01037/12/ES
WP 196

Dictamen 05/2012 sobre la computación en nube

Adoptado el 1 de julio de 2012

Resumen

En el presente dictamen, el Grupo de Trabajo del Artículo 29 analiza todas las cuestiones pertinentes en materia de proveedores de servicios de computación en nube que operan en el Espacio Económico Europeo (EEE) y sus clientes, especificando todos los principios aplicables de la Directiva europea sobre protección de datos (95/46/CE) y de la Directiva sobre privacidad 2002/58/CE (modificada por la Directiva 2009/136/CE), según proceda.

A pesar de las claras ventajas de la computación en nube, tanto en términos económicos como sociales, el presente dictamen explica de qué manera el despliegue a gran escala de los servicios de computación en nube puede provocar diversos riesgos para la protección de datos, principalmente la falta de control sobre los datos personales, así como la insuficiente información en relación a cómo, dónde y por quién son los datos tratados o subtratados. Los organismos públicos y las empresas privadas deben evaluar estos riesgos cuidadosamente al contratar los servicios de un proveedor de servicios de computación en nube. El presente dictamen examina cuestiones relacionadas con la puesta en común de recursos con otras partes, la falta de transparencia de una cadena de externalización compuesta por múltiples encargados del tratamiento y subcontratistas, la inexistencia de un marco común general de portabilidad de datos, y la incertidumbre con respecto a la admisibilidad de la transferencia de datos personales a los proveedores establecidos fuera del EEE. Del mismo modo, el dictamen aborda, como cuestión preocupante, la falta de transparencia en cuanto a la información que un responsable del tratamiento puede proporcionar a los interesados sobre la manera en que se tratan sus datos personales. Los interesados deben[1] ser informados de quién trata sus datos y para qué fines, a fin de poder ejercer los derechos que tienen a este respecto.

Una de las principales conclusiones del presente dictamen es que las empresas y las administraciones que deseen utilizar la computación en nube deben efectuar, como un primer paso, un análisis de riesgos completo y riguroso. Los proveedores en el EEE deben proporcionar al cliente toda la información necesaria para evaluar adecuadamente los pros y los contras de la adopción de tal servicio. La seguridad, transparencia y seguridad jurídica para los clientes deberán ser los principales impulsores de la oferta de servicios de computación en nube.

Por lo que respecta a las recomendaciones contenidas en el presente dictamen, se subrayan las responsabilidades de un cliente de servicios de computación en nube (como responsable del tratamiento y se recomienda, por tanto, que el cliente seleccione un proveedor de servicios de computación en nube que garantice el cumplimiento de la legislación de la UE sobre protección de datos. El dictamen aborda las salvaguardias contractuales apropiadas estableciendo la condición de que todo contrato entre el cliente y el proveedor deberá ofrecer garantías suficientes en términos de medidas técnicas y de organización. También es importante la recomendación de que el cliente de servicios computación en nube deberá verificar si el proveedor de tales servicios puede garantizar la legalidad de las transferencias internacionales de datos.

[1] Las palabras clave «DEBERÁN», «NO DEBERÁN», «DEBEN», «NO DEBEN», «NECESARIO», «DEBERÍAN», «NO DEBERÍAN», «RECOMENDADO», «PODRÁN» y «OPCIONAL» utilizadas en el presente documento deberán interpretarse según lo descrito en la petición de observaciones RFC 2119. El documento está disponible en: http://www.ietf.org/rfc/rfc2119.txt. No obstante, en aras de la facilidad de lectura, estas palabras no aparecen en mayúsculas en el presente documento.

Como cualquier proceso evolutivo, el avance de la computación en nube como paradigma tecnológico mundial representa un desafío. El presente dictamen, en su estado actual, puede considerarse un paso importante para definir las tareas que debe asumir en este sentido los responsables de la protección de datos en los próximos años.

Índice

Resumen 2
1. Introducción 5
2. Riesgos para la protección de los datos de la computación en nube 6
3. Marco jurídico 8
3.1 Marco de protección de datos 8
3.2 Legislación aplicable 8
3.3 Funciones y responsabilidades de las diversas partes 9
3.3.1 Clientes y proveedores de servicios de computación en nube 9
3.3.2 Subcontratistas 11
3.4 Requisitos de protección de datos en la relación cliente-proveedor 12
3.4.1 Cumplimiento de los principios básicos 12
3.4.1.1 Transparencia 12
3.4.1.2 Especificación y limitación de la finalidad 13
3.4.2 Garantías contractuales de las relaciones entre el responsable y el encargado del tratamiento 14
3.4.3 Medidas técnicas y de organización para garantizar la protección de los datos y su seguridad 16
3.4.3.1 Disponibilidad 17
3.4.3.2 Integridad 17
3.4.3.3 Confidencialidad 17
3.4.3.4 Transparencia 18
3.4.3.5 Aislamiento (limitación de la finalidad) 18
3.4.3.5 Posibilidad de intervención 18
3.4.3.6 Portabilidad 18
3.4.4.7 Responsabilidad 19
3.5 Transferencias internacionales 19
3.5.1 Puerto seguro y países adecuados 20
3.5.2 Excepciones 21
3.5.3 Cláusulas contractuales tipo 21
3.5.4 Normas corporativas vinculantes (NCV): hacia un enfoque global 22
4. Conclusiones y recomendaciones 22
4.1 Directrices para los clientes y proveedores de servicios de computación en nube 23
4.2 Certificaciones de protección de datos de terceros 25
4.3 Recomendaciones: evolución futura 26
ANEXO 28
a) Modelos de implantación 28
b) Modelos de prestación de servicios 29

1. Introducción

Para algunos, la computación en nube es una de las mayores revoluciones tecnológicas de los últimos tiempos. Para otros, es solamente la evolución natural de un conjunto de tecnologías destinadas a lograr el tan esperado sueño del desarrollo de programas informáticos. En cualquier caso, un gran número de partes interesadas han destacado la computación en nube en el marco del desarrollo de sus estrategias tecnológicas.

La computación en nube consta de una serie de tecnologías y modelos de servicio que se centran en el uso de Internet y la prestación de aplicaciones informáticas, capacidad de tratamiento, espacio de memoria y almacenamiento. La computación en nube puede generar importantes beneficios económicos, ya que los recursos a la carta pueden configurarse, ampliarse y ser accesibles fácilmente en Internet. Junto a las ventajas económicas, la computación en nube también puede aportar beneficios de seguridad; las empresas, especialmente las pequeñas y medianas, pueden adquirir, por un coste marginal, tecnologías de alto nivel, que de lo contrario estarían fuera de su presupuesto.

Existe una amplia gama de servicios ofrecidos por los proveedores de servicios de computación en nube (en lo sucesivo, «proveedores») que van desde sistemas de tratamiento virtual (que sustituyen o trabajan junto con servidores convencionales bajo el control directo del responsable del tratamiento) hasta servicios de apoyo al desarrollo de aplicaciones avanzadas y alojamiento avanzado, o hasta programas informáticos basados en la web que pueden sustituir a las aplicaciones instaladas convencionalmente en los ordenadores personales de los usuarios finales. Esto incluye aplicaciones de tratamiento de textos, agendas y calendarios, sistemas de archivo para el almacenamiento en línea de documentos y soluciones de correo electrónico externalizadas. Algunas de las definiciones más comúnmente utilizadas para todos estos tipos de servicios figuran en el anexo al presente dictamen.

En el presente dictamen, el Grupo de Trabajo del Artículo 29 (en lo sucesivo, GT 29) analiza la legislación aplicable y las obligaciones de los responsables del tratamiento en el Espacio Económico Europeo (en lo sucesivo, EEE) y de los proveedores de servicios de computación en nube con clientes en el EEE. El dictamen se centra en la situación de una relación entre el responsable y el encargado, considerándose al cliente responsable y al proveedor, encargado. En los casos en que el proveedor actúa también como responsable del tratamiento, este debe cumplir requisitos adicionales. Como consecuencia de ello, una condición previa para los acuerdos de computación en nube es que el responsable del tratamiento realice una evaluación de riesgos adecuada, incluyendo las ubicaciones de los servidores donde se tratan los datos y la consideración de los riesgos y ventajas desde la perspectiva de la protección de datos, con arreglo a los criterios indicados en los apartados que figuran a continuación.

El dictamen especifica los principios aplicables a los responsables y los encargados del tratamiento derivados de la Directiva europea sobre protección de datos (95/46/CE), como la especificación de la finalidad y la limitación, la supresión de datos y las medidas técnicas y de organización. El dictamen establece directrices sobre los requisitos de seguridad, como salvaguardia estructural y de procedimiento. Se hace especial hincapié en las disposiciones contractuales que deben regular la relación entre los responsables y los encargados del tratamiento en este sentido. Los objetivos clásicos de seguridad de los datos son la disponibilidad, la integridad y la confidencialidad. Sin embargo, la protección de los datos no se limita a la seguridad y, por tanto, estos objetivos se complementan con los objetivos específicos de transparencia, aislamiento, posibilidad de intervención y portabilidad para

justificar el derecho del individuo a la protección de datos, con arreglo a lo previsto en el artículo 8 de la Carta de los Derechos Fundamentales de la UE.

Por lo que se refiere a las transferencias de datos personales fuera del EEE, se analizan instrumentos tales como las cláusulas contractuales estándar adoptadas por la Comisión Europea, la comprobación del nivel adecuado de protección de los datos y posibles futuras normas corporativas vinculantes (NCV) relativas al encargado del tratamiento, así como los riesgos para la protección de los datos derivados de las solicitudes internacionales de intervención legal.

El presente dictamen concluye con recomendaciones para los clientes de servicios de computación en nube que actúen como responsables del tratamiento, los proveedores de servicios de computación en nube que actúen como encargados, y para la Comisión Europea por lo que se refiere a futuros cambios del marco europeo de protección de datos.

En abril de 2012, el Grupo de trabajo internacional de Berlín sobre protección de datos en las telecomunicaciones adoptó el *Memorándum Sopot*[2]. Este memorándum examina cuestiones de intimidad y protección de datos en la computación en nube y pone de relieve que esta no debe conducir a una disminución de los niveles de protección de datos en comparación con el tratamiento convencional.

