UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

SECCIÓN DEPARTAMENTAL DE DERECHO CONSTITUCIONAL DE LA FACULTAD DE CIENCIAS DE LA INFORMACIÓN

TESIS DOCTORAL

La contratación de servicios de cloud computing: movimientos internacionales de datos y gestión de riesgos de privacidad y seguridad

MEMORIA PARA OPTAR AL GRADO DE DOCTORA

PRESENTADA POR

Nathaly Rey Arenas

DIRECTOR

Manuel Sánchez de Diego Fernández de la Riva

Madrid, 2017

UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE DERECHO
PROGRAMA DE DOCTORADO:
EL DERECHO DE LA COMUNICACIÓN EN LA SOCIEDAD ACTUAL
SECCIÓN DEPARTAMENTAL DE DERECHO CONSTITUCIONAL
DE LA FACULTAD DE CIENCIAS DE LA INFORMACIÓN

TESIS DOCTORAL

LA CONTRATACIÓN DE SERVICIOS DE CLOUD COMPUTING: MOVIMIENTOS INTERNACIONALES DE DATOS Y GESTIÓN DE RIESGOS DE PRIVACIDAD Y SEGURIDAD

NATHALY REY ARENAS

DIRECTOR: MANUEL SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA

MADRID, 2015

ÍNDICE

RESUMEN

La contratación de servicios de Cloud Computing[1] en el ámbito B2B, plantea una serie de retos jurídicos que van desde la correcta articulación de los movimientos internacionales de datos a la luz de la normativa aplicable en materia de privacidad, hasta la delimitación de las cuestiones relativas a la ley aplicable y jurisdiccionales, y el establecimiento de un marco adecuado para procurar la seguridad de la información que va a ser procesada a través de los servicios.

Hablar de Cloud Computing es hablar de Internet, un entorno en el que los datos se encuentran en constante movimiento a través de las fronteras, en consecuencia, la gestión de los riesgos de privacidad y seguridad requiere del establecimiento de protecciones jurídicas y técnicas centradas en los datos, en lugar de protecciones centradas en geografías concretas. Dada la falta de una normativa global en materia de privacidad, y específicamente, en materia de movimientos internacionales de datos, estas garantías deben procurarse contractualmente.

Si bien el cumplimiento de las normativas aplicables, en función del lugar del establecimiento u operaciones responsable del tratamiento de dichos datos, o de su actividad sectorial, debe guiar las protecciones mínimas que deben asegurarse por

[1] También conocidos como servicios en la nube o servicios de cloud.

vía contractual, el mero cumplimiento normativo no implica necesariamente la protección efectiva de los datos contra los riesgos que envuelve el ciberespacio para la información, tales como los ataques e intrusiones provenientes de hackers y otros actores, incluidos gobiernos, en detrimento de la confidencialidad de los datos y los derechos de sus titulares. Por tanto, el establecimiento de medidas de seguridad adecuadas teniendo en cuenta el estado del arte tales como el cifrado robusto, la autenticación de doble factor, así como la realización de ciberejercicios para probar la robustez y resiliencia de los servicios de Cloud Computing, entre otras, resultan imprescindibles.

Los contratos de Cloud Computing admiten la elección por las partes de la legislación aplicable y jurisdicción competente en los ámbitos civil, mercantil, y de protección de datos, siempre que no se contravengan normas de orden público. No obstante, en virtud de que en el ámbito penal los pactos contractuales no son posibles, a los efectos de valorar y gestionar los riesgos de privacidad y seguridad vinculados al acceso gubernamental a la información en la nube en el marco de una investigación criminal, es necesario analizar qué protecciones jurídicas aplicarían a los datos y a sus titulares a la luz del ordenamiento jurídico del establecimiento de las partes, y si éste fuera distinto, debe determinarse si el ordenamiento aplicable al proveedor de servicios de Cloud Computing ofrece una protección equiparable en este sentido, o no. En general, los sistemas jurídicos avanzados, aunque difieren en su enfoque,

otorgan a las autoridades gubernamentales poderes de investigación, a la par que establecen limitaciones similares. Este es el caso de España, el Reino Unido y los Estados Unidos.

El tratamiento multinacional de información en la nube produce algo que se percibe por algunos Estados como una pérdida de soberanía sobre los datos de sus ciudadanos, puesto que su jurisdicción penal es eminentemente territorial y su ejercicio el ámbito de Internet puede verse limitado. Esto podría motivar requerimientos de localización forzada de las infraestructuras que soportan los servicios de Cloud, lo cual produciría la fragmentación de Internet y la ruptura de las economías de escala del Cloud Computing, por ello, resulta necesario revisar los mecanismos de cooperación judicial internacional existentes, a los efectos de que se garantice la interoperabilidad y celeridad necesarias en el ámbito criminal. Asimismo, la incorporación de elementos de extraterritorialidad amparada en principios reconocidos y en el interés legítimo de los Estados, y su incorporación por el Derecho Internacional se configura como una posible solución.

SUMMARY

The contracting for Cloud Computing services in the B2B space poses a number of legal challenges; from the correct articulation of international data flows in the light of applicable privacy legislation, to the delimitation of applicable law and jurisdictional issues, and the establishment of an adequate framework to procure the security of the information to be processed through the services.

Talking about Cloud Computing is talking about the Internet, an environment in which data are constantly moving across borders, therefore, privacy and security risks management require the establishment of data-centric legal and technical protections, rather than geography-centric protections. Given the lack of a global privacy framework, specifically regarding cross border data flows, these protections should be sought via contractual arrangements.

