EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

CCBE Evaluación de CLOUD Act de EE.UU.

28/02/2019

El Consejo de la Abogacía Europea (CCBE) representa a las Abogacías de 45 países, y a través de ellas, a más de 1 millón de abogados europeos. CCBE responde regularmente en nombre de sus miembros sobre cuestiones políticas que afectan a los ciudadanos y abogados europeos.

En este documento, CCBE presenta su análisis de la "Clarifying Lawful Overseas Use of Data Act" (*CLOUD Act*) de los Estados Unidos (EE.UU.) y evalúa en qué medida sus disposiciones son coherentes con la legislación europea.

A. Resumen de las disposiciones legales CLOUD

El 22 de marzo de 2018, el Congreso de los Estados Unidos aprobó *CLOUD Act*, que modifica el Código de los Estados Unidos de América con el fin de insertar disposiciones nuevas o modificadas para el acceso del Gobierno de los Estados Unidos a los datos almacenados fuera de dicho territorio y el acceso de los gobiernos extranjeros a los datos almacenados dentro de los EE.UU. La ley fue aprobada sin ningún escrutinio real como parte de la Ley de Asignaciones de 2018, una medida general.

Lo más importante desde una perspectiva europea es que *CLOUD Act* modifica el capítulo 121 del título 18 del Código de los Estados Unidos, añadiendo al Código un nuevo artículo §2713 con el título de "preservación necesaria y la divulgación de las comunicaciones y los registros".

La adición establece que la SCA ("Stored Communications Act – Ley de Comunicaciones Almacenadas") también se aplica a los datos almacenados fuera de la EE.UU. La SCA ha introducido el §2703 y siguientes al Código de los EE.UU. en 1986 con el objetivo de imponer obligaciones de confidencialidad estatutarias sobre los proveedores de información y prescribir las circunstancias en las que el gobierno puede obligar a revelar las comunicaciones electrónicas almacenadas a distancia[1]. La disposición más importante de la SCA para una mejor comprensión de *CLOUD Act* es el §2703 del Código de los Estados Unidos. Esta disposición describe en detalle las reglas bajo las cuales una entidad gubernamental puede requerir la divulgación por parte de un proveedor y las formas en que se puede acceder a dichas comunicaciones, ya sea mediante la obtención de una orden emitida de conformidad con las Normas Federales del Procedimiento Penal (sin previo aviso al suscriptor o cliente) o mediante la utilización de una citación u orden judicial (con notificación a la persona afectada), cf. §2703(b) (1) (A-B). Dado que la notificación al suscriptor o cliente suele ser indeseable, la evaluación jurídica de las disposiciones del *CLOUD Act* que sigue se basará en el supuesto de que la revelación se solicitará normalmente mediante una orden judicial.

El impulso inmediato para la adopción del *CLOUD Act* ha sido el asunto Microsoft Warrant (EE.UU. contra Microsoft, asunto 17-2 del Tribunal Supremo de los Estados Unidos) que buscaba determinar

[1] 1 cf. S. REP. 99-541, 5, 1986 U.S.C.C.A.N. 3555, 3559.

si la recuperación por el gobierno de los EE.UU. de los datos almacenados en el extranjero constituía una "búsqueda nacional" legal en virtud de la ley en cuestión, siendo el caso de que era posible recuperar estos datos teniendo acceso a ellos desde una terminal informática situada en EE.UU. El Gobierno norteamericano ha sostenido que lo había hecho, pero Microsoft (que ha ganado ante la *Circuit Court of Appeals* de los EE.UU.) ha hecho valer que no lo había hecho y ha sido apoyado delante del Tribunal Supremo americano por un determinado número de *Amici curiae* (incluido CCBE) que también presentaron informes[2]. Tras la conclusión de los alegatos y mientras que el Tribunal tomaba la decisión, se promulgó el *CLOUD Act* y el gobierno de los EE.UU. abandonó su apelación, dejando la interpretación correcta del *CLOUD Act* en suspenso. Ahora, el nuevo artículo §2713 del Código de los Estados Unidos indica:

> "Un proveedor de servicios de comunicación electrónica o de servicios informáticos a distancia [i.e en particular la informática en la nube] tiene que conformarse con la obligación del presente capítulo §§2703 y siguientes] de preservar, salvaguardar o divulgar el contenido de una comunicación por cable o electrónica y todo registro e información perteneciente a un cliente o suscriptor en posesión, custodia o control de dicho proveedor, independientemente de si dicha comunicación, registro u otra información se encuentra dentro o fuera de los Estados Unidos".

El §2703 del Código de los Estados Unidos permite a toda entidad gubernamental americana a emitir un mandato a fin de exigir la divulgación prevista del artículo §2713 de los EE.UU. En el caso de que un "proveedor de servicios de comunicaciones electrónicas o de servicios informáticos a distancia" fijado en los EE.UU. reciba una orden, el artículo §2703 prevé una vía de recursos por la que puede exigir que dicha orden sea declarada inválida (anulada) o modificada por un tribunal americano (artículo §2703 (h) (2) requisitos para la anulación o modificación).

El proveedor debe presentar la solicitud correspondiente dentro de los 14 días siguientes a la entrega de la orden demostrando lo siguiente:

> "(i) que el cliente o el abonado no sea un extranjero de los EE.UU. y que no reside en los EE.UU.; y
>
> (ii) que la divulgación requerida supondría un riesgo importante de que el proveedor violara las normas de un gobierno extranjero cualificado" (§2703 (h) (2) del Código de los Estados Unidos)"

Se entiende por "gobierno extranjero cualificado" cualquier gobierno extranjero que concluyera un acuerdo ejecutivo con los EE. UU., ver §2703 (h) (1).