2. Riesgos para la protección de los datos de la computación en nube

Puesto que el presente dictamen se centra en las operaciones de tratamiento de datos personales que utilizan servicios de computación en nube, sólo se tienen en cuenta los riesgos específicos relacionados con este contexto[3]. La mayoría de estos riesgos se dividen en dos grandes categorías, a saber, la falta de control de los datos y la insuficiente información sobre la propia operación de tratamiento (falta de transparencia). Los riesgos específicos de la computación en nube considerados en el presente dictamen incluyen los siguientes:

Falta de control

Al introducir datos personales en los sistemas gestionados por un proveedor, los clientes de servicios de computación en nube (en lo sucesivo, «clientes») pueden no seguir teniendo el control exclusivo de estos datos y no pueden aplicar las medidas técnicas y de organización necesarias para garantizar la disponibilidad, integridad, confidencialidad, transparencia, aislamiento, posibilidad de intervención y portabilidad de los datos[4]. Esta falta de control puede manifestarse de la siguiente manera:

- Falta de disponibilidad debido a la falta de interoperatividad (dependencia respecto del proveedor): si el proveedor se basa en tecnología patentada, puede resultar difícil para un cliente mover los datos y documentos entre diferentes sistemas en la nube (portabilidad de los datos) o intercambiar información con entidades que utilicen

2 http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

3 Además de los riesgos asociados al tratamiento de datos personales «en la nube» mencionados explícitamente en el presente dictamen, también deben tenerse en cuenta todos los riesgos relacionados con la subcontratación del tratamiento de datos personales.

4 En Alemania se ha introducido el concepto más amplio de «imposibilidad de establecer vínculos». Véase la nota a pie de página 24.

servicios de computación en nube gestionados por distintos proveedores (interoperatividad).

- Falta de integridad causada por la puesta en común de los recursos: una nube se compone de sistemas e infraestructuras comunes. Los proveedores tratan datos personales procedentes de una amplia gama de interesados y organizaciones, y es posible que surjan conflictos de intereses u objetivos diferentes.
- Falta de confidencialidad por lo que respecta a las solicitudes de intervención legal realizadas directamente a un proveedor: los datos personales tratados en la nube pueden ser objeto de solicitudes de intervención legal por parte de las autoridades policiales o judiciales de los Estados miembros de la UE y de terceros países. Existe el riesgo de revelación de datos personales a servicios incluso extranjeros sin una base jurídica de la UE válida y, por tanto, se daría una violación de la legislación de la UE sobre protección de datos.
- Falta de posibilidad de intervención debido a la complejidad y la dinámica de la cadena de subcontratación: el servicio de computación en nube ofrecido por un proveedor puede realizarse combinando servicios de varios proveedores distintos, que pueden añadirse o suprimirse dinámicamente a lo largo de la duración del contrato del cliente.
- Falta de posibilidad de intervención (derechos de los interesados): un proveedor no podrá aportar las medidas e instrumentos necesarios para ayudar al responsable del tratamiento a gestionar los datos en términos de, por ejemplo, acceso, supresión o corrección.
- Falta de aislamiento: un proveedor podrá ejercer su control físico sobre los datos de distintos clientes para vincular los datos personales. Si se proporciona a los administradores derechos de acceso suficientemente privilegiados (funciones de alto riesgo), podrían vincular información de distintos clientes.

Falta de información sobre el tratamiento (transparencia)

La falta de información sobre las operaciones de tratamiento de un servicio de computación en nube plantea un riesgo para los responsables del tratamiento y para los interesados, que pueden no ser conscientes de las amenazas y riesgos potenciales y por tanto no podrán adoptar las medidas que consideren apropiadas.

Algunas posibles amenazas pueden derivarse de que el responsable del tratamiento no sepa que:

- Se realiza un tratamiento en cadena con múltiples encargados del tratamiento y subcontratistas.
- Los datos personales se tratan en diferentes zonas geográficas del EEE. Ello incide directamente en la legislación de protección de datos aplicable a los litigios que puedan surgir entre usuario y proveedor.
- Se transmiten datos personales a terceros países no pertenecientes al EEE. Los terceros países pueden no proporcionar un nivel adecuado de protección de datos y las transferencias pueden no contar con las medidas de protección adecuadas (por ejemplo, cláusulas contractuales estándar o normas empresariales vinculantes) y, por tanto, esto puede ser ilegal.

Es preceptivo que los interesados cuyos datos personales sean objeto de tratamiento en la nube sean informados acerca de la identidad del responsable del tratamiento y de los fines del tratamiento (un requisito para todos los responsables del tratamiento en virtud de la

Directiva sobre protección de datos 95/46/CE). Dada la posible complejidad de las cadenas de tratamiento en el entorno de la computación en nube, con el fin de garantizar un tratamiento de datos leal respecto del interesado (artículo 10 de la Directiva 95/46/CE), los responsables del tratamiento deberán también, a modo de buena práctica, proporcionar más información sobre los (sub)encargados que prestan servicios de computación en nube.

3. Marco jurídico

3.1 Marco de protección de datos

El marco jurídico pertinente es la Directiva 95/46/CE sobre protección de datos. Esta Directiva se aplica en todos los casos en que se tratan datos personales a resultas del uso de servicios de computación en nube. La Directiva 2002/58/CE sobre privacidad (modificada por la Directiva 2009/136/CE) se aplica al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones (operadores de telecomunicaciones) y, por tanto, es pertinente si tales servicios se prestan por medio de una solución en nube[5].

3.2 Legislación aplicable

Los criterios para determinar la aplicabilidad de la legislación se recogen en el artículo 4 de la Directiva 95/46/CE, que se refiere a la legislación aplicable a los responsables del tratamiento[6] con uno o varios establecimientos en el EEE y también a la ley aplicable a los responsables del tratamiento que se encuentren fuera del EEE, pero que utilicen equipo situado en el EEE para el tratamiento de los datos personales. El GT 29 analizó esta cuestión en su Dictamen 8/2010 sobre la ley aplicable[7].

En el primer caso, el factor que determina la aplicación del Derecho de la UE al responsable del tratamiento es la localización del establecimiento de éste y las actividades que realice, de conformidad con el artículo 4, apartado 1, letra a), de la Directiva, siendo irrelevante el tipo de modelo de servicio de computación en nube de que se trate. La legislación aplicable será la del país en que esté establecido el responsable del tratamiento que contrata los servicios de computación en nube, y no la del lugar donde se encuentren los proveedores de servicios de computación en nube.

Si el responsable del tratamiento está establecido en varios Estados miembros y el tratamiento de datos lo realiza como parte de sus actividades en estos países, la ley aplicable será la de cada uno de los Estados miembros en que se realice este tratamiento.

---

5 Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (modificada por la Directiva 2009/136/CE). La Directiva 2002/58/CE se aplica a los proveedores de servicios de comunicaciones electrónicas disponibles al público y les obliga a garantizar el cumplimiento de las obligaciones relativas a la confidencialidad de las comunicaciones y a la protección de los datos personales, así como los derechos y obligaciones respecto a las redes y servicios de comunicaciones electrónicas. En los casos en que los proveedores de computación en nube actúen como proveedores de servicios de comunicaciones electrónicas disponibles al público, estarán sujetos a esta Directiva.

6 El concepto de responsable del tratamiento puede encontrarse en el artículo 2, letra h), de la Directiva y fue analizado por el GT 29 en su dictamen 1/2010 sobre los conceptos de responsables y encargados del tratamiento.

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf

El artículo 4, apartado 1, letra c)[8], se refiere a la manera en que la legislación de protección de datos se aplica a los responsables del tratamiento que no están establecidos en el EEE y que recurran, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio del Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito. Esto significa que, si un cliente está establecido fuera del EEE, pero contrata a un proveedor situado en el EEE, entonces el proveedor exporta la legislación sobre protección de datos al cliente.

3.3 Funciones y responsabilidades de las diversas partes

Como se ha indicado anteriormente, la computación en nube engloba a varias partes distintas. Es importante evaluar y aclarar el papel de cada uno de ellas a fin de determinar sus obligaciones específicas en relación con la legislación vigente sobre protección de datos.

Cabe recordar que el GT 29 señaló en su dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» que «*el papel primero y primordial del concepto de responsable del tratamiento es determinar quién debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera los interesados pueden ejercer sus derechos en la práctica. En otras palabras, debe asignar la responsabilidad*». Estos dos criterios generales relativos al cumplimiento y la asignación de responsabilidad deberán ser tenidos en cuenta por las partes implicadas en todo el análisis.

3.3.1 Clientes y proveedores de servicios de computación en nube

El cliente determina el objetivo último del tratamiento y decide sobre la externalización de este tratamiento y la delegación de la totalidad o de parte de las actividades de tratamiento a una organización externa. El cliente actúa por tanto como responsable del tratamiento. La Directiva define al responsable del tratamiento como «*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales*». El cliente, como responsable del tratamiento, debe aceptar la responsabilidad de respetar la legislación sobre protección de datos, y es responsable y está sujeto a todas las obligaciones legales que figuran en la Directiva 95/46/CE. El cliente podrá encargar al proveedor que elija los métodos y medidas técnicas y de organización adecuados para alcanzar los fines del responsable del tratamiento.

El proveedor es la entidad que presta los servicios de computación en nube de las distintas formas que se han mencionado. Cuando el proveedor suministra los medios y la plataforma, actuando en nombre del cliente, se considera que es el encargado del tratamiento es decir, con arreglo a la Directiva 95/46/CE, «*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*».[9][10]

---

8 El artículo 4, apartado 1, letra c), dispone que los Estados miembros aplicarán las disposiciones nacionales que hayan aprobado para la aplicación de la Directiva a todo tratamiento de datos personales cuando «el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea».

9 El presente dictamen se centra únicamente en la relación normal entre el responsable y el encargado del tratamiento.

10 La computación en nube también puede ser utilizada por personas físicas (usuarios) para realizar actividades exclusivamente personales o domésticas. En tal caso, deberá analizarse cuidadosamente si se aplica la

Como se señaló en el dictamen 1/2010, pueden utilizarse algunos criterios para evaluar la responsabilidad del tratamiento[11]. De hecho, pueden darse situaciones en que un proveedor puede considerarse como responsable del tratamiento conjunto o responsable del tratamiento por derecho propio en función de circunstancias concretas. Por ejemplo, este podría ser el caso cuando el proveedor trata datos para sus propios fines.

Cabe insistir en que, incluso en entornos complejos de tratamiento de datos en los que distintos responsables desempeñen un papel en el tratamiento de datos personales, el cumplimiento de las normas de protección de datos y la responsabilidad por posibles infracciones de tales normas deben estar claramente asignados a fin de evitar que la protección se vea mermada o que se produzca un «conflicto negativo de competencia» o lagunas por las que ciertas obligaciones o derechos emanados de la Directiva no estén garantizados por ninguna de las partes.