While compliance with applicable laws regulations based on the establishment or the operations of the data controller, or its sectoral activity, should guide the minimal protections to be contractually achieved, compliance *per se* does not necessarily imply the effective protection of data against risks in the cyberspace such as attacks and intrusions from hackers and other actors, including governments, in detriment of both data confidentiality, and data controllers and/or data subjects rights. Therefore, the establishment of appropriate security measures taking into account the state of

the art, such as strong encryption and two-factor authentication, as well as conducting cyber-exercises in order to test the robustness and resilience Cloud Computing services, among others, are essential.

Cloud Computing contracts allow for the parties' choice of applicable law and jurisdiction in civil, commercial, and data protection areas, as long as there is no contravention of public order rules. However, when it comes to criminal matters, the contractual agreements are not possible at all, consequently, for the purposes of assessing and managing privacy and security risks linked to government access to information in the Cloud in connection with criminal investigations, it is necessary to analyze what legal protections would apply to the data and the data subjects in light of the legal system of the establishment of the parties, and if such an establishment is different, it should be determined whether the legal regime applicable to the provider offers strong, or at least, comparable protections in this regard or not. In general, although advanced legal systems differ in their approach, they provide government authorities similar accesses powers and establish alike limitations. This is the case for Spain, the United Kingdom and the United States.

The multinational processing of data in the cloud produces something perceived by some States as a loss of sovereignty on the data of their citizens, given that their criminal jurisdiction is essentially territorial and its exercise within a borderless

Internet may be limited. This could motivate forced data location requirements on the infrastructure supporting Cloud services, which would create Internet fragmentation and the breakdown of Cloud Computing economies of scale. In order to prevent such postures, it is necessary to review the existing international judicial cooperation mechanisms to ensure the necessary interoperability and velocity in the criminal field. Also, the incorporation of extraterritorial elements based on recognized principles and on the legitimate interest of States, and its incorporation by international law represents a possible solution.

1. INTRODUCCIÓN

El Cloud Computing o computación en la nube, es un modelo de prestación de servicios informáticos de reciente creación, producto de la evolución de muchas tecnologías, que permite ofrecer la informática (aplicaciones, infraestructura y almacenamiento) como un servicio disponible a través de Internet.[2] Se trata de un modelo disruptivo que combina el avance de la computación, con el poder de Internet y de las economías de escala.

Ya por 1997, Steve Jobs[3] arrojó luz sobre este fenómeno con las siguientes palabras: *"Gran parte del tremendo impacto de usar ordenadores en la actualidad, es su utilización no sólo para ejecutar tareas de computación intensivas, sino su utilización como una ventana de comunicación para para acceder a estas tareas de computación intensivas. Nunca he visto algo más poderoso que ésta computación combinada con la tecnología de red que ahora tenemos (*refiriéndose a Internet, que se encontraba aún en una etapa temprana*)... Y, yo sólo quiero centrarme en algo que está muy cerca de mí, que es vivir en un mundo conectado a alta velocidad para hacer mi trabajo todos los días. Pregunto: ¿cuántos de ustedes gestionan el*

[2] Internet es el nombre genérico que recibe la unión de todas las redes de comunicación a nivel mundial, que utilizan el Protocolo TPC/IP u otros similares para entablar comunicación entre sí.

[3] Steve Jobs (1955 –2011) fue conocido como el co- fundador, ex presidente y ex director ejecutivo de Apple Inc. pionero y visionario de la revolución de la microcomputación.

almacenamiento en sus propios equipos? ¿Cuántos de ustedes hacen copias de seguridad, por ejemplo? ¿Cuántos han tenido un accidente con esos equipos en los últimos tres años...? De acuerdo, permítanme describir el mundo en el que vivo. Hace unos 8 años, teníamos redes de alta velocidad conectadas a nuestros ordenadores obsoletos. Y gracias a que estábamos usando NFS,[4] fuimos capaces de sacar toda la información fuera de nuestros ordenadores y de ponerla en un servidor. El software lo hizo de forma completamente transparente, y debido a que el servidor tenía una gran cantidad de memoria RAM[5], en algunos casos, era de hecho más rápido obtener información desde el servidor, que desde el disco duro local (...) Pero lo que fue realmente notable, fue que la organización pudo contratar a un profesional para respaldar ese servidor cada noche, y pudo darse el lujo de gastar un poco más en ese servidor, así que tal vez tenía discos redundantes, y también fuentes de alimentación redundantes. En los últimos 7 años, ¿saben cuántas veces he perdido algún dato personal? Cero. ¿Saben cuántas veces he hecho una copia de seguridad de mi equipo? Cero. Tengo computadoras de Apple, en Next, en Pixar y en casa, inicio una sesión con mi usuario y obtengo acceso a mi información, esté donde esté. Nada se encuentra guardado en mi disco duro. Y el Giga-Internet vendrá, y hará que sea aún

[4] El NFS (por sus siglas en inglés, Network File System) es un protocolo de nivel de aplicación desarrollado originalmente en 1984 por Sun Microsystems. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.