El Tribunal que se ocupe de la cuestión podrá aprobar la solicitud del proveedor, previa audiencia del Gobierno de los Estados Unidos, si lo considera oportuno necesario:

> "(i) la revelación requerida induciría al proveedor a violar las leyes de un gobierno extranjero que reúne los requisitos;
>
> (ii) habida cuenta de todas las circunstancias, el interés de la justicia exige que el proceso judicial es enmendado o cancelado; y
>
> (iii) el cliente o suscriptor no es nacional de los Estados Unidos y no reside en los Estados Unidos. (§ 2703 (h) (2) (B) Código de los Estados Unidos)"

El apartado (ii) requiere un "análisis de cortesía" (comity analysis) basado en otros ocho criterios que el Tribunal debe considerar:

> "(A) los intereses de los Estados Unidos, incluyendo los intereses de investigación de la entidad gubernamental que busca la divulgación;

[2] Memoria CCBE como amicus curiae en apoyo al demandado Microsoft Irlanda

(B) el interés del gobierno extranjero elegible para prevenir cualquier divulgación prohibida;

(C) la probabilidad, alcance y naturaleza de las sanciones impuestas al proveedor o a sus empleados como resultado de los requisitos legales incompatibles impuestos al proveedor;

(D) la ubicación y nacionalidad del abonado o cliente cuyas comunicaciones son buscado, si se conoce, así como la naturaleza y el alcance en los Estados Unidos [...];

(E) la naturaleza y el alcance de la relación y presencia del proveedor en los Estados Unidos;

(F) la importancia para la investigación de la información que debe divulgarse;

(G) la probabilidad de un acceso oportuno y efectivo a la información que debe divulgarse por medios que causen consecuencias negativas menos graves; y

(H) si el procedimiento legal [es decir, la orden judicial] se ha solicitado en nombre de una autoridad extranjera de conformidad con el §3512, los intereses de la autoridad extranjera que hace la solicitud de asistencia. "(§2703 (h) (3) Código de los Estados Unidos)"

Los destinatarios potenciales del artículo §2713 son empresas de Internet como Google, redes sociales como Facebook, Instagram y Twitter, así como proveedores de tecnología en la nube, registros de nombres de dominio, registradores y "mercados digitales" que permiten a los consumidores o comerciantes realizar transacciones de igual a igual[3].

El artículo §2713 del Código de los EE.UU., a primera vista, sólo se aplica a compañías con sede en los Estados Unidos. Sin embargo, las órdenes extraterritoriales de los Estados Unidos podrían aplicarse a las empresas extranjeras si existe un vínculo jurisdiccional suficiente. Por ejemplo, el servicio de mensajería de Telegram, aunque no sea una entidad americana, podría estar sujeta a una orden judicial ya que sirve a clientes americanos[4].

B. Cambios positivos resultantes de *CLOUD Act*

CCBE considera como un avance positivo que el acceso de los gobiernos a los datos almacenados fuera de los Estados Unidos se basa ahora en un marco legal establecido que también define los procedimientos por los que los prestadores de servicios pueden impugnar una orden. Esto crea un mayor grado de seguridad jurídica para los prestadores de servicios que bajo el antiguo régimen SCA, exigía a los proveedores que tomaran medidas legales para evitar tener que tratar con cumplir con una orden (como, por ejemplo, en el caso de las órdenes de Microsoft).

Además, CCBE reconoce el incentivo (ver artículo §2523 del Código de los Estados Unidos enmendado) para gobiernos extranjeros para celebrar acuerdos ejecutivos con los Estados Unidos sobre el acceso a los datos relativo a los nacionales o a los residentes permanentes de EE.UU. Por acuerdos ejecutivos bajo el § 2523 del Código de los Estados Unidos, los proveedores de servicios están autorizados a responder a las solicitudes de información de gobiernos extranjeros, lo que facilita las solicitudes transfronterizas de información. Aunque, en principio, CCBE acoge con satisfacción estos avances hacia la normalización de los procesos transfronterizos, siguen siendo una verdadera preocupación, en particular debido al enfoque unilateral adoptado por la legislación.

C. Preocupaciones generales sobre *CLOUD Act*

I. Procedimiento legislativo abreviado

CLOUD Act no ha sido objeto de ninguna audiencia en comisión, ni en la Cámara de Representantes ni en el Senado. CCBE considera que este procedimiento legislativo truncado es particularmente

[3] https://www.eff.org/de/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom .
[4] https://www.eff.org/de/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom#_ftn1.%20

sorprendente, dado que la misma cuestión jurídica fue fuertemente cuestionada en el caso de *Microsoft* ante el Tribunal Supremo.

El Tribunal Supremo tuvo que tratar numerosas memorias de amicus curiae que contenían argumentos sólidos tanto a favor como en contra de la legitimidad de la orden de divulgación en cuestión[5]. Aunque la cuestión de la necesidad de una evaluación jurídica de la solicitud se ha llevado ya a cabo por *CLOUD Act* la complejidad de los hechos de estas solicitudes no ha cambiado. Por lo tanto, CCBE hubiera querido que *CLOUD Act* hubiera sido objeto de un debate más exhaustivo.