En la actual situación de la computación en nube, los clientes de estos servicios pueden no tener margen de maniobra a la hora de negociar las condiciones de uso de los mismos, ya que las ofertas normalizadas son una característica de muchos servicios de computación en nube. No obstante, en última instancia, es el cliente quien decide sobre la asignación de parte o de la totalidad de las operaciones de tratamiento a los servicios en nube con fines específicos; la función del proveedor de estos servicios será la de contratista frente al cliente, que es el punto clave en este caso. Tal como se recoge en el Dictamen 1/2010 del GT 29[12] sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», «*el desequilibrio en cuanto al poder contractual entre un pequeño responsable del tratamiento y un gran proveedor de servicios no debería considerarse una justificación para que el primero acepte cláusulas y condiciones de contratos que no se ajusten a la legislación en materia de protección de datos*». Por esta razón, el responsable del tratamiento debe elegir un proveedor que garantice el cumplimiento de la legislación sobre protección de datos. Debe prestarse una atención especial a las características de los contratos, que deberán incluir una serie de garantías de protección de datos normalizadas, incluidas las señaladas por el Grupo de Trabajo en el punto 3.4.3 (Medidas técnicas y de organización) y en el punto 3.5 (Flujos de datos transfronterizos), así como cualesquiera mecanismos adicionales que puedan resultar adecuados para facilitar la diligencia debida y la responsabilidad (como auditorías de terceros independientes y certificaciones de los servicios de un proveedor – véase el apartado 4.2).

Los proveedores (como encargados del tratamiento) tienen la obligación de garantizar la confidencialidad. La Directiva 95/46/CE establece que: «*Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal*». El acceso a los datos por parte del proveedor durante la prestación de servicios también se rige fundamentalmente por el requisito de cumplir las disposiciones del artículo 17 de la Directiva – véase el apartado 3.4.2.

Los encargados del tratamiento deben tener en cuenta el tipo de nube en cuestión (pública, privada, comunitaria o híbrida / IaaS, SaaS o PaaS [véase el anexo A) Modelos de implantación - b) Modelos de prestación de servicios]) y el tipo de servicio contratado por el

---

denominada excepción doméstica que exime a los usuarios de ser considerados responsables del tratamiento. Sin embargo, esta cuestión queda fuera del ámbito del presente dictamen.

11 Por ejemplo, nivel de instrucciones, seguimiento por el cliente, conocimientos especializados de las partes.

12 Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

cliente. Los encargados del tratamiento son responsables de la adopción de las normas de seguridad, de conformidad con las disposiciones de la legislación de la UE aplicadas en las jurisdicciones del responsable y del encargado del tratamiento. Los encargados del tratamiento deben también apoyar y asistir al responsable del tratamiento a respetar los derechos (ejercidos) de los interesados.

3.3.2 Subcontratistas

Los servicios de computación en nube pueden implicar la participación de un número de partes contratadas que actúen como encargados del tratamiento. También es frecuente que los encargados del tratamiento subcontraten subencargados del tratamiento adicionales que, a su vez, acceden a los datos personales. En caso de que los encargados del tratamiento subcontraten los servicios, están obligados a comunicarlo al cliente, detallando el tipo de servicio subcontratado, las características de los subcontratistas actuales o potenciales y las garantías que estas entidades ofrecen al proveedor de servicios de computación en nube para dar cumplimiento a lo dispuesto en la Directiva 95/46/CE.

Todas las obligaciones pertinentes se aplican por tanto también a los subencargados del tratamiento a través de contratos entre el proveedor y el subcontratista que reflejen las disposiciones del contrato entre el cliente y el proveedor. En su Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», el GT 29 hace referencia a la multiplicidad de encargados del tratamiento en casos en que puedan tener una relación directa con el responsable del tratamiento o actuar como subcontratistas cuando los encargados del tratamiento externalizan parte de la actividad de tratamiento encomendada. «*No hay nada en la Directiva que impida que, por exigencias organizativas, se pueda designar a varias entidades como encargadas (o subencargadas) del tratamiento de datos, incluso subdividiendo los cometidos en cuestión. Ahora bien, todas ellas tienen que ajustarse a las instrucciones dadas por el responsable del tratamiento de los datos al llevar a cabo el tratamiento*»[13].

En tales supuestos, las obligaciones y responsabilidades derivadas de la legislación sobre protección de datos deberán consignarse claramente y no dispersarse a lo largo de la cadena de externalización o subcontratación, con el fin de garantizar el control efectivo sobre las actividades de tratamiento y asignar una responsabilidad clara a este respecto.

Un posible modelo de garantías que pueden utilizarse para aclarar los derechos y obligaciones de los encargados del tratamiento cuando subcontratan actividades de tratamiento de datos se introdujo por primera vez mediante la Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países[14]. En este modelo se permite el subtratamiento únicamente previa autorización, por escrito, del responsable del tratamiento y previo acuerdo escrito que imponga al subencargado del tratamiento las mismas obligaciones que al encargado. En caso de que el subencargado no cumpla sus obligaciones de protección de los datos con arreglo a dicho acuerdo escrito, el encargado responderá plenamente frente al responsable del tratamiento por la ejecución de las obligaciones del subencargado con arreglo a dicho acuerdo. Una disposición de este tipo podría utilizarse en las cláusulas contractuales entre un responsable del tratamiento y un proveedor, cuando este último prevea prestar

---

13 Véase WP169, p. 29, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)

14 Véase Preguntas Frecuentes II.5 del WP176.

servicios mediante subcontratación, a fin de contar con las garantías exigidas para el subtratamiento.

La Comisión ha propuesto recientemente una solución similar por lo que respecta a las garantías en el subtratamiento, en la propuesta de Reglamento general sobre protección de datos[15]. La realización del tratamiento por un encargado se regirá por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento y que disponga, en particular, que el encargado solo recurrirá a otro encargado del tratamiento con la autorización previa del responsable del tratamiento (artículo 26, apartado 2, de la propuesta).

En opinión del GT 29, el encargado del tratamiento podrá subcontratar sus actividades únicamente sobre la base del consentimiento del responsable del tratamiento, que suele darse al inicio del servicio[16], con la inequívoca obligación para el encargado de informar al responsable sobre cualquier cambio previsto en lo que respecta a la adición o sustitución de subcontratistas, teniendo el responsable del tratamiento en todo momento la posibilidad de oponerse a tales cambios o de rescindir el contrato. Debe existir la clara obligación del proveedor de nombrar a todos los subcontratistas. Además, debería firmarse un contrato entre el proveedor y el subcontratista que refleje las disposiciones del contrato entre el cliente y el proveedor. El responsable del tratamiento debería poder hacer uso de las posibilidades contractuales de recurso en caso de incumplimiento de los contratos causado por los subcontratistas. Esto podría organizarse garantizando que el encargado responda directamente ante el responsable por los incumplimientos causados por cualquier subcontratista que haya contratado, o mediante la creación de un derecho de tercero beneficiario en beneficio del responsable del tratamiento en los contratos firmados entre el encargado del tratamiento y los subcontratistas o por el hecho de que tales contratos se firmen en nombre del responsable del tratamiento, haciendo a este último parte del contrato.

3.4 Requisitos de protección de datos en la relación cliente-proveedor

3.4.1 Cumplimiento de los principios básicos

La legalidad del tratamiento de los datos personales en la nube depende de la observancia de los principios básicos de la normativa europea de protección de datos. Básicamente, debe garantizarse la transparencia con respecto al interesado, debe cumplirse el principio de especificación del objetivo y de limitación de la finalidad, y los datos personales deben suprimirse tan pronto como su conservación no sea necesaria. Por otra parte, deberán establecerse medidas técnicas y de organización adecuadas para garantizar un nivel adecuado de protección y seguridad de los datos.

3.4.1.1 Transparencia

La transparencia es un factor clave de cara a un tratamiento equitativo y legítimo de los datos personales. La Directiva 95/46/CE obliga al cliente a proporcionar al interesado cuyos datos se recaben información sobre su identidad y la finalidad del tratamiento. El cliente deberá facilitar también información adicional tal como la relativa a los destinatarios o categorías de destinatarios de los datos, que pueden incluir también los encargados del tratamiento y

[15] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos, 25.1.2012.

[16] Véanse Preguntas Frecuentes II, 1) del WP176, adoptado el 12 de julio de 2010.

subencargados, en la medida en que dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado (artículo 10 de la Directiva)[17].

La transparencia debe garantizarse también en la relación entre el cliente, el proveedor y los subcontratistas (en su caso). El cliente sólo es capaz de evaluar la legalidad del tratamiento de datos personales en la nube si el proveedor le informa sobre todas las cuestiones pertinentes. Un responsable del tratamiento que contrate a un proveedor deberá comprobar cuidadosamente las condiciones de éste y evaluarlas desde el punto de vista de la protección de datos.

La transparencia en la nube supone que es necesario que el cliente tenga conocimiento de todos los subcontratistas que contribuyan a la prestación de los respectivos servicios en nube, así como de la localización de todos los centros donde puedan tratarse los datos personales[18].

Si la prestación del servicio requiere la instalación de programas informáticos en los sistemas del cliente (por ejemplo, *plug-ins* de navegador), el proveedor, a modo de buena práctica, deberá informar al cliente sobre esta circunstancia y, en particular, sobre sus implicaciones desde el punto de vista de la protección y la seguridad de los datos. E inversamente, el cliente deberá plantear esta cuestión con carácter previo, si no es abordada de manera suficiente por el proveedor.

3.4.1.2 Especificación y limitación de la finalidad

El principio de especificación y limitación de la finalidad exige que los datos personales sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines (véase el artículo 6, apartado 1, letra b), de la Directiva 95/46/CE). El cliente deberá determinar la finalidad del tratamiento antes de la recogida de los datos personales del interesado, e informarle de ello. El cliente no deberá tratar los datos personales para otros fines que no sean compatibles con los originales.