[5] RAM: Random Access Memory: Memoria de acceso aleatorio. Memoria donde la computadora almacena datos que le permiten al procesador acceder rápidamente al sistema operativo, las aplicaciones y los datos en uso. Tiene estrecha relación con la velocidad de la computadora. Se mide en megabytes. GONZÁLEZ, R: "Diccionario de Computación y Electrónica". México D.F, 2004.

más rápido acceder a la información en el servidor (...) Y no me importa cómo se hace, no me importa lo que hay en la caja está en el otro extremo (...) una de mis esperanzas es que Apple (...) pueda hacer esto una realidad fácil y disponible para cualquiera".[6]

Catorce años más tarde, esta esperanza se denominaría iCloud, un proyecto que solo vivió algunos años en el mercado, y que llegó a estar disponible únicamente en el ámbito *Business to Consumer* (B2C). Hoy compañías como Amazon, Box, Dropbox, Google, Microsoft y Salesforce son algunos de los jugadores más relevantes del Cloud Computing en el ámbito *Business to Business* (B2B) a nivel mundial, mientras que Apple ha centrado su estrategia principalmente en el negocio del hardware. No obstante, el mundo descrito por Job es, sin duda, el mundo en el que vivimos.

El Cloud está cambiando la economía de las TI y transformando forma de entender la informática en el mundo corporativo, educativo y gubernamental. Y es que la nube brinda a las organizaciones la posibilidad de acceder a un gran número de recursos tecnológicos y de disponer de una enorme capacidad de procesamiento y almacenamiento sin necesidad de invertir en infraestructura (centros de datos),

[6] JOBS, Steve. Apple WWDC conference, 1997 https://www.youtube.com/watch?v=Or7zaUaP-J8

orientando siempre sus costes a los recursos efectivamente utilizados, y convirtiendo de esta manera su CAPEX en OPEX en el ámbito de la computación.[7]

Los servicios en la nube se benefician de las economías de escala y operativas que los departamentos de Tecnologías de la Información (TI) de las empresas normalmente no pueden alcanzar. Por un lado, la infraestructura de TI es llevada a centros de datos de gran tamaño; estos centros se aprovechan de escalas principalmente en tres áreas (i) la cadena de suministro[8] (ii) la demanda[9] y (iii) las aplicaciones multiusuario.[10] Por otro lado, la nube estandariza y comparte recursos, automatizando muchas de las tareas de operación y mantenimiento que tradicionalmente se hacían de forma manual.

Sobre la disyuntiva de "producir o comprar" recursos de TI en la organización empresarial, es decir construir y operar centro de datos propios, y desarrollar y mantener aplicaciones propias, o adquirir estos de un tercero en forma de servicios,

[7] El término CAPEX (del inglés Capital Expenditures) se refiere a aquellas inversiones de capital que crean beneficios. Un CAPEX se ejecuta cuando un negocio invierte en la compra o mejora de un activo fijo (propiedades, edificios, data centers, servidores, etc.). Por su parte, el OPEX (del inglés Operating Expense) se refiere a los gasto de funcionamiento operacionales (por ejemplo, licencias, publicidad, gastos de oficina, suministros, honorarios,etc.).

[8] En un gran centro de datos el coste por servidor es menor.

[9] La concentración de la demanda hace que las tasas de utilización del servidor puedan aumentar.

[10] Al cambiar a un modelo de aplicación multiusuario, al aumentar el número de usuarios disminuye la gestión de aplicaciones y el coste del servidor por usuario.

resulta ilustrativo traer a colación la visión aportada por COESE[11] en su ensayo "La Naturaleza de la Empresa". COESE planteó una teoría sobre cuándo una empresa va a producir algo para sí misma y, por el contrario, cuando va a adquirirlo de un tercero, llegando a una conclusión tan válida hoy como hace más de siete décadas: Si es más barato, en la suma, comprarlo, una empresa irá al buscarlo en el mercado o en sus socios. De lo contrario, producirá el bien o servicio para sí misma. Las cifras del Cloud Computing ejemplifican la teoría de COESE, Gartner predice que la mayor parte de los nuevos gastos de TI para el 2016 se dirigirán a plataformas y aplicaciones Cloud,[12] y que solo el mercado de la seguridad basado en la nube tendrá un valor de 2.7 billones de euros en 2015 a nivel mundial.[13] Por su parte, la UE el considera que el impacto del Cloud Computing en su PIB[14] podría ser de 957 billones de euros y de 3.8 millones de puestos de trabajo en el año 2020.[15]

[11] COESE, Ronald: "The Nature of the Firm". Economica, New Series, Vol. 4, No. 16. London School of Economics, 1937, p. 386-405. Accesibe desde http://www.jstor.org/stable/2626876?seq=1#page_scan_tab_contents

[12] Gartner Symposium, 2013 http://www.gartner.com/newsroom/id/2613015

[13] Según Gartner http://www.gartner.com/newsroom/id/2616115

[14] Producto Interior Bruto.

[15] EUROPEAN COMMISSION COMMUNICATION: "Unleashing the Potential of Cloud Computing in Europe". Bruselas, 2012, p.2. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

Muchos coinciden en que el Cloud Computing se erigirá como la clave de una nueva Revolución Industrial,[16] llegando a referirse a la nube como "el vapor del siglo XXI".[17] En mirada retrospectiva, puede afirmarse que lo verdaderamente importante de la Revolución Industrial del siglo XIX no fue la incorporación del vapor como combustible para el transporte *per se*, lo que hizo que la fuerza del vapor resultara mejor que la de un caballo para la sociedad, fueron las nuevas posibilidades que el vapor trajo consigo: un desplazamiento más rápido y más potente, capaz de crear nuevas oportunidades que simplemente no podrían haber existido sin él (p.ej. el transporte aéreo y marítimo). En el ámbito de las TI, lo que hace que el Cloud Computing pueda traer más beneficios para la sociedad que la computación tradicional, incluida la computación del *mainframe*,[18] son precisamente esas nuevas posibilidades que se abren por virtud de una computación más rápida, potente, fácil y barata: nuevos modelos de negocio, reducción de costes, y mayor competencia por virtud de la eliminación de barreras tecnológicas de entrada al mercado.