II. Jurisdicción extraterritorial

CLOUD Act otorga a los organismos encargados de hacer cumplir la ley, jurisdicción ilimitada para todos los datos controlados por un proveedor de servicios con factores de conexión con los Estados Unidos (véase más arriba).

Por lo tanto, los procedimientos bien establecidos para facilitar el acceso a los datos personales almacenados fuera de la jurisdicción de un país, como los tratados de asistencia judicial recíproca, se ignoran y los esfuerzos para adaptarlos a los nuevos desafíos se ven socavados. CCBE considera que se trata de una evolución no deseable y sugiere que sería más apropiado que las normas y procedimientos para el acceso de organismos encargados de hacer cumplir la ley almacenados en jurisdicciones extranjeras se formularan por consenso y mediante acuerdos internacionales.

El Parlamento Europeo abordó la cuestión en su resolución sobre la ciberdelincuencia declarando "la preocupación por el alcance extraterritorial de la acción de las autoridades encargadas de hacer cumplir la ley que necesitan tener acceso a los datos en el contexto de las investigaciones penales y subrayando la necesidad de aplicar normas estrictas a este respecto"[6].

al tiempo que se pide a la Comisión Europea que se oponga a

> "la apropiación de la jurisdicción extraterritorial por parte de terceros países"

De manera más concreta, el Parlamento Europeo expresó su preocupación el 5 de julio de 2018, observando que el *CLOUD Act*

> "amplía la competencia de las autoridades estadounidenses y extranjeras encargadas de la aplicación de la ley permitiéndoles identificar y acceder a datos personales más allá de las fronteras internacionales sin recurrir a los instrumentos de asistencia jurídica mutua (MLAT), que proporcionan las garantías adecuadas y respetan la jurisdicción judicial de los países en cuyo territorio se almacena la información"[7].

y consideró que

> "una solución más equilibrada habría sido fortalecer el actual sistema internacional de tratados de asistencia judicial recíproca a fin de fomentar la cooperación internacional y judicial; [en particular porque], tal y como prevé el artículo 48 del Reglamento General sobre la Protección de Datos, la asistencia judicial mutua y otros tratados internacionales constituyen un mecanismo privilegiado para permitir el acceso a los datos personales en el extranjero".[8]

---

[5] *Ibid*

[6] Resolución del Parlamento Europeo del 3 de octubre de 2017 sobre la lucha contra la cibercriminalidad (2017/2068(INI)), art. 63 y 80, disponibles en el enlace https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_ES.html

[7] Resolución del Parlamento Europeo del 5 de julio sobre el carácter adecuado de la protección ofrecida por el escudo de protección de la vida privada UE/Estados Unidos considerando 27, disponible en el enlace https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_FR.pdf?redirect

[8] Resolución del Parlamento Europeo del 5 de julio sobre el carácter adecuado de la protección ofrecida por el escudo de protección de la vida privada UE/Estados Unidos considerando 28, disponible en el enlace https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_FR.pdf?redirect

Además, *CLOUD Act* establece un precedente para cualquier país que se comprometa a exigir la recuperación de los datos almacenados en cualquier parte del mundo basándose únicamente en la autoridad judicial de ese país. CCBE expresa sus fuertes reservas sobre estas medidas, que tienen el efecto de ampliar unilateralmente la prórroga de jurisdicción.

III. Leyes en conflicto

CLOUD Act es contrario a los derechos humanos fundamentales, ya que no prevé las normas mínimas establecidas por los tribunales europeos para restringir la vigilancia electrónica del gobierno. Tanto el Tribunal Europeo de Derechos Humanos como el Tribunal de Justicia de la Unión Europea han indicado una clara preferencia por la revisión judicial previa y el requisito de una base fáctica suficiente para cualquier vigilancia del individuo.

Además, la revelación de datos personales almacenados en la Unión Europea a una agencia del gobierno de los EE.UU. de un mandato en virtud de *CLOUD Act* constituye una violación del Reglamento General de Protección de Datos (RGPD). De acuerdo con las disposiciones del RGPD una orden de los Estados Unidos no constituye una base legal para tal transferencia fuera de la Unión Europea[9].

Derechos fundamentales

El artículo 8 del Convenio Europeo de Derechos Humanos y artículos 7 y 8 del Carta Europea de Derechos Fundamentales reconoce un derecho fundamental a la privacidad. De acuerdo con la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea, cualquier interferencia con el derecho a la privacidad debe ser conforme a la ley, tener un propósito legítimo y estar limitado a lo que es necesario en una sociedad democrática[10]. En cuanto al derecho a la protección de datos, ambos tribunales aplican una norma de "necesidad estricta"[11]. Tanto el Tribunal Europeo de Derechos Humanos (que aplica el Convenio Europeo) como el Tribunal de Justicia de la Unión Europea (que aplica la Carta Europea) han establecido numerosas garantías para el control gubernamental de las comunicaciones electrónicas[12].

a) Falta de notificación y vías de recurso

CLOUD Act no cuenta con un sistema integral de protección de la privacidad a través de normas procesales y de organización. No se da ninguna notificación a ningún nivel. Ni el Estado en el que se almacenan los datos o el Estado del que el interesado es ciudadano, son informados. Pero sobre todo, según el Tribunal Europeo de Derechos Humanos, la notificación y el recurso efectivo tendrían que ser facilitados al interesado, ya que la notificación está vinculada a la eficacia de los recursos. En el caso *Szabó*, el Tribunal Europeo de Derechos Humanos sostuvo que tiene que presentarse una notificación tan pronto como se completen las medidas de seguimiento y que la notificación ya no compromete las investigaciones.