Además, es preciso garantizar que el proveedor o alguno de sus subcontratistas no traten (ilegalmente) los datos personales para otros fines. Como la computación en nube puede fácilmente implicar a un gran número de subcontratistas, el riesgo de tratamiento de los datos personales para otros fines incompatibles debe considerarse bastante elevado. Para reducir al mínimo este riesgo, el contrato entre el proveedor y el cliente deberá incluir medidas técnicas y de organización al efecto y ofrecer garantías para el registro y la auditoría de las operaciones de tratamiento de datos personales realizadas por los empleados del proveedor o los subcontratistas[19]. Deberán imponerse en el contrato sanciones para el proveedor o los subcontratistas en caso de infracción de la legislación sobre protección de datos.

3.4.1.3 Supresión de datos

De conformidad con el artículo 6, apartado 1, letra e), de la Directiva 95/46/CE, los datos personales deberán ser conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los datos personales que ya no sean necesarios deberán suprimirse o anonimizarse. Si no pueden suprimirse debido a una obligación jurídica de conservarlos (por ejemplo, normas fiscales), el acceso a ellos deberá

---

[17] La obligación de informar al interesado existe cuando los datos que no se han recabado del propio interesado, sino de otras fuentes, se registran o divulgan a un tercero (véase el artículo 11).

[18] Sólo entonces podrá evaluar si los datos personales pueden ser transferidos a un llamado tercer país fuera del Espacio Económico Europeo (EEE) que no garantice un nivel adecuado de protección en el sentido de la Directiva 95/46/CE. Véase también la sección 3.4.6.

[19] Véase la sección 3.4.3.

bloquearse. Es responsabilidad del cliente garantizar que los datos personales se supriman tan pronto como dejen de ser necesarios en el sentido mencionado[20].

El principio de supresión de datos se aplica a los datos personales con independencia de si están almacenados en un disco duro o en otros medios (por ejemplo, cintas de copia de seguridad). Dado que los datos personales pueden mantenerse de forma redundante en diferentes servidores en diferentes lugares, deberá garantizarse que todos ellos se supriman irreversiblemente (es decir, las versiones anteriores, ficheros temporales e incluso fragmentos de ficheros también deberán suprimirse).

Los clientes deberán ser conscientes de que los datos de registro[21] que facilitan la auditoría de, por ejemplo, el almacenamiento, la modificación o la supresión de datos, también pueden considerarse datos personales relativos a la persona que inició la operación de tratamiento en cuestión[22].

Garantizar la supresión de los datos personales exige que los medios de almacenamiento sean destruidos o desmagnetizados, o que los datos personales se supriman efectivamente grabando encima de ellos. Para esta sobreescritura, deberán utilizarse programas informáticos especiales que sobreescriban datos múltiples veces de conformidad con una especificación reconocida.

El cliente deberá asegurarse de que el proveedor garantice una supresión segura en el sentido mencionado y que el contrato entre el proveedor y el cliente contenga disposiciones claras relativas a la supresión de los datos personales[23]. Lo mismo se aplica a los contratos entre proveedores y subcontratistas.

3.4.2 Garantías contractuales de las relaciones entre el responsable y el encargado del tratamiento

Cuando un responsable del tratamiento decida contratar servicios de computación en nube, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas (artículo 17, apartado 2, de la Directiva 95/46/CE). Además, estará legalmente obligado a firmar un contrato formal con el proveedor de servicios, tal como se establece en el artículo 17, apartado 3, de la Directiva 95/46/CE. Este artículo establece la condición de que exista un contrato u otro acto jurídico vinculante para regular las relaciones entre el responsable y el encargado del tratamiento. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas técnicas y de organización constarán por escrito o en otra forma equivalente.

Como mínimo, el contrato deberá establecer, en particular, que el encargado del tratamiento deberá seguir las instrucciones del responsable y que deberá aplicar medidas técnicas y de organización para proteger adecuadamente los datos personales.

A fin de garantizar la seguridad jurídica, el contrato deberá también exponer los siguientes aspectos:

---

[20] La supresión de datos es pertinente tanto a lo largo de la duración de un contrato de computación en nube como a su finalización. También es pertinente en caso de sustitución o retirada de un subcontratista.

[21] En el apartado 4.3.4.2 figuran observaciones referentes a los requisitos de registro.

[22] Esto significa que deberán definirse los periodos de conservación razonables para los ficheros de registro y que deberán estar establecidos los procedimientos para garantizar la oportuna supresión o anonimización de estos datos.

[23] Véase la sección 3.4.3.

1. Datos sobre el alcance y las modalidades de las instrucciones del cliente que deberán darse al proveedor, con especial atención a los acuerdos sobre nivel de servicios aplicables (que deberán ser objetivos y mensurables) y las sanciones correspondientes (financieras o de otro tipo, incluida la posibilidad de demandar al proveedor en caso de incumplimiento).
2. Especificación de las medidas de seguridad que deberá cumplir el proveedor, en función de los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse. Es muy importante que se especifiquen medidas técnicas y de organización concretas como las descritas en el apartado 3.4.3. Esto se entiende sin perjuicio de la aplicación de medidas más estrictas, en su caso, en virtud de la legislación nacional del cliente.
3. Objeto y calendario del servicio de computación en nube que deberá prestar el proveedor, alcance, forma y finalidad del tratamiento de datos personales por el proveedor, así como tipos de datos tratados.
4. Especificación de las condiciones necesarias para devolver los datos (personales) o destruirlos una vez finalizado el servicio. Además, debe garantizarse que los datos personales se borran con seguridad a petición del cliente.
5. Inclusión de una cláusula de confidencialidad, vinculante tanto para el proveedor como para cualesquiera de sus empleados que puedan tener acceso a los datos. Sólo las personas autorizadas podrán tener acceso a los datos.
6. Obligación del proveedor de apoyar al cliente facilitando el ejercicio de los derechos de los interesados a acceder, rectificar o suprimir sus datos.
7. El contrato deberá establecer expresamente que el proveedor no podrá comunicar los datos a terceros, ni siquiera con fines de conservación, a menos que el contrato prevea la existencia de subcontratistas. El contrato deberá especificar que sólo podrá contratarse subencargados del tratamiento previa autorización que puede otorgar en general el responsable del tratamiento, en consonancia con la inequívoca obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de cualquier cambio previsto a este respecto, teniendo el responsable del tratamiento en todo momento la posibilidad de oponerse a tales alteraciones o de rescindir el contrato. Deberá existir una clara obligación para el proveedor de nombrar a todos los subcontratistas contratados (por ejemplo, en un registro digital público). Deberá garantizarse que los contratos suscritos entre proveedores y subcontratistas reflejen las condiciones del contrato entre el cliente y el proveedor (esto es, que los subencargados del tratamiento están sujetos a los mismos derechos contractuales que el proveedor). En particular, deberá garantizarse que tanto el proveedor como todos los subcontratistas sólo actuarán siguiendo instrucciones del cliente. Tal como se explica en el capítulo sobre el subtratamiento, la cadena de responsabilidad deberá exponerse claramente en el contrato. Deberá fijarse la obligación por parte del encargado del tratamiento de definir las transferencias internacionales, por ejemplo firmando contratos con subcontratistas, basándose en las cláusulas contractuales tipo 2010/87/UE.
8. Clarificación de las responsabilidades del proveedor en cuanto a notificación al cliente en caso de violaciones de datos que afecten a sus datos.
9. Obligación del proveedor de proporcionar una lista de los lugares donde se tratarán los datos.

10. Derecho del responsable del tratamiento a controlar, y la correspondiente obligación del proveedor de cooperar.
11. Debe establecerse contractualmente que el proveedor deberá informar al cliente acerca de los principales cambios relativos a sus respectivos servicios, tales como la ejecución de funciones adicionales.
12. El contrato deberá prever el registro y la auditoría de las operaciones de tratamiento de datos personales realizadas por el proveedor o los subcontratistas.
13. Notificación al cliente de toda solicitud jurídicamente vinculante de divulgar datos personales presentada por las autoridades policiales o judiciales a menos que esté prohibido; por ejemplo, la prohibición en virtud del Derecho penal de mantener la confidencialidad de una investigación policial.
14. Obligación general del proveedor de garantizar que su organización interna y disposiciones de tratamiento de datos (y las de sus subcontratistas, en su caso) son conformes con las normas y los requisitos legales nacionales e internacionales aplicables.

En caso de infracción por el responsable del tratamiento, toda persona que sufra daños y perjuicios como consecuencia de un tratamiento ilegal tendrá derecho a obtener del responsable del tratamiento compensación por los daños causados. Si los encargados del tratamiento utilizan los datos para cualquier otro fin, o los comunican o utilizan de forma que se vulnere el contrato, también se considerarán responsables del tratamiento, y responderán de las infracciones en que hayan participado personalmente.

Hay que señalar que, en muchos casos, los proveedores ofrecen contratos y servicios estándar para su firma por los responsables del tratamiento, que establecen un formato estándar para el tratamiento de datos personales. Este desequilibrio en cuanto al poder contractual entre un pequeño responsable del tratamiento y un gran proveedor de servicios no debería considerarse una justificación para que el primero acepte cláusulas y condiciones de contratos que no se ajusten a la legislación en materia de protección de datos.

3.4.3 Medidas técnicas y de organización para garantizar la protección de los datos y su seguridad

El artículo 17, apartado 2, de la Directiva 95/46/CE prevé la plena responsabilidad de los clientes (actuando como responsables del tratamiento) para elegir un proveedor que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y para asegurarse de que se cumplen dichas medidas.

Además de los objetivos de seguridad esenciales de disponibilidad, confidencialidad e integridad, debe prestarse atención igualmente a los objetivos complementarios de transparencia (véase 3.4.1.1), aislamiento[24], posibilidad de intervención, responsabilidad y portabilidad. Esta sección destaca estos objetivos esenciales en materia de protección de datos, sin perjuicio de otros análisis de riesgos complementarios orientados a la seguridad[25].

---

[24] En la legislación alemana se ha introducido el concepto más amplio de «imposibilidad de establecer vínculos», promovido por la Conferencia de Comisarios encargados de la protección de datos.

[25] Véase por ejemplo, ENISA en http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[26] Un ataque de denegación de servicio es un intento coordinado de hacer que un ordenador o un recurso de red no esté disponible para sus usuarios autorizados, ya sea de forma temporal o indefinida (por ejemplo,

3.4.3.1 Disponibilidad

La disponibilidad supone garantizar un acceso oportuno y fiable a los datos personales.

Una grave amenaza para la disponibilidad en la nube es la pérdida accidental de conectividad de red entre el cliente y el proveedor, o del rendimiento de los servidores a causa de acciones malintencionadas tales como ataques de denegación de servicio (distribuido)[26]. Otros riesgos para la disponibilidad incluyen fallos accidentales de los equipos tanto en la red como en los sistemas de almacenamiento de datos y de tratamiento en la nube, cortes de suministro y otros problemas de infraestructura.