[16] Sobre éste tema, véase RIFKIN, Jeremy: "La Tercera Revolución Industrial: Cómo el poder lateral está transformando la energía, la economía y el mundo", Editorial Paidós, 2011.

[17] MENEGAZ, Gery: "Cloud Computing: the 4th IT Industrial Revolution!". ZDNet, 2012. Disponible en: http://www.zdnet.com/article/cloud-computing-the-4th-it-industrial-revolution/

[18] Hacia 1950, los mainframes estaban a disposición de grandes organizaciones y gobiernos. Los usuarios iniciaban sesión en un terminal que dependía íntegramente del mainframe para funcionar (de hecho, se le denominaba "terminal tonto"). Este modelo es bastante análogo al Cloud Computing, con la diferencia de que en lugar de una unidad central o mainframe en el centro de una habitación, los servicios se basan en una infraestructura global de servidores y centros de datos para hacer el trabajo pesado. Sobre esta analogía véase: http://gizmodo.com/what-is-the-cloud-and-where-is-it-1682276210

La arquitectura del Cloud Computing es básicamente un espejo de la arquitectura de Internet, una red de comunicaciones que se extiende por la tierra, en la que los que los datos cruzan las fronteras jurisdiccionales millones de veces cada segundo de forma transparente para el usuario. Ante este escenario, surgen distintos retos en materia de privacidad y seguridad en el marco de la contratación de servicios de Cloud Computing en el ámbito B2B:

1. El primer reto que nos encontramos es el encaje de esta realidad tecnológica con normas pre- Internet en materia de privacidad y protección de datos, que restringen los movimientos internacionales de datos.

2. El segundo reto que plantea el tratamiento multijurisdiccional de la información, tiene que ver con el correcto entendimiento de las cuestiones sobre ley aplicable y la jurisdicción competente de cara a una adecuada valoración y gestión de riesgos, en tanto y en cuanto éstas cuestiones pueden afectar a la privacidad y seguridad de los datos; y de cómo estas cuestiones pueden o no regularse contractualmente por las partes.

3. El tercer reto que plantea la transnacionalidad de los es la adecuada comprensión de los eventuales poderes de acceso de los Estados a través de sus autoridades competentes a los datos tratados en servicios de Cloud

Computing, de las garantías aplicables y de la limitaciones de dichos poderes, así como de los mecanismos de cooperación internacional que pueden activarse por parte de los distintos Estados para obtener dicho acceso. A los efectos de la gestión de los riesgos de privacidad y seguridad, resulta imprescindible distinguir el acceso gubernamental ilegal frente al acceso gubernamental amparado en la ley, son cuestiones distintas y los riesgos asociados a cada una de estas actividades deben gestionarse de forma distinta por parte de las organizaciones.[19]

4. El cuarto reto gira en torno a la seguridad de la información que se trata en los servicios de Cloud Computing, esto es, su confidencialidad,[20] integridad[21] y disponibilidad[22] cuya gestión externaliza en el proveedor de servicios, en particular, este reto se materializa en cuatro aspectos que aparecen respectivamente en distintos momentos del proceso de contratación, a saber: (i) los niveles de seguridad apropiados para los activos de información en

[19] La atención sobre la injerencia gubernamental sobre las redes de comunicaciones y los servicios de Internet crecieron sustancialmente tras desvelarse en 2013 el alcance de los programas de vigilancia llevados a cabo por agencias de seguridad nacional e inteligencia como la NSA en los Estados Unidos y en GCHQ en el Reino Unido, entre otras.

[20] Según la norma ISO/IEC 13335-1:2004 es la característica o propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

[21] Según la norma ISO/IEC 13335-1:2004 es la característica o propiedad de salvaguardar la exactitud y completitud de los activos.

[22] Según la norma ISO/IEC 13335-1:2004 es la característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

cuestión (ii) la determinación de si un proveedor o servicio particular puede cubrir estos niveles o no (iii) las garantías contractuales que resultan exigibles al proveedor, y (iv) los mecanismos que permitirán al cliente de Cloud Computing la verificación de la implantación efectiva de los niveles de seguridad esperados. [23] Los dos primeros aspectos se deben abordar en la fase pre-contractual, los dos segundos se concretan en la fase contractual propiamente dicha, y tienen relevancia en la fase *post* contractual.

A la luz de lo retos descritos, la presente Tesis Doctoral responde a las siguientes preguntas (i) ¿Qué tipo de movimientos internacionales ocurren en el Cloud Computing? ¿Cuál es su régimen jurídico desde la perspectiva de la privacidad? (ii) ¿Qué ley resulta aplicable a los datos en la nube?, ¿Cuál es la jurisdicción competente? (iii) ¿Qué reglas rigen el acceso gubernamental a los datos en la nube? ¿Qué mecanismos de cooperación internacional existen en materia de acceso gubernamental a la información en la nube? (iv) ¿Cómo pueden gestionarse los riesgos de privacidad y de seguridad en una relación contractual entre organizaciones? ¿Qué niveles de seguridad son exigibles en el Cloud Computing?.

