

Comentarios de CCBE sobre la revisión del Acuerdo del Escudo de privacidad UE-EE.UU

25/09/2017

El Consejo de la Abogacía Europea (CCBE) representa a las Abogacías de 45 países, y a través de ellos a más de un millón de abogados europeos.

Antes de la primera revisión anual del Escudo de la Privacidad en septiembre de 2017, CCBE desea instar a la Comisión Europea a suspender su Decisión de implementación 2016/1250 sobre la adecuación de la protección proporcionada del escudo de privacidad por la Unión Europea y Estados Unidos sobre la base de que los EE.UU no garantizan un nivel de protección de los datos personales esencialmente equivalente al garantizado por la Unión Europea.

Fondo:

El 6 de octubre de 2015, el Tribunal de Justicia de la Unión Europea, dictó sentencia en el asunto Schrems contra el Comisario de Protección de Datos (C-362/14), que invalida la Decisión 2000/520/CE sobre la idoneidad de la protección proporcionada por los principios de privacidad en materia de seguridad.

Como resultado de esa sentencia, el 2 de febrero de 2016, la Comisión Europea y el gobierno de EEUU llegaron a un acuerdo político sobre un nuevo marco para el comercio transatlántico de datos personales con fines comerciales: Escudo de privacidad entre la Unión Europea- EEUU.

La Comisión Europea adoptó el 12 de Julio de 2016, una decisión de aplicación relativa a la adecuación de la protección proporcionada por el escudo de privacidad de la Unión Europea-EEUU reforzando la necesidad de protección de datos de una manera sustancialmente equivalente a la prevista por la legislación de la UE. A este respecto, la Comisión examinó la Ley de reparación judicial de los Estados Unidos de 4 de noviembre de 2015, que extiende a los nacionales de la UE, entre otras, las garantías concedidas a ciudadanos y residentes estadounidenses sobre el uso de datos personales por las agencias federales bajo la Ley de Privacidad, como un importante paso adelante y una salvaguarda importante.

Cabe recordar que, en su declaración de 29 de julio de 2016, en su artículo 29, el grupo de trabajo sobre protección de datos expresó reservas del escudo de privacidad con respecto al acceso de las

autoridades públicas estadounidenses a los datos transferidos de la UE. Destacó los problemas relacionados con la falta de independencia y poder del Defensor del Pueblo, y la falta de garantías concretas que prohíban a los servicios de inteligencia estadounidenses realizar una recopilación masiva e indiscriminada de datos personales.

En los asuntos acumulados Tele2 Sverige AB contra Post-och telestyrelsen (C-203/15) y el Secretario de Estado del ministerio de interior contra Watson y otros (C- 698/15) de 21 de diciembre de 2016, el TJUE dio una nueva indicación de las restricciones que la legislación debe imponer para el acceso a los datos conservados con el fin de cumplir con la Carta de los Derechos Fundamentales de la UE.

Por el momento, el escudo de privacidad tiene pendientes dos apelaciones presentadas por asociaciones frente al Tribunal General de la UE.

Las preocupaciones de CCBE con respecto a la legitimidad del Escudo de Privacidad.

Teniendo en cuenta los estándares que han sido identificados por el TJUE sobre la base de los derechos fundamentales y libertades garantizados por derecho de la UE, CCBE considera que el escudo de privacidad entre la UE-EEUU tiene un serie de deficiencias importantes que generan preocupación por su legitimidad, principalmente en lo que respecta a la falta de salvaguardas contra amplios programas de vigilancia de los EE.UU.

En este respecto, CCBE hizo unas [recomendaciones](#) sobre la protección de confidencialidad del cliente en el contexto de actividades de vigilancia, las cuales fueron adoptadas el 28 de Abril de 2016. Este documento estableció los estándares que deberían sostenerse para asegurar que los principios del secreto profesional y del privilegio legal profesional, no son determinados por el Estado mediante prácticas relativas a la interceptación de comunicaciones y el acceso a los datos de los abogados con el objetivo de vigilar y aplicar la ley. Posteriormente, se resumen de forma breve las principales preocupaciones:

Falta de control legislativo vinculante

Todas las actividades de vigilancia necesitan ser reguladas con la adecuada especificación y transparencia para evitar los riesgos del desprecio arbitrario por los derechos humanos.¹ En este respecto, el escudo de privacidad solo se refiere, por ejemplo a las “Directrices y Políticas del departamento de justicia”. Como base jurídica de normas claras, precisas y accesibles, estas políticas y directrices no pueden considerarse como una forma de control legislativo vinculante. Además, el término “seguridad nacional” en el escudo de privacidad no está circunscrito con especificidad adecuada como para garantizar que las infracciones de protección de datos puedan ser revisadas efectivamente en los tribunales para asegurar el cumplimiento de un estricto test de lo que es necesario y proporcional.