Los responsables del tratamiento deben comprobar si el proveedor ha adoptado medidas razonables para afrontar el riesgo de perturbaciones, tales como copia de seguridad de los enlaces de internet, almacenamiento suplementario y mecanismos efectivos para la copia de seguridad de los datos.

3.4.3.2 Integridad

La integridad puede definirse como la característica de que los datos son auténticos y no han sido maliciosamente o accidentalmente alterados durante el tratamiento, almacenamiento o transmisión. La noción de integridad puede ampliarse a los sistemas informáticos y exige que el tratamiento de datos personales en estos sistemas no se altere.

Pueden detectarse las alteraciones de datos personales mediante mecanismos de autenticación criptográfica tales como códigos de autenticación de mensajes o firmas.

La interferencia con la integridad de los sistemas informáticos en la nube puede prevenirse o detectarse mediante sistemas de prevención y detección de intrusiones (IPS/IDS). Esto es especialmente importante en el tipo de entornos de red abierta en que suelen operar las nubes.

3.4.3.3 Confidencialidad

En el medio en nube, el cifrado puede contribuir de forma significativa a la confidencialidad de los datos personales si se aplica correctamente, aunque no anonimice de forma irreversible los datos personales[27]. El cifrado de datos personales deberá utilizarse en todos los casos «en tránsito» y, cuando esté disponible, para los datos «en reposo»[28]. En algunos casos (por ejemplo, un servicio de almacenamiento IaaS) un cliente podrá no depender de la solución de cifrado solución propuesta por el proveedor y optar por cifrar los datos personales antes de enviarlos a la nube. Cifrar los datos en reposo exige prestar una atención especial a la gestión de las claves criptográficas, ya que la seguridad de los datos depende en última instancia de la confidencialidad de las claves de cifrado.

---

por medio de un gran número de sistemas atacantes que paralizan su objetivo con una multitud de solicitudes de comunicación externa).

[27] Directiva 95/46/CE, considerando 26: «considerando que (...); los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; (...)». En la misma línea, los procesos técnicos de fragmentación de datos que pueden utilizarse en el marco de la prestación de servicios de computación en nube no darán lugar a que los datos se anonimicen de forma irreversible y, por tanto, no implica que no sean de aplicación las obligaciones de protección de datos.

[28] Este es el caso, en particular, de los responsables del tratamiento que prevén transferir datos sensibles en el sentido del artículo 8 de la Directiva 95/46/CE (por ejemplo, datos sobre la salud) a la nube o que están sujetos a obligaciones jurídicas específicas de secreto profesional.

Las comunicaciones entre el proveedor y el cliente, así como entre los centros de datos, deberán estar cifradas. La administración remota de la plataforma en nube sólo deberá realizarse a través de un canal de comunicación seguro. Si un cliente prevé no sólo almacenar, sino también tratar datos personales en la nube (por ejemplo, búsqueda de bases de datos para los registros), deberá tener en cuenta que la codificación no puede mantenerse durante el tratamiento de los datos (con excepción de casos muy específicos).

Otras medidas técnicas destinadas a garantizar la confidencialidad incluyen mecanismos de autorización y autenticación (por ejemplo, autenticación de doble factor). Las cláusulas contractuales también deberían imponer obligaciones de confidencialidad a los empleados de los clientes, proveedores y subcontratistas.

3.4.3.4 Transparencia

Las medidas técnicas y de organización deben apoyar la transparencia que permita la revisión, véase 3.4.1.1.

3.4.3.5 Aislamiento (limitación de la finalidad)

En las infraestructuras en nube, los recursos como el almacenamiento, la memoria y las redes son comunes a muchos arrendatarios. Esto crea nuevos riesgos de que los datos se revelen y traten con fines ilegítimos. El objetivo de protección mediante «aislamiento» pretende abordar esta cuestión y contribuir a garantizar que los datos no se utilicen para propósitos distintos del inicial (artículo 6, apartado 1, letra b), de la Directiva 95/46/CE) así como mantener la confidencialidad y la integridad[29].

Para lograr el aislamiento se requiere en primer lugar una gestión adecuada de los derechos y funciones para acceder a los datos personales, objeto de revisión regular. Debería evitarse establecer funciones con privilegios excesivos (por ejemplo, ningún usuario ni administrador debe ser autorizado a acceder al conjunto de la nube). De manera más general, los administradores y usuarios sólo deben poder acceder a la información que necesiten para sus fines legítimos (principio del mínimo privilegio).

En segundo lugar, el aislamiento también depende de medidas técnicas tales como el endurecimiento de los supervisores y la correcta gestión de los recursos comunes si se utilizan máquinas virtuales para compartir recursos físicos entre diferentes clientes.

3.4.3.5 Posibilidad de intervención

La Directiva 95/46/CE otorga al interesado los derechos de acceso, rectificación, supresión, bloqueo y oposición (véanse los artículos 12 y 14). El cliente deberá verificar que el proveedor no impone obstáculos técnicos y de organización a estos requisitos, incluso en los casos en que los datos sean tratados posteriormente por los subcontratistas.

El contrato entre el cliente y el proveedor deberá precisar que el proveedor está obligado a apoyar al cliente facilitando el ejercicio de los derechos de los interesados y a garantizar que lo mismo se aplica a su relación con los subcontratistas[30].

3.4.3.6 Portabilidad

Actualmente, la mayoría de los proveedores no utiliza formatos de datos e interfaces de servicios estándar que facilitan la interoperatividad y la portabilidad entre los diferentes

[29] Véase 3.4.1.2.

[30] Véase la sección 3.4.2 nº 6. El proveedor podrá incluso recibir instrucciones para responder a las solicitudes en nombre del cliente.

proveedores. Si un cliente decide migrar de un proveedor a otro, esta falta de interoperatividad puede dar lugar a la imposibilidad o al menos a dificultades para transferir los datos (personales) del cliente al nuevo proveedor (esto se denomina dependencia respecto al proveedor). Lo mismo ocurre con los servicios desarrollados por el cliente en una plataforma ofrecida por el proveedor original (PaaS). Antes de contratar un servicio de computación en nube, el cliente deberá comprobar si el proveedor garantiza la portabilidad de los datos y servicios y de qué manera lo hace[31].

3.4.4.7 Responsabilidad

En informática, la responsabilidad puede definirse como la capacidad de determinar lo que hizo una entidad en un momento determinado en el pasado y de qué manera lo hizo. En el ámbito de la protección de datos, este concepto tiene a menudo un sentido más amplio y describe la capacidad de las partes para demostrar que tomaron las medidas adecuadas para garantizar la aplicación de los principios de protección de datos.

La responsabilidad en informática es especialmente importante para investigar violaciones de datos personales, en las que los clientes, proveedores y el subencargado del tratamiento pueden tener cada uno algún grado de responsabilidad operativa. La capacidad de la plataforma en la nube para proporcionar mecanismos de registro amplios y un control fiable es de vital importancia a este respecto.

Además, los proveedores deberán proporcionar pruebas documentales de la adopción de medidas adecuadas y efectivas que aporten los resultados de los principios de protección de datos señalados en las secciones anteriores. Son ejemplos de dichas medidas los procedimientos para garantizar la identificación de todas las operaciones de tratamiento de datos; para responder a las solicitudes de acceso; la asignación de recursos, incluida la designación de agentes de protección de datos que sean responsables de la organización del cumplimiento de la protección de datos; o los procedimientos de certificación independientes. Además, los responsables del tratamiento deberán garantizar que están dispuestos a demostrar, previa petición, el establecimiento de las medidas necesarias a la autoridad de supervisión competente[32].

3.5 Transferencias internacionales

Los artículos 25 y 26 de la Directiva 95/46/CE prevén la libre circulación de datos personales a países situados fuera del EEE sólo si el país en cuestión o el beneficiario garantizan un nivel adecuado de protección de datos. De otro modo, el responsable del tratamiento y sus corresponsables o encargados deberán establecer garantías específicas. Sin embargo, la computación en nube se basa a menudo en la total falta de ubicación estable de los datos en la red del proveedor. Los datos pueden encontrarse en un centro de datos a las 2 horas y en el otro lado del mundo a las 16 horas. Por tanto, el cliente rara vez se encuentra en posición de saber en cualquier momento en qué lugar están situados, almacenados o transferidos los datos. En este contexto, los instrumentos jurídicos tradicionales que ofrecen un marco para regular las transferencias de datos a terceros países que no ofrecen una protección adecuada, tienen sus límites.

---

[31] Preferiblemente, el proveedor deberá utilizar interfaces y formatos normalizados o abiertos. En cualquier caso, deberán acordarse cláusulas contractuales que estipulen formatos garantizados, la preservación de las relaciones lógicas y los costes derivados de la migración a otro proveedor.

[32] El Grupo de Trabajo presentó observaciones detalladas sobre el tema de la responsabilidad en su Dictamen 3/2010 sobre el principio de responsabilidad http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_es.pdf

3.5.1 Puerto seguro y países adecuados

Es muy difícil realizar las comprobaciones pertinentes, incluido el puerto seguro, relativas al ámbito geográfico, y por tanto no cubren todas las transferencias dentro de la nube.
Las transferencias a organizaciones de estadounidenses que están adheridas a los principios pueden realizarse legítimamente en virtud de la legislación de la UE, ya que se considera que las organizaciones beneficiarias proporcionan un nivel adecuado de protección de los datos transferidos.

Sin embargo, en opinión del GT, la autocertificación con puerto seguro por sí sola no puede considerarse suficiente en ausencia de una sólida aplicación de los principios de protección de datos en la computación en nube. Asimismo, el artículo 17 de la Directiva de la UE requiere la firma de un contrato entre el responsable y el encargado del tratamiento a efectos del tratamiento de datos, lo que se confirma en la FAQ 10 de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Este contrato no está sujeto a la autorización previa de las autoridades de protección de datos europeas. Dicho contrato especifica el tratamiento que debe efectuarse y las medidas necesarias para garantizar que los datos están seguros. Otras legislaciones nacionales y autoridades de protección de datos pueden exigir otros requisitos.