En cuanto a los recursos, *CLOUD Act* también viola el artículo 19 del Acuerdo entre los Estados Unidos y la Unión Europea sobre la protección de datos personales en asuntos relacionados con la prevención, investigación, detención y enjuiciamiento de delitos. El artículo 19 de este Acuerdo impone a las partes

[9] Ver Memoria CCBE como amicus curiae en apoyo del demandado en Microsoft Irlanda (EN).

[10] Por ejemplo, el Tribunal Europeo de Derchos Hhumanos, Liberty c. Reino Unido, Dem. Nº 58243/00, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22ENG%22],%22appno%22:[%2258243/00%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-87207%22]}

[11] Tribunal Europeo de Derechos Humanos, Szabó, Aplicación 37138/14, p. 33; Tribunal Europeo de Justicia, Derechos digitales Ir. Ltd. v. Ministro de Asuntos Marítimos y Desarrollo del Norte

[12] Tribunal Europeo de Derechos Humanos, Zakharov c. Russie, asunto 47143/06, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2247143/06%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-160008%22]}

la obligación de prever, en su derecho interno, los derechos de los recursos judiciales concretos para sus respectivos ciudadanos.

b) Imprecisión del alcance y la duración de las medidas de vigilancia

CLOUD Act no establece límites adecuados en cuanto al alcance y la duración de las medidas de vigilancia.

No se indican las circunstancias en las que las autoridades públicas tienen derecho a utilizar las medidas descritas en *CLOUD Act*. El Tribunal Europeo de Derechos Humanos requiere una definición clara tanto de la "naturaleza de los delitos que pueden dar lugar a una orden judicial" como de la "naturaleza de los delitos que pueden dar lugar a una orden judicial" y una "definición de las categorías de personas que pueden ser objeto de seguimiento"[13]. Como garantía a este respecto, *CLOUD Act* tendría que especificar la naturaleza de los delitos a los que se aplica, ya sea especificando la naturaleza de estos delitos o haciendo referencia al menos a los niveles mínimos de sanciones autorizadas.

El Tribunal Europeo de Derechos Humanos ha aclarado que este doble requisito no significa que un individuo tenga que ser capaz de predecir cuándo es probable que las autoridades intercepten sus comunicaciones para adaptar su comportamiento en consecuencia. La "previsibilidad" significa la existencia de condiciones previas claras y detalladas para reducir al mínimo el riesgo de decisiones arbitrarias. En el caso *Weber c. Alemania* (demanda 54934/00), el Tribunal Europeo de Derechos Humanos consideró que una ley era razonablemente previsible basándose en el hecho de que la ley especificaba los delitos exactos para los que podía ordenarse y exigirse la vigilancia el objetivo ha realizado llamadas telefónicas internacionales utilizando tecnologías específicas o pronunciando palabras clave específicas (considerando 97 de la sentencia, en el que se especificaba que las personas interesadas tendrán que haber participado en una conversación telefónica internacional mediante por satélite o por radio (o a través de líneas telefónicas en el caso de la vigilancia destinada a prevenir un ataque armado contra Alemania, de conformidad con el punto 1 del apartado 1 del artículo 3).

Las restricciones apropiadas en cuanto a la duración incluyen una indicación clara del período tras el cual expira una orden de intercepción, las condiciones en las que puede renovarse y las circunstancias en las que debe ser cancelado. *CLOUD Act* no contiene ninguna disposición sobre esos plazos.

c) Medidas de protección adicionales

En virtud del Convenio Europeo, la legalidad y la necesidad de un régimen de vigilancia se evaluarán en términos de accesibilidad de la legislación nacional, los procedimientos a seguirse para almacenar, acceder, examinar, utilizar, comunicar y destruir los datos interceptados, los procedimientos de autorización y de control de aplicación de las medidas de vigilancia secreta[14].

Es muy probable que las órdenes de detención dictadas en virtud de *CLOUD Act* no cumplan los requisitos de los tribunales europeos sobre las condiciones de control accesibles (es decir, accesibles al público). Por ejemplo, en el caso *Liberty c. Reino Unido*, los informes anuales en los que el Ministro de Interior británico simplemente declaró, sin detalles, qué "medidas" garantizaban un acceso restringido a las pruebas obtenidas mediante la vigilancia era no tienen "ninguna incidencia en la claridad y accesibilidad de las "medidas" en cuestión, ya que no estaban facultados para divulgarlo"[15].

---

[13] Tribunal Europeo de Derechos Humanos, Zakharov c. Rusia, demanda 47143/06, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2247143/06%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-160008%22]}

[14] Tribunal Europeo de Derechos Humanos, Zakharov c. Rusia, demanda 47143/06, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2247143/06%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-160008%22]} , p. 60.

[15] Tribunal Europeo de Derechos Humanos, Liberty c. Reino Unido, demanda 58243/00, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2258243/00%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-87208%22]}.

Los datos obtenidos a través de medidas de vigilancia no tienen que ser almacenados ilimitadamente. En principio, los datos tienen que destruirse inmediatamente si ya no son pertinentes de acuerdo con la finalidad con los que fueron obtenidos[16]. Incluso si los datos almacenados son pertinentes, su conservación de manera prolongada tiene que estar justificado por criterios objetivos[17]. Por ejemplo, ningún dato podrá conservarse sobre "personas por las cuales no exista ningún indicio para dejar de creer que su comportamiento pueda tener una conexión, indirecto o lejano, con infracciones graves[18].

