INFORME SOBRE LAS SANCIONES POR INCUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS DE LAS HIPERESCALARES DE SERVICIOS CLOUD

Conclusiones (apartado 9 del informe completo).

9.1. Aspectos generales.

PRIMERA: De acuerdo con lo expuesto, todas las empresas que presente servicios *"Cloud computing"* y traten datos personales de interesados de la Unión Europea bien como responsables, bien como encargadas del tratamiento, se encuentran sujetas al RGPD. Con carácter general, la externalización de los servicios de "*Cloud computing*" conlleva importantes ventajas, pero también es **cierto que, por sus características, presenta unos riesgos específicos que se deben afrontar mediante una adecuada elección del prestador de servicios.** Que tal como se ha evidenciado a lo largo del desarrollo del presente informe, los proveedores de Cloud Computing optan por modelos que han sido anulados por el TJUE, siendo deber de los entes y órganos de la administración pública, promover el derecho fundamental de las personas físicas a la protección de datos de carácter personal y no propiciar o fomentar dichas prácticas anuladas por el TJUE por parte de los prestadores de servicios de Cloud Computing.

Corresponde al responsable del tratamiento, es decir al usuario-cliente, cumplir todas las obligaciones impuestas por el RGPD, incluidas la responsabilidad proactiva. Es quien efectivamente posee el poder de decisión sobre el fin y los medios del tratamiento y elige al encargado que le ofrezca fiabilidad en la prestación del servicio *"Cloud*", por lo que responde por su actuación si aquel no ofrece las garantías apropiadas.

Al respecto, se debe tener en cuenta que los principales riesgos a los que se puede enfrentar una empresa a la hora de contratar servicios de *cloud computing* de una empresa estadounidense es la **falta de transparencia sobre las condiciones de prestación del servicio y la falta de control sobre el uso y la gestión de los datos** personales por parte de los agentes implicados en el servicio. Por tal motivo, se deben detallar cuantas medidas sean necesarias para asegurar un tratamiento adecuado por parte del encargado a la hora de contratar estos servicios. Por su parte, el encargado del tratamiento, proveedor del servicio *"cloud computing*" debe tratar los datos de acuerdo con lo establecido en el contrato y las instrucciones recibidas del responsable, ofreciendo las garantías adecuadas para aplicar las medidas técnicas y organizativas apropiadas, no sólo para cumplir con el RGPD, sino también, para garantizar la protección de los derechos de los interesados. **Si, en su caso, se llegase a demostrar que la función del encargado va más allá de cumplir las instrucciones y deberes que le corresponde, se lo considerará responsable del tratamiento con todas sus responsabilidades.** Por ello es importante que el rol de cada sujeto en el contrato de los servicios de *"cloud computing"* se encuentren claramente asignados para garantizar que las responsabilidades y consecuencias del incumplimiento de la normativa de protección de datos sean asumidas por cada parte. Recordemos que las infracciones contenidas en el RGPD conllevan la aplicación de sanciones importantes, según el sujeto y la causa por la que se concrete la infracción.

SEGUNDA: Cuando las grandes empresas tecnológicas estadounidenses prestan servicios *cloud*

realizan una transferencia de protección de datos. Para agilizar estas transferencias, la Unión Europea ha intentado, sin éxito, legitimar aquellas transferencias a través de la aprobación de Decisiones de adecuación -"*Safe Harbour y "Privacy Shield*- invalidadas por las sentencias del TJUE Scherms I y Schrems II, respectivamente. En sustitución de ambas Decisiones se aprobó, recientemente por la Comisión la Decisión EU-EEUU DPF que ha sido criticada por no cumplir efectivamente con las exigencias señaladas del TJUE. Cabe destacar en este sentido que el problema de fondo se encuentra en la diferente **concepción que existe del Derecho a la protección de datos en Estados Unidos respecto de Europa**. Para aquel país, la protección de datos se materializa a través de distintas normas de carácter sectorial que protegen a los consumidores. **No tiene la consideración de Derecho fundamental ni tampoco existe una norma federal que lo proteja.** Por el contrario, existen distintas normas – en particular FISA y *Cloud Act*- que permiten a las autoridades de inteligencia y de seguridad del gobierno acceder en masa o de forma discriminada a datos personales sin ningún tipo de control. Además, se reconoce al Presidente estadounidense la potestad para modificarlas por decreto o para aprobar decretos secretos. Los ciudadanos tampoco pueden ejercer sus derechos de acceso y rectificación y obtener una resolución motivada al respecto. Además, no existe una vía judicial independiente en la materia.