El GT considera que las empresas exportadoras de datos no deben basarse únicamente en la declaración del importador de datos de que tiene una certificación de puerto seguro. Por el contrario, la empresa que exporta datos debe obtener pruebas de la existencia de las autocertificaciones de puerto seguro y solicitar pruebas de que se cumplen sus principios. Esto es especialmente importante por lo que se refiere a la información proporcionada a los interesados afectados por el tratamiento de datos[33] [34].

El GT también considera que el cliente debe comprobar si los contratos tipo elaborados por los proveedores cumplen los requisitos nacionales sobre tratamiento de datos contractual. La legislación nacional puede exigir que el subtratamiento se defina en el contrato, lo que incluye datos sobre los lugares y otros relativos a los subencargados del tratamiento, así como la trazabilidad de los datos. Normalmente, los proveedores no ofrecen al cliente tal información –su compromiso con el puerto seguro no puede sustituir la falta de las garantías anteriormente mencionadas, cuando así lo exija la legislación nacional. En tal caso, se anima al exportador a que utilice otros instrumentos jurídicos disponibles, como cláusulas contractuales tipo o normas corporativas vinculantes (NCV).

Por último, el GT considera que los principios de puerto seguro por sí solos pueden no garantizar al exportador de datos los medios necesarios para asegurar que el proveedor ha aplicado las medidas de seguridad apropiadas en los Estados Unidos, según pueden requerir las legislaciones nacionales sobre la base de la Directiva 95/46/CE[35]. En términos de seguridad de los datos, la computación en nube plantea varios riesgos de seguridad específicos de la nube, tales como pérdida de gobernanza, supresión de datos insegura o

---

[33] Véase la autoridad de protección de datos alemana: http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf..

[34] Por lo que respecta a los requisitos relativos a la contratación de subencargados del tratamiento, véase el punto 3.3.2.

[35] Véase el dictamen de la autoridad de protección de datos de Dinamarca: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

incompleta, pistas de auditoría insuficientes o fallos de aislamiento[36], que no son tenidos suficientemente en cuenta por los actuales principios de puerto seguro sobre la seguridad de los datos[37]. Así pues, podrán establecerse garantías adicionales para la seguridad de los datos, por ejemplo mediante la incorporación de conocimientos y recursos de terceros que sean capaces de evaluar la adecuación de los proveedores mediante distintos sistemas de auditoría, normalización y certificación[38]. Por estos motivos, podría ser aconsejable complementar el compromiso del importador de datos con el puerto seguro con salvaguardias adicionales que tengan en cuenta la naturaleza específica de la nube.

3.5.2 Excepciones

Las exenciones previstas en el artículo 26 de la Directiva 95/46/CE permiten a los exportadores de datos transferir datos fuera de la UE sin proporcionar garantías adicionales. Sin embargo, el GT 29 adoptó un dictamen en el que consideraba que las excepciones sólo se aplicarán cuando las transferencias no sean recurrentes, voluminosas ni estructurales[39].

Sobre la base de esas interpretaciones, es casi imposible recurrir a las excepciones en el marco de la computación en nube.

3.5.3 Cláusulas contractuales tipo

Las cláusulas contractuales tipo adoptadas por la Comisión Europea para delimitar las transferencias internacionales de datos entre dos responsables del tratamiento o entre un responsable y un encargado del tratamiento se basan en un enfoque bilateral. Cuando el proveedor es considerado encargado del tratamiento, las cláusulas tipo de conformidad con la Decisión 2010/87/CE de la Comisión son un instrumento que puede ser utilizado entre el encargado y el responsable del tratamiento como base para que la computación en nube ofrezca garantías adecuadas en el contexto de las transferencias internacionales.

Además de las cláusulas contractuales tipo, el GT considera que los proveedores podrían ofrecer a los clientes disposiciones que se basen en sus experiencias prácticas, siempre que no contradigan, directa ni indirectamente, las cláusulas contractuales tipo aprobadas por la Comisión ni prejuzguen los derechos fundamentales y las libertades de los interesados[40]. Sin embargo, las empresas no podrán alterar ni modificar las cláusulas contractuales tipo sin que ello implique que las cláusulas dejen de ser «tipo»[41].

Cuando el proveedor que actúe como encargado del tratamiento esté establecido en la UE, la situación podría ser más compleja ya que las cláusulas tipo se aplican, en general, únicamente a la transferencia de datos de un responsable del tratamiento de la UE a un encargado del

---

36 Descrito en detalle en el documento de ENISA «Cloud Computing: Benefits, risks and recommendations for information security» (Computación en nube: ventajas, riesgos y recomendaciones para la seguridad de la información) en: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

37 «Las organizaciones deben tomar precauciones razonables para proteger la información personal contra la pérdida, el uso indebido y el acceso no autorizado, la divulgación, la alteración y la destrucción».

38 Véase la sección 4.2.

39 Documento de Trabajo 12/1998: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, adoptado por el Grupo de Trabajo el 24 de julio de 1998 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_es.pdf).

40 Véase la Pregunta Frecuente IV B1.9 9, ¿Pueden las empresas incluir las cláusulas contractuales tipo en un contrato más amplio y añadir cláusulas específicas? Publicado por la CE en: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

41 Véase la Pregunta Frecuente IV B1.10, ¿Pueden las empresas enmendar y modificar las cláusulas contractuales tipo aprobadas por la Comisión?

tratamiento fuera de la UE (véase el considerando 23 de la Decisión 2010/87/UE de la Comisión sobre las cláusulas tipo y WP 176).

Por lo que se refiere a la relación contractual entre el encargado del tratamiento y los subcontratistas fuera de la UE, deberá establecerse un acuerdo escrito que imponga las mismas obligaciones al subencargado del tratamiento que las que se imponen al encargado del tratamiento en las cláusulas tipo.

3.5.4 Normas corporativas vinculantes (NCV): hacia un enfoque global

Las normas corporativas vinculantes (NCV) constituyen un código de conducta para las empresas que transfieren datos dentro de su grupo. Esta solución se proporcionará igualmente en el contexto de la computación en nube cuando el proveedor de los servicios sea encargado del tratamiento. De hecho, el GT 29 está trabajando actualmente en unas NCV para los encargados del tratamiento que permitirán la transferencia dentro del grupo en beneficio de los responsables del tratamiento, sin que se precise la firma de contratos entre el encargado y los subencargados del tratamiento para cada cliente[42].

Tales normas corporativas vinculantes para los encargados del tratamiento permitirían al cliente del proveedor confiar a sus datos personales al encargado del tratamiento, al tiempo que se asegura de que los datos transferidos en el ámbito del proveedor recibirán un nivel de protección adecuado.

4. Conclusiones y recomendaciones

Las empresas y administraciones que deseen utilizar la computación en nube deberán efectuar, como primer paso, un análisis de riesgos completo y riguroso. Este análisis deberá abordar los riesgos relacionados con el tratamiento de datos en la nube (falta de control e información insuficiente – véase la sección 2) por lo que respecta al tipo de datos tratados[43]. También deberá prestarse una atención especial a la hora de evaluar los riesgos jurídicos en materia de protección de datos, que afectan principalmente a las obligaciones de seguridad y a las transferencias internacionales. El tratamiento de datos sensibles a través de la computación en nube suscita inquietudes adicionales. Por tanto, sin perjuicio de las legislaciones nacionales, este tratamiento requiere salvaguardias adicionales[44]. Las conclusiones que figuran a continuación tienen por objetivo proporcionar una lista de control para el respeto de la protección de datos por parte de los proveedores y los clientes, sobre la base del marco jurídico actual; también se proporcionan algunas recomendaciones con vistas a la futura evolución del marco normativo de la UE y más allá de sus fronteras.

---

42 Véase el documento de trabajo 02/2012 sobre la creación de un cuadro con los elementos y principios que se recogen en las normas corporativas vinculantes para el encargado del tratamiento, aprobado el 6 de junio de 2012: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

43 ENISA ofrece una lista de los riesgos que deben tenerse en cuenta http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

44 Véase Memorándum Sopot, véase nota a pie de página 2.

4.1 Directrices para los clientes y proveedores de servicios de computación en nube

- Relación entre el responsable y el encargado del tratamiento: el presente dictamen se centra en la relación cliente-proveedor como relación responsable-encargado del tratamiento; (véase el apartado 3.3.1). No obstante, en circunstancias concretas, pueden darse situaciones en que el proveedor actúe también como responsable del tratamiento, por ejemplo, cuando el proveedor trata de nuevo algunos datos personales para sus propios fines. En tal caso, el proveedor de servicios de computación en nube tiene plena responsabilidad (conjunta) sobre el tratamiento y deberá cumplir todas las obligaciones jurídicas estipuladas por las Directivas 95/46/CE y 2002/58/CE (en su caso).
- Responsabilidad del cliente como responsable del tratamiento: el cliente como responsable del tratamiento debe aceptar la responsabilidad de respetar la legislación sobre protección de datos, y estará sujeto a todas las obligaciones mencionadas en las Directivas 95/46/CE y 2002/58/CE, cuando proceda, en particular con respecto a los interesados (véase el apartado 3.3.1). El cliente deberá seleccionar un proveedor que garantice el cumplimiento de la legislación de la UE sobre protección de datos tal como se refleja en las oportunas garantías contractuales que se resumen a continuación.
- Salvaguardias relativas a la subcontratación: en los contratos entre proveedores y clientes deberán preverse disposiciones relativas a los subcontratistas. Los contratos deberán especificar que sólo podrá contratarse a subencargados del tratamiento previa autorización general del responsable del tratamiento, en consonancia con la inequívoca obligación del encargado del tratamiento de informar al responsable de cualquier cambio previsto a este respecto, conservando el responsable del tratamiento en todo momento la posibilidad de oponerse a tales cambios o de rescindir el contrato. Debe existir una clara obligación para el proveedor de nombrar a todos los subcontratistas contratados. El proveedor deberá firmar un contrato con cada subcontratista que refleje las cláusulas de su contrato con el cliente; el cliente deberá asegurarse de que cuenta con posibilidades contractuales de recurso en caso de infracción del contrato por parte de los subcontratistas del proveedor (véase el punto 3.3.2).
- Cumplimiento de los principios fundamentales de protección de datos:
    - Transparencia (véase 3.4.1.1): en la negociación del contrato, los proveedores deberán informar a los clientes acerca de todos los aspectos pertinentes (sobre protección de datos) de sus servicios. En particular, deberá informarse a los clientes acerca de todos los subcontratistas que contribuyan a la prestación de los respectivos servicios en nube y de todos los lugares donde los datos puedan ser almacenados o tratados por el proveedor o sus subcontratistas (en particular, si algunos o todos los lugares se encuentran fuera del Espacio Económico Europeo-EEE). El cliente deberá disponer de información significativa sobre las medidas técnicas y de organización aplicadas por el proveedor. A modo de buena práctica, el cliente deberá informar a los interesados acerca del proveedor y de todos los subcontratistas (en su caso), así como acerca de los lugares donde los datos puedan ser almacenados o tratados por el proveedor o los subcontratistas.
    - Especificación y limitación de la finalidad (3.4.1.2): los clientes deberán garantizar el cumplimiento de los principios de especificación y limitación de la finalidad y garantizar que los datos no sean tratados posteriormente de manera incompatible con dichos fines por el proveedor o los subcontratistas.