RGPD

Las órdenes emitidas por *CLOUD Act* también entran en conflicto con la RGPD de la Unión Europea. Una orden por sí sola no proporciona una base jurídica para el tratamiento de datos en el contexto de la RGPD.

El consentimiento no puede justificar el tratamiento de datos con arreglo al *CLOUD Act*, dado que no se informa a la persona interesada de la emisión de la orden. Sin embargo, para que el consentimiento sea válido, la persona tiene que estar bien informada y se le tiene que dar la posbilidad de retirarlo. Estos requisitos no se cumplen en un entorno de aplicación de la ley.

La letra c) del apartado 1 del artículo 6 del RGPD tampoco justifica tal tratamiento. Aunque la letra c) del apartado 1 del artículo 6 reconoce la necesidad de "cumplir una obligación legal a la que está sujeto el responsable del tratamiento", esta obligación legal tiene que derivar de la legislación de la Unión Europea. Por lo tanto, una obligación en virtud de *CLOUD Act* no constituye una obligación legal en el sentido de la sección 6 (1)(c) del RGPD.

El artículo 48 del RGPD dispone lo siguiente:

> "Toda decisión de un tribunal o de una autoridad administrativa de un tercer país por la que se exija a un responsable del tratamiento que transmita o comunique datos de carácter personal no podrá reconocerse ni hacerse aplicable de ninguna manera a menos que se base en un acuerdo internacional, como un tratado de asistencia judicial mutua en vigor entre el tercer país solicitante y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia en virtud del presente capítulo".

En virtud de esta disposición, sólo los tratados de asistencia judicial mutua o acuerdos internacionales comparables proporcionan una base admisible para la transferencia extraterritorial de datos de carácter personal. Por lo tanto, *CLOUD Act* no proporciona una base legal para la transferencia de datos a los Estados Unidos bajo el artículo 48 del RGPD. Por lo tanto, una orden de EE.UU. no responde a los requisitos del artículo 48 para la transferencia de datos de Europa a los Estados Unidos.

Tampoco está permitida por el artículo 49 del RGD una transferencia de datos resultante de *CLOUD Act*, ya que esta exención está restringida y debe interpretarse de forma estricta. Es muy probable que una orden de detención emitida en virtud de *CLOUD Act* no cumpla con las restricciones establecidas en el artículo 49 (1) de la RGPD, ya que el receptor de la orden de detención (es decir, el proveedor de servicios) no podrá evaluar las circunstancias de la transferencia de datos, ya que el gobierno puede podría no estar dispuesto a revelar información de vigilancia. Además, la derogación del artículo 49 (1)(d) no se aplica puesto que el interés público no puede basarse en una decisión unilateral de un tercer país[19].

---

[16] Tribunal Europeo de Derechos Humanos, Zakharov c. Rusia, demanda 47143/06, https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22FRE%22],%22appno%22:[%2247143/06%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-160008%22]}, p. 64.

[17] Tribunal de Justicia de la Unión Europea, Digital Rights Ir. Ltd. c. Ministro de la Marina y del Desarrollo del Norte. Res. en p. 63.

[18] Tribunal de Justicia de la Unión Europea, Derechos digitales Ir. Ltd. c. Ministro de la Marina y del Norte de Canadá.

[19] Véanse también las Directrices 2/2018 del Consejo Europeo de Protección de Datos sobre excepciones al artículo 49 del Reglamento 2016/679, páginas 10-11

Como beneficiarios de un mandato en virtud *CLOUD Act*, las empresas de tecnología se encontrarán entre dos leyes de datos contradictorias respecto de sus datos. Dado que el RGPD limita estrictamente las circunstancias en las que los datos pueden transferirse legalmente a terceros países y prevé fuertes multas por infracciones en caso de violación (hasta el 4% del volumen de negocios de un empresas), las empresas se encuentran atrapadas entre el incumplimiento de una orden de los Estados Unidos (por violación de una disposición del *CLOUD Act*) y el riesgo de sanciones monetarias o incluso penales significativas (por violación de las disposiciones de la RGPD). Las leyes nacionales que complementan el RGPD prevén penas de prisión de hasta tres años por violación del RGPD (artículo 42 (1) de la nueva ley federal alemana sobre protección de datos).

IV. Recurso limitado para el prestador de servicios de que se trate

CCBE acoge con satisfacción el hecho de que *CLOUD Act* garantice que la vigilancia no se ordene "al azar, de manera irregular o sin la debida consideración", mediante la presentación de cualquier procedimiento que autorice la supervisión al control judicial previo.

Aunque es positivo, en comparación con la situación anterior a *CLOUD Act*, que en la actualidad exista un proceso bien establecido para impugnar una orden antes de su ejecución, el posible recurso es de alcance limitado.

Los proveedores que se encuentran en un dilema entre las obligaciones legales de la Unión Europea y la obligación de cumplir con el mandato del *CLOUD Act* se ven una vez más obligados a rechazar el cumplimient y a litigar por desacato ya que no pueden presentar la moción para modificar o anular la orden. Esto se debe a que la UE, como se ha explicado anteriormente, no entra dentro del término "gobierno cualificado" porque es una organización supranacional. El proveedor no se encuentra en posición de declarar un "riesgo significativo que infringiría las leyes del gobierno extranjero elegible" al seguir la orden. Tal razonamiento de riesgo significativo es, sin embargo, una condición previa esencial para la moción, como indica la palabra “y” en el §2713 del Código de los Estados Unidos.