[23] En España, esta preocupación suele estar orientada principalmente hacia el cumplimiento de la normativa de en materia de protección de datos de carácter personal, debido a que es la más desarrollada y rigurosa en Europa y en el mundo entero, con relación a aspectos que afectan directamente al Cloud Computing, como son las medidas de seguridad y las transferencias internacionales de datos.

A lo largo del análisis se proponen soluciones prácticas para abordar estos riesgos en el ámbito jurídico y técnico, y que permiten conciliar la adopción de servicios de Cloud Computing con la protección efectiva de los activos de información, y con el cumplimiento de la normativa aplicable en un contexto regulatorio complejo. El análisis se restringe a las relaciones B2B producto de la externalización de servicios de TI, en las que, en consecuencia, el cliente es el responsable del tratamiento y el proveedor de Cloud Computing es un mero encargado de tratamiento que actúa bajo las Instrucciones del primero.

2. CAPÍTULO I. GENERALIDADES SOBRE EL CLOUD COMPUTING

2.1. Origen del término

El término Cloud Computing, busca representar por un lado, a Internet como si fuera una nube (cloud) y por otro, a los recursos de computación (computing) tradicionales como el hardware y el software. La unión apunta a que estos recursos de computación tradicionales, están ahora disponibles a través de la Red.

2.2. Concepto

Cloud Computing ha sido definido por el National Institute of Standards and Technology (NIST) como *"*Un modelo para habilitar acceso conveniente por demanda a un conjunto compartido de recursos computacionales configurables, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente provisionados y liberados con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios*"*. [24]

[24] MELL, Peter; GRANCE, Timothy: "THE NIST Definition of Cloud Computing" Gaithersburg, 2011, p.6. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Por su parte, la Cloud Security Alliance (CSA), organización internacional de referencia en materia de seguridad en el ámbito del Cloud Computing, ha asumido también esta definición.[25]

2.3. Objetivos del Cloud Computing

Los objetivos del Cloud Computing son fundamentalmente (i) el aprovechamiento de economías de escala[26] y (ii) el incremento de la flexibilidad de los recursos de tecnologías de la información (TI) de las organizaciones.

La nube permite el aprovechamiento de las economías de escala que se pueden generar, por parte de operadores que prestan servicios estandarizados a un gran número de clientes, pudiendo disminuir los costes de los servicios que ofrecen.

Asimismo, la flexibilidad del modelo permite a las organizaciones escalar rápidamente en función de sus necesidades, dotándolas así de una enorme capacidad de procesamiento, almacenamiento y gestión, sin necesidad de instalar

[25] CLOUD SECURITY ALLIANCE: "Guía para la seguridad en áreas críticas de atención en Cloud Computing" traducida al castellano por ISMS Forum Spain. Madrid, 2009, p.8. https://cloudsecurityalliance.org/guidance/csaguide-es.v2.pdf

[26] Para STIGLITZ "hay economías de escala cuando, al duplicar todos los factores, la producción aumenta en más del doble; y cuando hay economías de escala, la curva del coste total a medio a largo plazo tiene pendiente negativa". STIGLITZ, Joseph E., WALSH, Carl E.: Microeconomía, Barcelona, 2009, p. 175.

servidores localmente y sin tener que añadir equipamiento, o contratar personal para operarlo, pagando según un modelo de cálculo que se basa en el uso (capacidad o número de usuarios).

2.4. Beneficios del Cloud Computing

Para algunos, la computación en nube es una de las mayores revoluciones tecnológicas de los últimos tiempos. Para otros, es solamente la evolución un conjunto de tecnologías destinadas que permiten ofrecer la computación como un servicio más a través de Internet.

En su expresión más simple, el Cloud Computing es una nueva forma de entregar recursos de computación a través de Internet. Los sistemas de Cloud Computing tienen su anclaje en enormes colecciones de servidores que, gracias al software que los une, trabajan como un único cerebro capaz de dispersar los distintos trabajos de forma eficiente. La nube estandariza y comparte recursos, automatizando muchas de las tareas de mantenimiento realizadas que tradicionalmente se han hecho de forma manual. Debido a que existe menos desperdicio de recursos y más flexibilidad, la computación como un todo resulta mucho más potente que la suma de sus distintos componentes.[27]

[27] HARDY, Q: "Computing Goes to the Cloud. So Does Crime" New York Times. Diciembre, 2014. http://bits.blogs.nytimes.com/2014/12/02/computing-goes-to-the-cloud-so-does-crime/

Desde una perspectiva económica, gracias a las economías de escala inherente a la nube, ha visto la luz una computación más avanzada, barata y en algunos casos más segura, que puede alquilarse como un servicio, sin tener que adquirir la propiedad de las distintas partes y asumir los costes de operación y mantenimiento.

2.5. Cloud Computing frente al outsourcing tradicional

La computación en la nube no debe confundirse con los modelos de alojamiento o *hosting* tradicionales (hosting dedicado, hosting gestionado o hosting compartido) ni tampoco con la mera externalización de infraestructuras o servicios TIC hacia un proveedor de servicios. Las particularidades de la computación en la nube se centran en su propia definición: Un servicio abstraído de la tecnología sobre la que corre, fácilmente escalable, en la que **se paga por el uso de los recursos que se consumen en cada momento**, y por supuesto, con un componente de virtualización muy relevante.