Mecanismos de supervisión judicial e independiente

Toda injerencia en los derechos fundamentales a la privacidad y la protección de datos debe ser supervisada por un órgano judicial, que es financieramente y políticamente independiente del ejecutivo y debe ser inamovible porque solo un juez puede ofrecer las garantías necesarias de independencia. En las recomendaciones, se mencionan numerosos requisitos² relativos a la naturaleza

¹ CCBE Recomendaciones puntos 2.1-2.4, pags 19-20.

² CCBE Recomendaciones puntos 4.1-.4.7, pags 22-24.

de supervisión o al mandato del órgano de supervisión que debe cumplir el órgano de supervisión antes de que el control de las actividades de vigilancia pueda considerarse satisfactorio.

En primer lugar, las recomendaciones estipulan que el control de supervisión debe confiarse a un órgano judicial, que es políticamente y económicamente independiente del poder ejecutivo y debe ser inamovible.³ El marco legal del mecanismo de supervisión en el escudo de privacidad es de múltiples capas y consta de dos partes principales: la supervisión interna y externa. Al parecer, ninguno de los órganos de supervisión interna puede ser financieramente y políticamente independiente del poder ejecutivo porque, básicamente, es parte de él, por lo tanto, la supervisión interna no cumplirá con el requisito de control de supervisión como se ha indicado anteriormente. Bajo el escudo de privacidad, la supervisión externa está proporcionada porque se dice que son órganos judiciales⁴, incluidos los comités de inteligencia del Congreso y la Junta de Supervisión de la Libertad de Privacidad y Libertades Civiles. Estos dos últimos no son órganos judiciales, por lo que el requisito de control de supervisión solo puede ser cumplido por el Tribunal de la FISA. Sin embargo, cabe señalar que el procedimiento ante este tribunal es ex parte, lo que significa que las personas no pueden ser oídas, o incluso no puede ser conocedoras del caso.

También hay que destacar que las características de una determinada actividad de vigilancia dependen de la base jurídica que se invoca cuando se realizan programas de vigilancia. Por ejemplo, las actividades de vigilancia realizadas sobre la base de la Sección 215 de la Ley de Vigilancia de Inteligencia Extranjera están casi totalmente sujetas a una supervisión judicial a priori por el Tribunal de la FISA. Por el contrario, las actividades de vigilancia realizadas sobre la base de la Orden Ejecutiva 12333 no están sujetas a ninguna revisión judicial, ni a priori, ni a posteriori.

Para cumplir con su mandato, la ley debe otorgar a la entidad de supervisión poderes proporcionados, adecuados y vinculantes. Estas competencias deben permitir al organismo tomar decisiones plenamente informadas y ejecutables.⁵ Sin embargo, el escudo de privacidad sólo especifica la competencia bastante limitada del Defensor del Pueblo, e incluso si se considera a este como un órgano de supervisión (lo cual no está claro), es evidente que el Defensor del Pueblo carece de poderes efectivos y solo puede solicitar medidas adicionales por parte del órgano gubernamental apropiado de los EEUU o solicitar información a otras entidades gubernamentales.

También hay que subrayar que si el órgano de control no tiene por lo menos el poder de poner fin la vigilancia ilícita, entonces ese órgano no puede cumplir suficientemente su mandato. Un órgano de control solo puede adoptar decisiones ejecutorias si puede ordenar a las autoridades que cese y suspenda la vigilancia ilegal u ordene la destrucción permanente de la información obtenida mediante la vigilancia directa e indirecta.

Falta de recursos legales eficaces

A fin de proporcionar una protección jurídica eficaz contra la vigilancia ilícita, es necesario que los recursos jurídicos se pongan a disposición de los abogados y sus clientes que han sido objeto de una vigilancia ilegal. El Gobierno de los Estados Unidos no tiene en consideración las protecciones de la Constitución de los EEUU, que prohíbe búsquedas e incautaciones “irrazonables” e impone un requisito de autorización para prevenir tales acciones, como extenderlo a personas no estadounidenses que se encuentran fuera de los Estados Unidos. Por lo tanto, en el contexto de la vigilancia de la inteligencia,

³ CCBE Recomendaciones punto 4.2-4.3, pag 22.

⁴ Anexo VI del escudo de privacidad invoca la Ley de Vigilancia de Inteligencia Extranjera Sección 702.

⁵ Recomendaciones punto 4.7, pag 14.

las personas de la UE que no son estadounidenses no se benefician de estas protecciones constitucionales, mientras que en la UE, cualquiera puede acudir a los tribunales si tienen una razón legítima para sospechar una injerencia de sus derechos fundamentales, independientemente de su ciudadanía.