Sin embargo, incluso si el término "gobierno cualificado" debe interpretarse en sentido amplio para aplicar a las organizaciones supranacionales como la UE, se impedirá probablemente a la UE entrar en un acuerdo ejecutivo bajo el §2523 del Código de los Estados Unidos debido al artículo 48 del RGPD (véase más arriba). Lo mismo se aplica a los propios Estados Miembros de la UE, que están también obligados por el artículo 48 del RGPD. En su lugar, sería necesario que los Estados Unidos celebrasen un acuerdo internacional, como un tratado de asistencia judicial mutua con la UE o con los Estados Miembros de la Unión Europea, algo, a lo que parece no estar dispuesto a hacer de momento.

Por tanto, el control jurisdiccional previo a la ejecución es prácticamente inexistente para los suscriptores y los clientes que sean nacionales de un Estado Miembro de la Unión Europea.

Un control jurisdiccional previo a la ejecución de una orden tendrá que efectuarse independientemente del hecho de que el Estado en el que se requieran las informaciones estén, o bien almacenadas o bien no de un “gobierno cualificado”. Así, debe cambiarse el requisito (ii) de presentar una solicitud conexa a: “(ii) que la divulgación solicitada originaría un riesgo material tan importante que el proveedor violaría las leyes del Estado extranjero donde se encuentrase la información solicitada”.

V. Control (judicial) débil

Como se ha explicado anteriormente, la UE violaría sus propias leyes, a saber, el artículo 48 RGPD, mediante la celebración de un acuerdo ejecutivo en virtud del §2523 del Código de los Estados Unidos. Sin embargo, incluso si la UE, firmara un acuerdo de este tipo para que se reconozcan sus intereses en la revisión judicial previa a una moción, los criterios de cortesía mostrarían deficiencias.

En primer lugar, el "gobierno extranjero cualificado" – otro que no sea el Gobierno de los Estados Unidos- no se escucharía antes del análisis de cortesía. Por lo tanto, es probable que el tribunal

competente otorgue más importancia a los intereses de los Estados Unidos que a los intereses del "gobierno extranjero calificado" en contra de la divulgación.

En segundo lugar, dado que la naturaleza y la gravedad de los delitos en cuestión no son un requisito previo para la emisión de la orden de detención, aquellos deberían ser considerados al menos como un criterio a tener en cuenta en el análisis de la cortesía.

En tercer lugar, el criterio (F) relativo a la importancia de la información para la investigación se interpreta de manera demasiado amplia. En cambio, el §2713 debería establecer que la divulgación sólo se permite en caso de que la investigación fuera considerablemente más difícil o no ofrezca perspectivas de éxito.

Por último, sería deseable una revisión judicial previa general. Con respecto al análisis de cortesía, *CLOUD Act* debería cambiarse de "(i) la divulgación requerida haría que el proveedor violara las leyes de un gobierno calificado; [...]" a "(i) la divulgación requerida haría que el proveedor violara las leyes del Estado donde se encuentre la información solicitada". Asimismo, deberían modificarse las especificaciones (A) a (H) con dicha referencia.

VI. Falta de supervisión posterior a la autorización

CLOUD Act no prevé ninguna supervisión posterior a la autorización. Sin embargo, estos acuerdos de supervisión son una salvaguardia vital. En el asunto *Schrems c el Comisario de Protección de Datos*, el Tribunal de Justicia de la Unión Europea sostuvo que una autoridad nacional de control tiene que "examinar, con total independencia, cualquier reclamación relativa a la protección de los derechos y libertades de las personas en relación con el tratamiento de datos personales". Esta supervisión posterior a la autorización podría adoptar la forma de requisito para un informe anual sobre las medidas ordenadas de conformidad con *CLOUD Act* a una comisión de la Cámara. En el informe podría exigirse que se indicara el número de procedimientos incoados y los delitos subyacentes a los que se refieren esos procedimientos. Para garantizar la transparencia, debería exigirse la publicación del informe.

D. Falta de protección del secreto profesional de las personas jurídicas

I. Secreto profesional en general

A CCBE le preocupa especialmente que *CLOUD Act* no tenga en cuenta la especial sensibilidad de las comunicaciones confidenciales entre los abogados y sus clientes. Todas las asociaciones profesionales de abogados de todos los Estados miembros de la Unión Europea consideran la confidencialidad como algo inherente en la profesión de abogados. Se menciona en todos los códigos de conducta nacionales, siguiendo el ejemplo de CCBE[20]. La confidencialidad es parte de la ética de la profesión de abogado.[21]

Aunque los Estados europeos adoptan diferentes enfoques para proteger el secreto profesional, el principio de tal protección está generalmente reconocido. En todos los Estados miembros de la UE, (y de los Estados miembros del Consejo de Europa) tiene el rango de principio fundamental y el estatus de una norma de orden público.[22]

En el artículo 41 de la Carta de los Derechos Fundamentales de la Unión Europea, la protección del secreto profesional está expresamente declarada, como sigue

[20] Conclusiones del Abogado General en el caso C-305/05 ante TJUE el 14 diciembre 2006, recital 37.
[21] Conclusiones del Abogado General en el caso C-305/05 ante TJUE el 14 diciembre 2006, recital 37
[22] Véase, en este sentido, el considerando 182 de las conclusiones del Abogado General Léger en el Tribunal de Justicia de las Comunidades Europeas, asunto C-309/99, Wouters y otros.