TERCERA: La reciente Decisión EU-EEUU DPF aprobada recientemente por la Comisión ha sido valorada negativamente tanto por el Comité Europeo de Protección de Datos como por el Parlamento Europeo y **la organización NOYB fundada por Schrems señala que impugnará la misma ante el TJUE.** Por su parte, las instancias europeas consideran que la aprobación por parte de Estados Unidos de un nuevo marco jurídico si bien supone alguna mejora, no cumple las exigencias reiteradamente señaladas por las instituciones mencionadas. Estas consideran que el respeto a la vida privada y familiar y la protección de datos personales son derechos fundamentales en tanto trasunto en la materia de la dignidad de la persona. Por ello mismo, la Decisión de adecuación que se adopte debe ser una "decisión jurídica", "no política". **Los Derechos fundamentales nunca pueden ser objeto de ponderación con respecto a intereses comerciales o políticos, sino únicamente, con otros derechos fundamentales.** En este marco supremo se considera que no puede recaer en los ciudadanos de la Unión Europea la carga de recurrir ante el TJUE para proteger este derecho fundamental.

CUARTA: Los "responsables del tratamiento" siempre deben responder por el cumplimiento de las obligaciones en materia de protección de datos, pero dicho cumplimiento "no sólo exige cumplir" la normativa sino, también, "demostrar que se cumple" en todos los tratamientos como responsable, con independencia de la naturaleza, el alcance, el contexto, los fines y los riesgos para los interesados.

QUINTA: La valoración de la adecuación de un tercer país no sólo se debe fundar con base en la legislación y las prácticas vigentes en el momento de adoptar la Decisión de adecuación. **Antes al contrario, se debe garantizar que existen mecanismos claros y estrictos de seguimiento y de revisión para garantizar que la evolución jurídica y la práctica en los Estados Unidos** cumple con las exigencias de los derechos fundamentales a la vida privada y a la protección de datos.

SEXTA: Es preciso destacar que la Decisión de adecuación vigente plantea dudas sobre el cumplimiento de las exigencias del RGPD. Por tanto, las empresas que han contratado estos servicios se encuentran en una situación de inseguridad jurídica, y corresponde que ofrezcan garantías adecuadas al respecto.

SÉPTIMA: Es preciso señalar que al margen de que la UE quiera fortalecer y asegurar las relaciones y el comercio con EEUU, la Comisión debe centrase en trabajar para concretar un régimen jurídico, de normalización y de estrategia industrial, que permita afianzar y apoyar a las empresas europeas

proveedoras de estos servicios *"cloud computing*" para que, como propuso en su día Francia, permita preservar la independencia para para que los poderes públicos, pero también determinadas instituciones privadas claves para un país, puedan utilizarlas con garantía del cumplimiento del RGPD. No es posible olvidar que estas empresas ofrecen un impulso europeo importante en torno a la gobernanza de los datos y los servicios digitales que tanto insisten las distintas instituciones de la UE, como el Parlamento o la Comisión. Esta apuesta, **además de cumplir con las exigencias jurídicas, también persigue objetivos geoestratégicos y económicos como el desarrollo de una industria europea capaz de prestar estos servicios, así como el fomento de desarrollo de otros nuevos, garantizando también el nivel de seguridad exigido** por la UE así como la accesibilidad a los datos.

OCTAVA: La Administración Pública debe respaldar a empresas europeas que demuestren un compromiso estricto con la normativa de protección de datos al proporcionar servicios de computación en la nube, de este modo, no solo fortalece la confianza en la seguridad y privacidad de los datos, sino que también fomenta un ambiente empresarial más competitivo y equitativo en el sector de la computación en la nube.

La promoción activa de estas compañías europeas a través de políticas de contratación y fomento empresarial contribuye a diversificar el mercado y reduce la dependencia de proveedores estadounidenses. Asimismo, al hacerlo, se contrarrestan posibles prácticas abusivas por parte de empresas extranjeras al establecer estándares más altos en términos de protección de datos y seguridad. Estas medidas son esenciales para salvaguardar la privacidad de los ciudadanos europeos y fortalecer la posición de la Unión Europea en el ámbito de la tecnología y la innovación.