Los compromisos a este respecto deberán recogerse en las medidas contractuales apropiadas (incluidas las garantías técnicas y de organización).

- Conservación de datos (3.4.1.3): el cliente es responsable de garantizar que los datos personales sean suprimidos (por el proveedor y los subcontratistas) dondequiera que se encuentren almacenados, en cuanto dejen de ser necesarios para los fines específicos. Deberán establecerse contractualmente mecanismos seguros de supresión (destrucción, desmagnetización, sobreescritura).

- Garantías contractuales (véase 3.4.2, 3.4.3 y 3.5):

  - En general: el contrato con el proveedor (y los que se establezcan entre el proveedor y los subcontratistas) deberán ofrecer suficientes garantías en términos de medidas de seguridad técnica y de organización (en virtud del artículo 17, apartado 2, de la Directiva) y deberán constar por escrito o de otra forma equivalente. El contrato deberá especificar las instrucciones del cliente al proveedor e incluir el objeto y el calendario del servicio, niveles de servicio objetivos y mensurables y las sanciones correspondientes (financieras o de otro tipo). Deberá asimismo precisar las medidas de seguridad que deben respetarse, en función de los riesgos del tratamiento y de la naturaleza de los datos, en consonancia con los requisitos correspondientes y con sujeción a las medidas más estrictas previstas en la legislación nacional de los clientes. Si los proveedores pretenden utilizar cláusulas contractuales tipo, deberán garantizar que éstas cumplen con los requisitos de protección de datos (véase 3.4.2). En particular, las medidas técnicas y de organización aplicadas por el proveedor deberán especificarse en los términos respectivos.

  - Acceso a los datos: únicamente las personas autorizadas deberán tener acceso a los datos. En el contrato deberá incluirse una cláusula de confidencialidad por lo que respecta al proveedor y sus empleados.

  - Divulgación de datos a terceros: esta cuestión deberá regularse únicamente a través del contrato, que deberá incluir la obligación de que el proveedor haga públicos todos sus subcontratistas (por ejemplo, en un registro digital público) y garantice el acceso del cliente a información sobre cualquier cambio, a fin de que éste pueda oponerse a tales cambios o rescindir el contrato. El contrato también deberá exigir al proveedor que notifique toda solicitud jurídicamente vinculante de divulgar datos personales presentada por las autoridades policiales o judiciales a menos que dicha divulgación esté prohibida por otras razones. El cliente deberá garantizar que el proveedor rechazará cualquier solicitud de divulgación jurídicamente no vinculante.

  - Obligación de cooperar: el cliente deberá garantizar que el proveedor esté obligado a cooperar con él en el ejercicio de su derecho a controlar las operaciones de tratamiento, a facilitar el ejercicio por los interesados de sus derechos a acceder, corregir o suprimir sus datos, y (en su caso), a notificarle toda violación que afecte a sus datos.

  - Transferencias de datos transfronterizas: el cliente deberá verificar si el proveedor puede garantizar la legalidad de las transferencias de datos transfronterizas y limitar las transferencias a los países elegidos por el cliente, siempre que sea posible. Las transferencias de datos a terceros países que no ofrezcan garantías, requieren salvaguardias específicas mediante el uso de disposiciones de puerto seguro, cláusulas contractuales tipo o normas corporativas vinculantes (NCV), según proceda. El uso de cláusulas

contractuales tipo para los encargados del tratamiento (en virtud de la Decisión 2010/87/CE de la Comisión) exige determinadas adaptaciones del entorno de la nube (para evitar tener diferentes contratos por cliente entre un proveedor y sus subencargados) lo que podría implicar la necesidad de una autorización previa de la autoridad de protección de datos competente. En el contrato deberá incluirse una lista de ubicaciones donde podrá prestarse el servicio.

- Registro y auditoría del tratamiento: el cliente deberá solicitar el registro de las operaciones de tratamiento realizadas por el proveedor y sus subcontratistas. El cliente deberá estar facultado para auditar tales operaciones de tratamiento. No obstante, podrán aceptarse certificaciones y auditorías de terceros elegidos por el responsable del tratamiento siempre que se garantice la plena transparencia (por ejemplo, estableciendo la posibilidad de obtener una copia de un certificado de auditoría de terceros o una copia del informe de auditoría que verifique la certificación).
- Medidas técnicas y de organización: deberán tener como objetivo paliar los riesgos que implica la falta de control y de información que rige en general el medio de la computación en nube. Las primeras incluyen medidas dirigidas a garantizar la disponibilidad, integridad, confidencialidad, aislamiento, posibilidad de intervención y portabilidad, tal como se definen en este documento, mientras que las últimas se centran en la transparencia (véase 3.4.3 para más detalles).

4.2 Certificaciones de protección de datos de terceros

- La verificación independiente o la certificación por terceros que gocen de reconocido prestigio puede ser un medio creíble para que los proveedores demuestren el cumplimiento de sus obligaciones según lo especificado en el presente dictamen. Dicha certificación indicaría, como mínimo, que los controles de protección de datos han sido objeto de una auditoría o revisión con respecto a una norma reconocida que cumple los requisitos expuestos en el presente dictamen, por una organización tercera que goce de reconocido prestigio[45]. En el contexto de la computación en nube, los clientes potenciales deben examinar si los proveedores de servicios en la nube pueden presentar una copia de este certificado de auditoría realizado por un tercero o una copia del informe de auditoría que verifique la certificación, incluso con respecto a los requisitos que figuran en el presente dictamen.
- La realización de auditorías individuales de datos alojados en un medio de servidores virtualizados con múltiples operadores puede ser poco práctica desde el punto de vista técnico y puede en algunos casos puede aumentar los riesgos para los controles físicos y lógicos de seguridad de las redes. En tales casos, podrá considerarse que la auditoría por un tercero de reconocido prestigio elegido por el responsable del tratamiento puede sustituir al derecho de un responsable del tratamiento de realizar una auditoría.
- La adopción de normas y certificaciones específicas sobre protección de la intimidad es esencial para establecer una relación de confianza entre los proveedores, los responsables del tratamiento y los interesados.

[45] Tales normas incluyen las emitidas por la Organización Internacional de Normalización, el Consejo de Normas Internacionales de Auditoría y Aseguramiento y el Consejo de Normas de Auditoría del American Institute of Certified Public Accountants, en la medida en que estas organizaciones hayan establecido normas que cumplen los requisitos que figuran en el presente dictamen.

- Estas normas y certificaciones deben cubrir las medidas técnicas (como la localización de los datos o la codificación), así como los procesos seguidos por los proveedores de servicios de computación en nube para garantizar la protección de los datos (tales como políticas de control del acceso, controles de acceso o copias de seguridad).

4.3 Recomendaciones: evolución futura

El Grupo de Trabajo es plenamente consciente de que la complejidad de la computación en nube no puede resolverse totalmente a través de las garantías y soluciones que se exponen en el presente dictamen, que, sin embargo, aportan una buena base para asegurar el tratamiento de los datos personales que los clientes establecidos en el EEE someten a los proveedores. La presente sección tiene por objeto hacer hincapié en algunas cuestiones que deben abordarse a corto y medio plazo para mejorar las salvaguardias existentes y para ayudar al sector de la computación en nube a resolver los problemas planteados, garantizando al mismo tiempo el respeto de los derechos fundamentales a la intimidad y a la protección de datos.

- Un mejor equilibrio de las responsabilidades entre el responsable y el encargado: el Grupo de Trabajo se congratula de las disposiciones contenidas en el artículo 26 de la propuesta de la Comisión (proyecto de Reglamento general de protección de datos de la UE) que tiene como objetivo hacer que los encargados del tratamiento respondan en mayor medida frente a los responsables del tratamiento, ayudándoles a garantizar el cumplimiento de la normativa, en particular en materia de seguridad y obligaciones conexas. El artículo 30 de la propuesta introduce la obligación legal para el responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas. El proyecto de propuesta aclara que un encargado del tratamiento que no se atenga a las instrucciones del responsable del tratamiento será considerado responsable del tratamiento y estará sujeto a las normas específicas en materia de control conjunto. El GT 29 considera que esta propuesta va en la dirección adecuada para remediar el desequilibrio que a menudo caracteriza el medio de la computación en nube, en el que el cliente (especialmente si se trata de una PYME) puede experimentar dificultades a la hora de ejercer el control total, exigido por la legislación de protección de datos, sobre la forma en que el proveedor presta los servicios solicitados. Además, en vista de la asimetría de la situación jurídica de los interesados y los usuarios que sean pequeñas empresas frente a los grandes proveedores de computación en nube, se recomienda a los clientes y empresas comerciales que desempeñen un papel más dinámico a fin de negociar unas condiciones generales más equilibradas con los proveedores.
- Acceso a los datos personales con fines de seguridad nacional y de aplicación de la ley: es primordial que el futuro Reglamento prevea la prohibición, para los responsables del tratamiento que operan en la UE, de revelar datos personales a un país tercero si así lo solicita una autoridad judicial o administrativa de dicho país tercero, salvo autorización expresa derivada de un acuerdo internacional o de tratados de asistencia jurídica mutua, o salvo autorización de la autoridad de supervisión. El Reglamento (CE) nº 2271/96 del Consejo constituye un buen ejemplo de fundamento jurídico adecuado [46]. Este desequilibrio en la propuesta de la Comisión preocupa al Grupo de Trabajo, por cuanto implica una considerable pérdida de seguridad jurídica para los interesados cuyos datos personales se almacenan en centros de datos en todo el mundo. Por esta razón, el Grupo de Trabajo desearía subrayar [47] la necesidad de incluir en el reglamento el recurso

[46] Reglamento (CE) nº 2271/96 del Consejo, de 22 de noviembre de 1996, relativo a la protección contra los efectos de la aplicación extraterritorial de la legislación adoptada por un tercer país, y contra las acciones basadas en ella o derivadas de ella, DO L 309 de 29.11.1996 pp. 1-6, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:ES:HTML.