"derecho de toda persona a acceder a su expediente, respetando los intereses legítimos de la confidencialidad y del secreto profesional y empresarial".

El reconocimiento del secreto profesional ante los tribunales europeos tiene una larga historia, en jurisdicciones individuales anteriores tanto a la UE como el Consejo de Europa. A través de su jurisprudencia, el Tribunal de Justicia de la Unión Europea ha defendido el principio de confidencialidad de las comunicaciones escritas entre un abogado y su cliente[23] y ha reconocido la naturaleza específica de la profesión jurídica[24].

El Tribunal Europeo de Derechos Humanos exige a todos los signatarios del Convenio Europeo que garanticen la inviolabilidad del secreto profesional en su territorio. En *Michaud c. Francia*, el Tribunal subrayó que el intercambio entre los abogados y sus clientes había reforzado su protección. La jurisprudencia del Tribunal Europeo de Derechos Humanos revela dos principios diferentes en los que la protección del secreto profesional tiene sus raíces. En la sentencia del caso *Niemitz c. Alemania*, el Tribunal dictaminó que, cuando se trataba de un abogado, una violación del secreto profesional "puede repercutir en la buena administración de la justicia y, por ende, en los derechos garantizados por el artículo 6 [derecho a un juicio justo]".[25] Sin la certeza del secreto, no hay confianza en la relación entre cliente y abogado. En efecto, no existe ninguna base que pueda conducir a la "manifestación de verdad y justicia"[26]. Asimismo, el Abogado General Léger declaró en sus conclusiones en *Wouters y Otros* que "los abogados ocupan un lugar central en la administración de justicia como intermediarios entre el público y los tribunales."[27] Así pues, el privilegio jurídico es el corolario esencial del derecho de defensa del cliente[28]. El segundo aspecto del secreto profesional es que el principio protege a los ciudadanos de las revelaciones que puedan dañar su reputación. Con respecto a este objetivo de protección, el Tribunal Europeo de Derechos Humanos, en su sentencia *Foxley c. el Reino Unido*, sostuvo que el derecho a la intimidad en virtud del artículo 8 de la Carta Europea de Derechos Humanos es otro componente esencial del principio[29].

En resumen, se considera que la protección del secreto profesional jurídico se deriva ahora del párrafo 8 (1) (protección de la correspondencia) en relación con el artículo 6 (1), (3)(c) de la Carta Europea de Derechos Humanos, así como del artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea (respeto por las comunicaciones) en relación con el artículo 47 (1), la segunda frase del artículo 47 (2) y el artículo 48 (2) de la Carta (derecho a ser informado, defendido y representado, respeto al derecho de defensa).[30]

II. Falta de protección procesal

CLOUD Act amenaza con comprometer la inviolabilidad de la asesoría legal sin proporcionar a los abogados o a sus clientes protección procesal para garantizar el privilegio concedido por la legislación de la Unión Europea.

El derecho del abogado europeo a la protección del secreto profesional con respecto a la incautación de material potencialmente privilegiado almacenado en servidores de datos en toda Europa no se aborda en *CLOUD Act* y SCA respectivamente. Sin embargo, el Tribunal Europeo de Derechos Humanos consideró que una incautación amplia e indiferenciada de la correspondencia por correo electrónico violaba el principio del secreto profesional.[31]

[23] Tribunal de Justicia de la Unión Europea, Caso 155/79 AM & S [1982], ECR 1575
[24] Tribunal de Justicia de la Unión Europea, Caso C-309/99, Wouters y Otros [2002] ECR 1-1577.
[25] Tribunal de Justicia de la Unión Europea, sentencia de 16 de diciembre de 1992, Niemitz c. Alemania, art. 37.
[26] Conclusiones del Abogado General en el caso C-305/05 ante TJUE el 14 December 2006, considerando 41.
[27] Opinión del Abogado General Léger en TJUE en el caso C-309/99, Wouters and Others, considerando 174
[28] Tribunal de Justicia de la Unión Europea caso 155/79, AM & S c. Comisión [1982] ECR 1575, considerandos 10 y 23.
[29] Tribunal Europeo de Derechos Humanos, sentencia de 10 de septiembre de 2000, Foxley contra Reino Unido, § 44.
[30] Conclusiones del Abogado General Kokott en el TJUE caso C-5550/07, el 29 Abril 2010, Akzo Nobel Chemicals y Akcros Chemicals c. Comisión, considerando 47.
[31] Tribunal Europeo de Derechos Humanos, Vinci Construction y GTM Génie Civil y Services c. Francia, App. Nos 63629/10 y 60567/10, 2 de abril de 2015.

Asimismo, la Abogada General Kokott declaró en la sentencia *Akzo y Akcros c. Comisión* que

> "Los abogados no estarían en condiciones de cumplir satisfactoriamente su misión de asesoramiento, de defensa y de representación de sus clientes, quienes se verían privados de los derechos contenidos en el artículo 6 de la Carta Europea de Derechos Humanos y los artículos 47 y 48 de la Carta de los Derechos Fundamentales, si los abogados estuvieran obligados, en el marco de un procedimiento judicial o en la preparación de dichos procedimientos, a cooperar con las autoridades haciéndoles pasar por información obtenida en el curso de consultas jurídicas conexas."[32]

Esto se aplica aún más cuando los abogados no tienen siquiera conocimiento de la incautación del material protegido, porque el procedimiento de divulgación basado en una orden judicial no implica notificación alguna. Mientras *CLOUD Act* no prevea la inadmisibilidad de las pruebas obtenidas a partir de material protegido, amenaza con privar a los ciudadanos europeos de sus derechos a la intimidad, a la representación y a un juicio justo.