NOVENA: Paraunagestióneficientederecursosenun Estadosocialrequiereunaestrategia de datos precisa por parte de la Administración Pública. La propuesta de la Comisión Europea para crear un espacio único de datos demuestra la importancia vital de esta materia en la economía digital y el crecimiento.

Para salvaguardar derechos y la soberanía, es esencial reducir la dependencia de proveedores no europeos en el procesamiento de datos. Esto exige un enfoque que proteja los derechos fundamentales, a diferencia de otros modelos existentes, para ello, resulta crucial promover el desarrollo de empresas europeas y evitar la dependencia de servicios de empresas estadounidenses por parte de las Administraciones Públicas. Esto no solo garantiza la seguridad de los datos personales de los ciudadanos europeos, sino que también facilita la ejecución de una estrategia de datos europea y española en un contexto global.

9.2. Aspectos específicos referidos a las transferencias internacionales de datos.

DÉCIMA: Ni Amazon Web Services ni Google Cloud cuentan con una Política de Privacidad en sentido estricto. La primera de ellas dispone solamente de un Aviso de Privacidad; Google Cloud pone a disposición del usuario o del cliente diferentes documentos referidos a la privacidad, pero no los sistematiza o aúna en un mismo documento. Además, en el caso de Google, la información disponible está redactada en inglés con la consecuencia de vulnerar el RGPD, dado que no permite la manifestación del consentimiento de acuerdo con los requisitos señalados en el artículo 4.11 de la misma norma. Tal circunstancia podría ser considerada, incluso, una infracción del principio de transparencia consagrado en el artículo 12 del RGPD, conforme a las Directrices del Grupo de Trabajo del Artículo 29.

UNDÉCIMA: Tanto Microsoft Azure y Google Cloud detallan ciertas medidas de garantía adoptadas

en relación con las transferencias internacionales de datos, pero Amazon Web Services realiza menciones al "*Privacy Shield"* que pueden inducir a error dado que dicho fuero fue anulado por el TJUE. Además, salvo Google Cloud, el resto de proveedores no menciona la posibilidad cierta de que los datos almacenados en la nube puedan ser requeridos por las autoridades estadounidenses, a pesar de estar obligados a ello de conformidad con el Cloud Act.

Madrid, Noviembre de 2023

AUTORES**.-**

- **Sor Arteaga.-** PhD Doctora en Derecho. Abogada colegiada No 105.096 del ICAM DPO. Especialista en Protección de Datos, Telecomunicaciones y IT. Dispone de más de 15 años de experiencia en el asesoramiento y consultoría a operadores nacionales e internacionales en materia de derecho de las telecomunicaciones, Es miembro del Grupo de Investigación en Gobierno, Administración y Políticas Públicas en España y Latinoamérica (GIGAPP),
- **Antonio Troncoso Reigada.-** Doctor en Derecho por la Universidad de Bolonia (con calificación summa cum laude). Posee un profundo conocimiento en áreas como la protección de datos, la regulación de las tecnologías de la información y la administración pública y ha desempeñado roles clave en organismos y comités.
- **Maria Nieves de la Serna Bilbao**.- Ph.D. en Derecho Administrativo y Profesora Titular de Universidad. Entre sus publicaciones se encuentran "La privatización en España: Fundamentos Constitucionales y Comunitarios", "Derecho de la Edificación. Instituciones básicas", y contribuciones en obras de referencia sobre Derecho Urbanístico y de las Telecomunicaciones
- **Iñaki Vicuña de Nicolás** es Licenciado en Derecho por la Universidad de Deusto y actualmente se desempeña como Letrado Mayor del Consejo General del Poder Judicial, así como Director del Centro de Documentación Judicial (CENDOJ) desde 2012. Entre sus roles anteriores se destaca su posición como Director de la Agencia Vasca de Protección de Datos (2004-2012) y como Letrado del Consejo General del Poder Judicial (1997-2004). Asimismo, ha representando a España en el Comité Consultivo del Convenio para la protección de personas respecto al tratamiento automatizado de datos de carácter personal.