El Cloud Computing se diferencia del modelo de outsourcing TIC tradicional, en que en éste último existe una computación autónoma e independiente, el contratante sabe en todo momento donde están alojados los datos y qué recursos se comparten con terceros, si es que se comparten, y los datos están vinculados a una infraestructura determinada. En la nube, el Servicio se desvincula de la

infraestructura y el contratante no tiene en absoluto transparencia de los recursos que le están dando servicio en cada momento.[28]

2.6. Características de los servicios de Cloud Computing

Las características del Cloud Computing gira principalmente en torno a cinco aspectos: recursos compartidos, escalabilidad masiva, elasticidad, pago por uso, y posibilidad de autoservicio por parte del usuario.[29]

Según NIST, los servicios en la nube contienen cinco características esenciales[30] que ejemplifican sus similitudes y diferencias con otros modelos de computación tradicionales, a saber:

a) Autoservicio a la carta y amplio acceso a la red

La nube permite al usuario abastecerse unilateralmente de capacidades de computación según sus necesidades, de forma automática, y sin requerir la

[28] WANG Chenxi: How Secure Is Your Cloud? Forrester Research, Cambridge, 2009, p. 2- 3.

[29]MATHER Tim, KUMARASWAMY Subra, SHAHED Latif: "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance". California-USA, 2009, p.7.

[30] CLOUD SECURITY ALLIANCE: "Guía para la seguridad en áreas críticas de atención en Cloud Computing" traducida al castellano por ISMS Forum Spain. Madrid, 2009, p.8. https://cloudsecurityalliance.org/guidance/csaguide-es.v2.pdf

interacción humana con el proveedor. Las capacidades de computación están disponibles en Internet, y puede acceder a ellas a través de mecanismos estándar (p.ej., teléfonos móviles, portátiles y PDAs).

b) Reservas de recursos en común

Los recursos computacionales del proveedor se ponen en reservas comunes para que puedan ser utilizados por múltiples consumidores, en el caso de que hayan elegido el modelo de nube pública (que es el modelo de nube disruptivo por excelencia). Estos recursos físicos y virtuales, son asignados dinámicamente y reasignados en función de la demanda de los consumidores. Existe un sentido de independencia de la ubicación física en que el cliente generalmente no tiene control o conocimiento sobre la ubicación exacta de los recursos suministrados, aunque se puede especificar una ubicación a un nivel más alto de abstracción (p.ej. país, región, o grupos de centro de datos). Algunos ejemplos de recursos son: almacenamiento, procesamiento, memoria, ancho de banda de la red y máquinas virtuales.

c) Rapidez y elasticidad

Las capacidades de computación pueden suministrarse de manera rápida y elástica, en algunos casos de manera automática, para poder realizar el redimensionado

correspondiente rápidamente. Para el consumidor, las capacidades disponibles para abastecerse a menudo aparecen como ilimitadas y pueden adquirirse en cualquier cantidad y en cualquier momento.

d) Servicio supervisado

Los sistemas de nube controlan y optimizan el uso de los recursos de manera automática utilizando una capacidad de evaluación en algún nivel de abstracción adecuado para el tipo de servicio (p.ej., almacenamiento, procesamiento, ancho de banda, y cuentas de usuario activas). El uso de recursos puede seguirse, controlarse y notificarse fácilmente, lo que aporta transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

2.7. Clasificación de los servicios de Cloud Computing

Los servicios en la nube pueden clasificarse atendiendo al modelo de servicio y también atendiendo a la titularidad de la infraestructura sobre la que están desplegados estos servicios.

2.7.1. Por el modelo de servicio

Atendiendo al modelo de servicios prestados (según se ofrezcan software, plataformas o infraestructuras) la clasificación es la siguiente:

a) Aplicaciones en modo servicio

Bajo este modelo mejor conocido como por su denominación en inglés, *Software as a Service* (SaaS) el proveedor permite el acceso a aplicaciones que están ejecutándose en su infraestructura Cloud, en consecuencia, el término SaaS se refiere a aquellas aplicaciones "consumidas" por el usuario a través de Internet y cuyo pago está condicionado por el uso efectivo de las mismas, sin la adquisición previa de una licencia.

SaaS implica que el usuario no ostenta la gestión ni el control de elementos como la infraestructura base, los servidores, los sistemas operativos o el almacenamiento asociado a las aplicaciones, por ello cuando hablamos de SaaS, nos referimos a que tanto las propias aplicaciones como los datos están alojados en la plataforma del proveedor de Cloud.

b) Plataforma como un servicio

Bajo este modelo mejor conocido por su denominación en inglés, *Platform as a Service* (PaaS) el usuario tiene la capacidad de desarrollar aplicaciones sobre la infraestructura del proveedor utilizando herramientas y lenguajes de programación cuyo mantenimiento está a cargo de dicho proveedor. PaaS implica que el usuario no ostenta la gestión ni el control de elementos como la infraestructura base, los servidores, los sistemas operativos o el almacenamiento, pero que tiene el control sobre la configuración de las aplicaciones desarrolladas y la posibilidad de solicitar las configuraciones propias del entorno host. Al igual que en SaaS, tanto la propia aplicación, como los datos, residen en la plataforma del proveedor de Cloud.

c) Infraestructura como un servicio

Bajo este modelo mejor conocido por su denominación en inglés, como *Infrastructure as a Service* (Iaas) el proveedor proporciona servicios de procesamiento, almacenamiento, redes y otros recursos fundamentales, donde el usuario puede desarrollar y ejecutar aplicaciones. El usuario no gestiona ni controla la infraestructura base pero sí que tiene control sobre los sistemas operativos, el almacenamiento, las aplicaciones desarrolladas y posibilidad de seleccionar elementos de red (firewalls, balanceadores, etc.). Evidentemente en el modelo IaaS, las aplicaciones y los datos residen también en la plataforma del proveedor de Cloud.