[47] Véase WP 191 - Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, página 23.

obligatorio a los tratados de asistencia jurídica recíproca en caso de divulgación de datos no autorizada por el Derecho de la Unión o de los Estados miembros.

- Precauciones especiales del sector público: cabe añadir una advertencia especial en cuanto a la necesidad de un organismo público de evaluar en primer lugar si la comunicación, tratamiento y almacenamiento de datos fuera del territorio nacional puede exponer a riesgos inaceptables la seguridad y privacidad de los ciudadanos y la economía y la seguridad nacional, en particular en el caso de bases de datos sensibles (por ejemplo, datos del censo) y servicios sensibles (por ejemplo, servicios de salud)[48]. Deberá prestarse esta especial consideración, en cualquier caso, siempre que se traten datos sensibles en la computación en nube. Desde esta óptica, podría estudiarse la posibilidad de que los Gobiernos nacionales y las instituciones de la Unión Europea investiguen más a fondo el concepto de una nube gubernamental europea como espacio virtual supranacional en el que podría aplicarse un conjunto de normas coherente y armonizado.
- Asociación Europea de Computación en Nube: el Grupo de Trabajo apoya la estrategia de la Asociación Europea de Computación en Nube (AECN) presentada por la Sra. Kroes, Vicepresidenta de la Comisión Europea, en enero de 2012 en Davos[49]. Esta estrategia implica la adjudicación de contratos públicos para estimular el mercado europeo de computación en nube. La transferencia de datos personales a un proveedor, obligado a respetar la legislación europea sobre protección de datos, podría suponer grandes ventajas para los consumidores en lo que respecta a la protección de datos, en particular mediante el fomento de la adopción de normas comunes (especialmente en materia de interoperatividad y portabilidad de datos), así como a la seguridad jurídica.

[48] A este respecto, la ENISA hace la siguiente recomendación en su documento sobre seguridad y resistencia en las nubes gubernamentales (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): «En cuanto a la arquitectura, para las aplicaciones sensibles las nubes privadas y comunitarias parecen ser la solución que mejor se adapta actualmente a las necesidades de las administraciones públicas, ya que ofrecen los mayores niveles de gobernanza, control y visibilidad, aunque a la hora de planificar una nube privada o comunitaria, deberá prestarse especial atención a la escala de la infraestructura».

[49] Neelie Kroes, Vicepresidenta de la Comisión Europea responsable de la Agenda Digital, Crear una Asociación Europea de Computación en Nube, Foro Económico Mundial, Davos, Suiza, 26 de enero de 2012, URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ANEXO

a) Modelos de implantación

La **nube privada**[50] es una infraestructura informática dedicada a una organización individual; está situada en las instalaciones de la organización o bien su gestión está subcontratada a un tercero (normalmente a través de alojamiento de servidores), bajo el control estricto del responsable del tratamiento. Una nube privada es comparable con un centro de datos convencional, con la diferencia de que se aplican disposiciones tecnológicas para optimizar la utilización de los recursos disponibles y mejorar estos recursos a través de pequeñas inversiones efectuadas de forma gradual.

Una **nube pública**, por el contrario, es una infraestructura propiedad de un proveedor especializado en la prestación de servicios que pone a disposición (y, por consiguiente, comparte) sus sistemas con los usuarios, empresas u órganos de la administración pública. Puede accederse a los servicios a través de Internet, lo que implica la transferencia de operaciones de tratamiento de datos o de datos a los sistemas del proveedor de servicios. Por tanto, el proveedor de servicios desempeña un papel clave por lo que se refiere a la protección eficaz de los datos almacenados en sus sistemas. Junto con los datos, el usuario está obligado a transferir una parte importante del control que ejerce sobre dichos datos.

A las nubes «públicas» y «privadas» se añaden las denominadas nubes «intermedias» o «híbridas», donde los servicios prestados por las infraestructuras privadas coexisten con los servicios adquiridos en nubes públicas. Conviene igualmente hacer referencia a las «nubes comunitarias», donde la infraestructura informática es compartida por varias organizaciones en beneficio de una comunidad de usuarios específica.

La flexibilidad y simplicidad de su configuración confieren a los sistemas en la nube una capacidad de dimensión «elástica», es decir, que estos sistemas pueden adaptarse a las necesidades específicas de conformidad con un enfoque basado en la utilización. Los usuarios no tienen que gestionar los sistemas informáticos, que se basan en acuerdos de externalización y, por tanto, son gestionados en su totalidad por el tercero en cuya nube se almacenan los datos. A menudo intervienen grandes proveedores con infraestructuras complejas; por esta razón la nube puede cubrir varios lugares y los usuarios pueden ignorar el lugar exacto donde se almacenan sus datos.

---

[50] En los Estados Unidos, el NIST (Instituto Nacional de Normas y Tecnología - National Institute of Standards and Technology) trabaja desde hace algunos años en la normalización de las tecnologías basadas en la nube y las definiciones que da se mencionan también en el documento de la ENISA:
Nube privada
La infraestructura de nube es utilizada por una sola organización. Puede estar gestionada por la organización o por un tercero, en el emplazamiento o fuera de él. Cabe señalar que una «nube privada» utiliza determinadas tecnologías que también son características de las «nubes públicas» como, en particular, las tecnologías de virtualización que favorecen la reorganización o la reforma de la arquitectura informática, como se ha explicado anteriormente.
Nube pública
La infraestructura en la nube se pone a disposición del público en general o de un gran grupo industrial, y pertenece a una organización que vende servicios en nube.

b) Modelos de prestación de servicios

En función de las necesidades de los usuarios, existen varias soluciones de computación en nube disponibles en el mercado. Pueden agruparse en tres categorías principales o «modelos de servicio» que suelen aplicarse a las soluciones en nube, tanto públicas como privadas.

- **IaaS («Cloud Infrastructure as a Service», infraestructura como servicio):** un proveedor alquila una infraestructura tecnológica, es decir, servidores remotos virtuales a los que puede recurrir el usuario final en virtud de mecanismos y disposiciones que hacen sencillo, eficaz y beneficioso sustituir a los sistemas informáticos de los locales de la empresa, o utilizar la infraestructura alquilada a la vez que dichos sistemas. Tales proveedores suelen ser operadores del mercado especializados y pueden basarse en una infraestructura física compleja que a menudo cubre varias zonas geográficas.
- **SaaS («Cloud Software as a Service», programa informático como servicio):** un proveedor proporciona en línea distintos servicios de aplicaciones y los pone a disposición de los usuarios finales. Estos servicios tienen a menudo por objeto sustituir las aplicaciones convencionales que instalan los usuarios en sus sistemas locales; en consecuencia, los usuarios están en última instancia destinados a externalizar sus datos al proveedor. Este es el caso, por ejemplo, de las aplicaciones ofimáticas típicas basadas en la web, como hojas de cálculo, herramientas de tratamiento de textos, agendas y registros informatizados, calendarios compartidos, etc. No obstante, los servicios en cuestión también incluyen aplicaciones de correo electrónico basadas en la nube.
- **PaaS («Cloud Platform as a Service», plataforma como servicio):** un proveedor ofrece soluciones de desarrollo avanzado y alojamiento de aplicaciones. Estos servicios suelen dirigirse a agentes del mercado que los utilizan para desarrollar y alojar soluciones basadas en aplicaciones propietarias para responder a necesidades internas o prestar servicios a terceros. De nuevo, los servicios prestados por un proveedor de PaaS hace innecesario que el usuario utilice equipos o programas específicos o adicionales a nivel interno.

Una transición plena a un sistema público en nube no parece viable a corto plazo por varias razones, en particular por lo que se refiere a grandes entidades como grandes empresas u organizaciones que tienen que cumplir obligaciones específicas – por ejemplo, los principales bancos, organismos gubernamentales, grandes municipios, etc. Esto puede explicarse básicamente por dos motivos: en primer lugar, factores dinámicos relacionados con las inversiones necesarias para realizar la transición; y en segundo lugar, la información especialmente valiosa o sensible que será tratada en casos específicos.

Otro factor en favor de la dependencia de nubes privadas (al menos en los casos mencionados) tiene que ver con la circunstancia de que ningún proveedor de nube pública puede garantizar siempre una calidad de servicio (sobre la base de acuerdos de nivel de servicio) capaz de responder a la naturaleza crítica del servicio prestado por el responsable del tratamiento, quizá porque el ancho de banda y la fiabilidad de la red no son suficientes o apropiadas en una zona determinada, o por lo que se refiere a las conexiones específicas entre el usuario y el proveedor. Por otro lado, cabe pensar razonablemente que se pueden alquilar nubes privadas en algunos de los casos mencionados (ya que esto podría resultar más rentable), o bien implantarse modelos híbridos (con componentes públicos y privados). Las correspondientes implicaciones deberían sopesarse cuidadosamente en cada caso.

En ausencia de normas acordadas a nivel internacional, existe el riesgo de que se desarrollen soluciones de computación en nube «personalizadas» o bien federadas, lo que implicaría un

mayor riesgo de cautividad (así como riesgos denominados «monocultivos de la protección de la intimidad»)[51] e impediría el pleno control de los datos sin garantizar la interoperatividad. Tanto la interoperatividad como la portabilidad de los datos son factores clave para el desarrollo de la tecnología de computación en nube, así como para permitir el pleno ejercicio de los derechos de protección de datos de los interesados (como el acceso o la rectificación).

Desde esta óptica, el actual debate sobre las tecnologías en nube es un importante ejemplo de la tensión existente entre los enfoques orientados a los costes y los orientados a los derechos, como se resume brevemente en el punto 2. Si bien basarse en una nube privada puede ser factible y aconsejable desde una perspectiva de protección de datos, habida cuenta de las circunstancias específicas del tratamiento, ello puede no ser viable para las organizaciones a largo plazo, principalmente por razón de los costes. Es preciso realizar una evaluación cuidadosa de los intereses en juego, puesto que actualmente no es posible señalar una solución única en este ámbito.

[51] Véase el estudio del Parlamento Europeo «Does it Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy» («¿Ayuda u obstaculiza? Promoción de la innovación en Internet y derecho de los ciudadanos a la intimidad», publicado en diciembre de 2011.