El artículo 6 del Convenio Europeo de los Derechos Humanos (CEDH) sobre el derecho a un juicio justo es absoluto (a diferencia del artículo 8 sobre el derecho a la intimidad, que se califica) y, por esa razón, CCBE sugiere que la existencia del secreto profesional en los datos que se pretende recuperar debe ser un impedimento total para la recuperación de tales datos. A este respecto, cabe señalar que, en algunas circunstancias, el material protegido por el secreto profesional de los abogados debería ser clasificado como un factor a tener en cuenta en la "totalidad de las circunstancias" como parte de un análisis de cortesía. De lo contrario, es probable que no se tengan en cuenta en absoluto el secreto profesional. Aunque Estados Unidos reconoce el "privilegio abogado-cliente" como regla absoluta de prueba, cuyo efecto es que los acusados en un caso penal no están obligados a presentar al fiscal ningún "informe, memorando u otros documentos hechos por el acusado, o por el abogado o agente del acusado, durante la investigación o la defensa del caso" (Regla Federal de Procedimiento Penal 16(b)(2)), la aplicación de este principio es difícil en toda la recopilación no contradictoria de pruebas.

Añadir el secreto profesional como factor de ponderación al análisis de cortesía (general) es aún más importante, dado que no existe un control judicial posterior a la recopilación.

Más allá, las obligaciones del secreto profesional en algunas naciones Europeas pueden ser de un alcance más amplio que en los Estados Unidos: en el Código judicial belga, por ejemplo, las comunicaciones entre abogado y cliente pueden que no sean usadas como pruebas y cualquier evidencia de privilegio deberá resolverse por el presidente de la Abogacía Belga.[33] Cualquier proceso de divulgación basado en una orden de *CLOUD Act* sería contrario a la ley belga.

E. Impacto en el Escudo de Privacidad

En teoría, *CLOUD Act* no afecta al Escudo de Privacidad, ya que este último se aplica a la transferencia transatlántica de datos entre entidades privadas con fines comerciales, mientras que *CLOUD Act* se aplica a la transferencia de datos transatlánticos de una entidad privada a una agencia gubernamental para fines legales con fines de ejecución y enjuiciamiento. En la práctica, sin embargo, *CLOUD Act* no hace nada para abordar el riesgo de que, tras una transferencia transatlántica con fines comerciales, los datos personales están sujetos a un requisito de obligación de divulgación a efectos de enjuiciamiento. Las dudas que se plantearon en relación con el caso de Microsoft sobre cuánta protección proporciona el Escudo de Privacidad en la actualidad, aún permanecen.

---

[32]Conclusiones de la Abogada General Kokott en el TJUE, asunto C-5550/07, presentadas el 29 de abril de 2010, Akzo Nobel Chemicals y Akcros Chemicals/Comisión, considerando 49, con más referencias.

[33] https://uk.practicallaw.thomsonreuters.com/2-103-2508?transitionType=Default&contextData=(sc.Default&firstPage=true&bhcp=1

Sin embargo, podría ser poco probable que la Comisión, debido a *CLOUD Act*, cambie su adecuación del Escudo de Privacidad. Antes de la aprobación de *CLOUD Act*, el gobierno de los EE.UU. era capaz de acceder a los datos personales de un ciudadano de la UE - transferidos a los EE.UU. de conformidad con el Escudo de Privacidad y almacenados después en EE.UU. - sobre la base de la SCA. Aunque el SCA no proporcionó ninguna solución legal, la Comisión llegó a la conclusión de que EE.UU. garantiza un nivel adecuado de protección de los datos. Una evaluación mucho más realista del nivel de protección de datos habría sido juzgar a los proveedores de servicios en línea de los EE.UU. por ser inseguros y no cumplir con las disposiciones del RGPD, debido a que existe el riesgo de que las autoridades de EE.UU. procesen sin restricciones los datos después de una orden de SCA. Como este riesgo subsiste, las conclusiones de la Comisión en cuanto a la idoneidad del Escudo de Privacidad se mantienen en este ámbito cuestionables y con la necesidad de ser aun desafiado.

F. Recomendaciones

Para eliminar el conflicto entre *CLOUD Act* y el Derecho Europeo, para crear suficientes salvaguardias y recursos legales contra las medidas de vigilancia de EE.UU. y para garantizar la protección del secreto profesional, CCBE recomienda que la Unión Europea adopte las siguientes medidas

1. Negociar un tratado de asistencia legal mutua con los Estados Unidos que se refiera explícitamente a *CLOUD Act*, y que establezca requisitos precisos para la transferencia de datos y no socave el nivel de protección que proporcionan las libertades fundamentales;

2. Asegurarse de que, de conformidad con ese tratado de asistencia judicial mutua, en cada caso, tras la firma de una solicitud de datos en virtud de *CLOUD Act*, los datos sólo se transferirán a los Estados Unidos después de que se haya notificado a una autoridad europea competente e independiente;

3. Asegurarse de que el proveedor de servicios afectado que aloja los datos solicitados esté informado por la autoridad europea competente sobre los recursos legales existentes en los Estados Unidos;

4. Garantizar que, de conformidad con ese tratado de asistencia judicial mutua, el secreto profesional constituye un motivo absoluto de objeción a la cesión de los datos a los Estados Unidos bajo el *CLOUD Act.*