2.7.2. Por la titularidad de la infraestructura

Atendiendo a la titularidad de la infraestructura de Cloud, se pueden distinguir tres tipos, a saber:[31]Privada, Pública, Comunitaria e Híbrida.

a) Pública

Es aquel tipo de Cloud en el cual la infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles al público en general a través de Internet. Suele ser propiedad de un proveedor que gestiona la infraestructura y el servicio o servicios que se ofrecen, aunque puede haber nubes públicas que se basan en infraestructuras de terceros.

b) Privada

Este tipo de infraestructuras Cloud se crean con los recursos propios de la empresa que lo implanta, generalmente con la ayuda de empresas especializadas en el despliegue de este tipo de tecnologías.

c) Comunitaria

[31]INTECO-CERT: "Riesgos y Amenazas en Cloud Computing". León, 2011, p.6. http://sie.fer.es/recursos/richImg/doc/14829/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

Una nube comunitaria se da cuando dos o más organizaciones forman una alianza para implementar una infraestructura Cloud orientada a objetivos similares y con un marco de seguridad y privacidad común.

d) Híbrida

Este es un término amplio que implica la utilización conjunta de varias infraestructuras Cloud de cualquiera de los tres tipos anteriores, que se mantienen como entidades separadas, pero que a su vez se encuentran unidas por la tecnología estandarizada o propietaria, proporcionando una portabilidad de datos y aplicaciones.

3. CAPÍTULO II. MOVIMIENTOS INTERNACIONALES DE DATOS

3.1. Flujos de datos en el Cloud Computing

El volumen de los movimientos internacionales de datos a nivel global ha crecido exponencialmente en los últimos años,[32] potenciado fundamentalmente por el avance de las redes de comunicaciones, la penetración de Internet, y el desarrollo servicios de la sociedad de la información, entre ellos, el Cloud Computing.[33] Estos movimientos transfronterizos de datos constituyen la base que conecta los flujos de la economía mundial: bienes, servicios, finanzas, y personas.[34]

Para entender cómo se producen estos movimientos de datos en la nube, debemos recurrir en primer lugar a la arquitectura de Internet, la columna vertebral del Cloud Computing. Internet es básicamente una red de comunicaciones que se extiende por la tierra, en la que los que los datos cruzan las fronteras jurisdiccionales millones de veces cada segundo de forma transparente para el usuario. Precisamente, una de las

[32] Según McKinsey, el tráfico global de Internet creció desde 84 petabytes al mes en el año 2000, a más de 40.000 petabytes al año 2012, un incremento de 500 veces. Vid. McKinsey Global Institute: "Global flows in a digital age: How trade, finance, people, and data connect the world". 2014, p.5.

[33] Según la Unión Internacional de Telecomunicaciones, a finales de 2014 el número de usuarios de Internet en todo el mundo alcanzó casi los 3 mil millones, mientras que los abonados a telefonía móvil sumaron casi 7 mil millones. Vid. ITU Yearbook of Statistics. Ginebra, 2014.

[34] Vid. McKinsey Global Institute: "Global flows in a digital age: How trade, finance, people, and data connect the world". 2014.

características esenciales del Cloud Computing es su amplio acceso de red[35] en el sentido de que los servicios, y en consecuencia, los datos, pueden ser accedidos por sus usuarios desde cualquier ubicación geográfica, a través de cualquier dispositivo conectado a Internet.

Desde la perspectiva del proveedor, existe una infraestructura de procesamiento y almacenamiento que forma los centros de datos. Estos centros de datos se encuentran distribuidos en distintos países y con frecuencia distintas regiones para cubrir adecuadamente los objetivos de seguridad del servicio, en cuanto a su disponibilidad e integridad. No todos los países en los que un proveedor de Cloud opera cuentan con un centro de datos. Desde la perspectiva económica, la nube es fundamentalmente no territorial, en el sentido de que alcanza su máximo beneficio económico si no es territorial[36]. De hecho, los requisitos de localización de datos a menudo impiden el acceso a servicios globales de computación en nube.[37]

El propósito del entorno de computación distribuida sobre una base global es permitir gran flexibilidad en las decisiones de tratamiento para lograr altos niveles de

[35] NIST: "The NIST Definition of Cloud Computing", 2011, p2. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[36] KUTTERER, C: "Law enforcement internet jurisdiction". Intervención en CDPD 2015, min. 43. Disponible en: https://www.youtube.com/watch?v=NL4nNlzyqmQ

[37] CHANDER, Anupam and LE, Uyen P.: "Breaking the Web: Data Localization vs. the Global Internet". Emory Law Journal, Forthcoming; UC Davis Legal Studies Research Paper No. 378. 2014, 40. Disponible en SSRN: http://ssrn.com/abstract=2407858

rendimiento y disponibilidad. Por ejemplo, las actividades de computación pueden desplazarse de un centro de datos o de un país a otro en función de la capacidad de carga, la hora del día, los picos de demanda, la necesidad de evitar latencia; o de realizar réplicas y/o copias de seguridad para la recuperación de los datos en caso de fallos en los equipos, o para garantizar la resiliencia del servicio ante amenazas físicas (p.ej. desastres naturales) o cibernéticas (p.ej. ataques maliciosos). Asimismo, en algunos casos los datos se almacenan troceados en fragmentos[38] que residen en distintos servidores, en distintos centros de datos y en distintas jurisdicciones para proveer servicios a gran escala de forma global, procurando la eficiencia y fiabilidad de acceso a los datos.

