación específica del contenido de ciertas telecomunicaciones.

D. Respeto de las libertades fundamentales por parte de las autoridades públicas en el ámbito de las interceptaciones

12. Es importante que el derecho nacional precise de manera rigurosa y tomando en cuenta todas las disposiciones previamente mencionadas:

- ✓ las autoridades habilitadas para permitir la interceptación legal de las telecomunicaciones, los servicios autorizados para proceder a las interceptaciones y el fundamento jurídico de su intervención,

- ✓ las finalidades según las cuales pueden tener lugar tales interceptaciones, que permitan apreciar su proporcionalidad respecto a los intereses nacionales en juego,

- ✓ la prohibición de cualquier vigilancia exploratoria o general de las telecomunicaciones a gran escala,

- ✓ las circunstancias y condiciones precisas (por ejemplo elementos de hecho que justifiquen la medida, duración de la medida) a las cuales están sometidas las interceptaciones, en cumplimiento del principio de especificidad al que se supedita toda injerencia en la intimidad de otros[19],

- ✓ el respeto de este principio de especificidad, corolario de la prohibición de cualquier vigilancia exploratoria o general, que implica, por lo que se refiere concretamente a los datos de tráfico, que las autoridades públicas no pueden tener acceso a estos datos sino con carácter particular, y no de manera general y proactiva.

- ✓ las medidas de seguridad por lo que se refiere al tratamiento y el almacenamiento de los datos, y la duración de su conservación,

- ✓ por lo que se refiere a las personas implicadas de manera indirecta o aleatoria[20] en las escuchas, las garantías particulares referentes al tratamiento de los datos personales: en particular, los criterios que justifican la conservación de los datos, y las condiciones de la comunicación de estos datos a terceros,

- ✓ la información a la persona supervisada, lo antes posible[21],

---

[19] Véase más arriba, nota 13.

[20] Los datos que aquí se contemplan se refieren a personas que no son objeto de medidas de vigilancia, pero cuyo corresponsal sí es objeto de tales medidas; por ejemplo: número de teléfono marcado por la persona supervisada y correspondiente a uno de los progenitores de este último; localización geográfica de personas en contacto por teléfono móvil con la persona objeto de escucha.

[21] La persona bajo vigilancia debería en efecto poder ser informada a partir del momento en que la información no perjudica o ya no perjudica más a la investigación.

- ✓ los tipos de recurso que puede ejercer la persona supervisada[22],

- ✓ las modalidades de vigilancia de estos servicios por una autoridad de control independiente[23],

- ✓ la publicidad - por ejemplo en forma de informes estadísticos regulares - de la política de interceptación de las telecomunicaciones efectivamente practicada[24],

- ✓ las condiciones precisas en las que pueden comunicarse los datos a terceros en el marco de acuerdos bilaterales o multilaterales.

Hecho en Bruselas, a 3 de Mayo de 1999

En nombre del grupo

Peter HUSTINX

Presidente

[22]La sentencia Leander antes citada recuerda que el órgano ante el cual puede presentarse el recurso "no es necesario que sea una institución judicial *strictu sensu*, pero sí que sus poderes y las garantías de procedimiento de que dispone permitan apreciar la eficacia del recurso". Este recurso "debe ser un recurso lo más efectivo posible, habida cuenta de las limitaciones inherentes a todo sistema de vigilancia secreta destinado a proteger la seguridad nacional" (83 y 84).

[23]La sentencia Leander contempla el control democrático de las interceptaciones cuando precisa que "incumbe al Parlamento y a instituciones independientes [del Gobierno] velar por el buen funcionamiento del sistema" (64).

[24]Esta exigencia de publicidad, así como, en particular, la necesidad de un control de las interceptaciones por una autoridad independiente, se mencionan en el "Common position on public accountability in relation to interceptation of private communications" adoptada en Hong Kong el 15 de abril de 1998 por el grupo internacional de trabajo sobre protección de datos en el sector de las telecomunicaciones.