Aunque el Escudo de privacidad destaca en general que hay recursos judiciales administrativos disponibles para los individuos en los Estados Unidos, esto ha sido seriamente cuestionado por la Orden Ejecutiva 13768 mejorando la Seguridad Pública en el Interior de los Estados Unidos.

La orden específicamente establece que las disposiciones de la Ley de Privacidad ya no se aplicarán a aquellos “que no sean ciudadanos de los Estados Unidos o residentes permanentes legales”. Por lo tanto, las garantías y recursos de la Ley de privacidad no beneficiarían a los ciudadanos de la UE que no sean residentes permanentes legales en los Estados Unidos. En consecuencia, este Decreto parece superar garantías otorgadas durante las discusiones sobre el Escudo de Privacidad.

La orden también permite a la Agencia de Seguridad Nacional compartir grandes cantidades de datos personales de personas no estadounidenses con otras 16 agencias gubernamentales sin ningún mandato, decisión judicial o autorización del Congreso.

El Congreso también ha autorizado a los proveedores de servicios de internet a vender los datos personales de sus suscriptores, incluida la historia y otra información privada, sin su consentimiento.

Dado que una Orden Ejecutiva tiene un estatus inferior al de un estatuto en el sistema jurídico de los Estados Unidos, se podría argumentar que la Orden de 25 de enero de 2017 no debe considerarse que pone en entredicho la Ley de reparación judicial de 4 de noviembre de 2015.

Sin embargo, esta Orden muestra, como mínimo (i), la intención del ejecutivo estadounidense de revertir las garantías otorgadas anteriormente a los ciudadanos de la UE con respecto a la protección de sus datos personales, (ii) plantea la preocupación de que, en la práctica, las autoridades gubernamentales estadounidenses directamente dependientes del ejecutivo buscan anular los compromisos asumidos durante la Presidencia de Obama hacia la UE, y (iii) expone a los ciudadanos de la UE al uso no autorizado de sus datos personales, ningún recurso efectivo.

En una declaración de 15 de febrero de 2017, el grupo de Trabajo sobre protección de datos del artículo 29, indicó que había enviado una carta a las autoridades de los Estados Unidos solicitando una aclaración sobre el impacto de esta orden en el escudo de privacidad. No se sabe si las autoridades de los Estados Unidos han respondido ya que no se hizo pública ninguna respuesta.

Jan Phiipp Albrecht, ponente para la protección de datos del Parlamento Europeo, se alarmó por la situación y declaró: “Si esto es cierto, la Comisión Europea debe suspender inmediatamente el Escudo de Privacidad y sancionar a Estados Unidos por romper el acuerdo paraguas entre UE-EEUU.

Revisión del Escudo de Privacidad

En virtud del artículo 4 del Escudo de Privacidad, que entró en vigor el 1 de agosto de 2016, se prevé una revisión anual del sistema.

El párrafo 5 del artículo 35 del Reglamento Europeo para la protección de Datos Generales (GDPR) establece que la competencia de la Comisión podrá derogar, modificar o suspender su decisión sobre la adecuación “cuando la información disponible revele, en particular tras la revisión mencionada en el párrafo 3 del presente artículo, que un tercer país, un territorio o uno o más sectores determinados

de un tercer país o una organización internacional ya no garantice un nivel adecuado de protección en el sentido del apartado 2 del presente artículo.

El 12 de Julio, la Comisaria de Justicia, Vera Jourová, pronunció un discurso ante la delegación del Parlamento Europeo para las relaciones con los Estados Unidos sobre como reevaluar el Escudo de Privacidad. Alentó el mantenimiento del Escudo de Privacidad, siempre que se mantuvieran las garantías sobre las que se construyó, en particular, el Defensor del pueblo encargado de atender las quejas de los ciudadanos contra la injerencia de las autoridades estadounidenses y las garantías contenidas en la Directiva Política Presidencial 28, implementado por la administración Obama. La Comisario no mencionó el impacto de la Orden Ejecutiva de 25 de enero de 2017 sobre la protección de los datos personales de los ciudadanos europeos.

Como parte de esta reevaluación anual, el CCBE invita a la Comisión a ejercer sus facultades en virtud del párrafo 5 del artículo 45 del GDPR con el fin de suspender el escudo de privacidad. En vista de las preocupaciones expuestas más arriba sobre la legitimidad del Escudo de Privacidad, parece – en particular- tras el Decreto del 25 de enero de 2017- que los Estados Unidos ya no protegen adecuadamente los datos personales de los ciudadanos de la UE.

La renegociación del acuerdo de Escudo de privacidad requerirá fuertes salvaguardias de protección de datos de Estados Unidos, especialmente en lo que respecta al acceso a datos personales por parte de las autoridades públicas y el proceso de certificación de las empresas estadounidenses.