Como puede verse, los movimientos internacionales de datos que se producen en la nube son complejos, en el sentido de que no constituyen una transmisión de un punto a otro, sino que ocurren como parte de una serie de procesos conectados hechos para entregar un resultado de negocio.[39]

[38] Por ejemplo, en el sistema de archivos Google, Google File System los datos no se almacenan como un todo, estos se fragmentan en piezas. A estas piezas se les asignan nombres de archivo aleatorios y se guardan en texto ofuscado a fin de que sean ininteligibles a los humanos. En este sentido, véase GHEMAWAT, S. GOBIOFF, H, and LEUNG, S.T: "The Google File System". 2003.

[39] SCHWARTZ M., Paul: "Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment". UC Berkeley School of Law. USA. 2009. p.5.

3.2. Privacidad y seguridad de los datos en movimiento

Desde una perspectiva puramente técnica, las fronteras resultan irrelevantes para Internet y, por tanto, para los servicios de Cloud Computing. Es por ello que en la nube debe hablarse de protecciones jurídicas y técnicas centradas en los activos de información con independencia de su ubicación temporal o permanente en lugar de protecciones centradas en un territorio, o una infraestructura determinada, ya que estos elementos son dinámicos.

Las garantías de privacidad y seguridad establecidas en un contrato deben ser uniformes con independencia de donde ocurra el procesamiento o el almacenamiento de los datos. Dichas garantías deben, como mínimo, cumplir con la normativa aplicable.[40] No obstantes, en relación con la seguridad de los activos de información, debe tenerse en cuenta que el cumplimiento de la normativa no necesariamente implica la protección efectiva de los activos de información contra las principales riesgos en el ciberespacio,[41] como los ataques a la confidencialidad por

[40] A la luz de la Directiva 95/46/CE, el régimen de protección de datos aplica al responsable del tratamiento y su cumplimiento debe garantizarse por el mismo, salvo en lo relativo a las medidas de seguridad, que resultan aplicables a los encargados del tratamiento encargado del tratamiento. No obstante, conviene destacar que la propuesta del Reglamento General de Protección de Datos pretende cambiar este enfoque, estableciendo un régimen general de obligaciones directamente aplicable al encargado del tratamiento.

[41] Por ejemplo, en España el RLOPD no exige la implantación de controles recomendables como el doble factor de autenticación, el cifrado en reposo, o la realización de ciberejercicios para probar la seguridad del código de las aplicaciones web frente a vulnerabilidades comunes como el *cross site scripting*.

parte de hackers y otros actores maliciosos. Estos actores maliciosos pueden ser privados (p.ej. bandas organizadas de cibercrimen) pero también estatales (p.ej. gobiernos y agencias de inteligencia). En definitiva, la privacidad y la seguridad son dos caras de la misma moneda, la información no puede ser privada si no está segura.

3.3. Restricciones legales a los movimientos internacionales de datos

Desde sus inicios, el fenómeno de los movimientos internacionales de datos atrajo el interés de reguladores y *policy maker*s debido al potencial impacto que estos flujos podían tener para la privacidad de las personas físicas, así como para la seguridad de los datos en sentido amplio.

Hoy no existe ni una regulación con alcance global en materia de privacidad, ni tampoco existe un acuerdo pacífico para la regulación de los movimientos de datos en un mundo global hiperconectado, no obstante, el uso de Internet y de servicios y funcionalidades basadas en él tales como el Cloud Computing, las Redes Sociales, en Big Data, y el Internet de las cosas, es imparable. La materia tiene importantes implicaciones no solo en el ámbito de la privacidad y protección de datos personales, sino en el ámbito del derecho internacional público y privado, y en el comercio

internacional. No en vano, la regulación de estos movimientos transfronterizos de datos ha sido y es hoy día uno de los puntos de más fricción en los procesos regulatorios (unilaterales y multilaterales), y uno de los principales obstáculos en el intento de armonizar la privacidad a nivel global.[42]

El Convenio 108 del Consejo de Europa, la Directiva 95/46/CE, y el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (Marco APEC) de 2005[43] son los principales instrumentos multilaterales de referencia en la materia, no obstante, estos tienen un enfoque completamente distinto; mientras que el Convenio y la Directiva apuntan a un modelo restrictivo de las transferencias internacionales, sujeto a distintos niveles de autorización previa y trámites que en ocasiones se tornan lentos y burocráticos, el Marco APEC establece un modelo permisivo y flexible, sujeto a la autorregulación y supervisión por parte de los propios actores privados.

El Convenio 108 establece las bases para la restricción de los flujos internacionales de datos y propone un sistema de protección centrado en países, asumiendo que los datos se encuentran protegidos por el mero hecho de residir en un territorio, lo cual

[42] En este sentido, véase la Sección 2.6 en relación con la Resolución de Madrid sobre Estándares Internacionales sobre Protección de Datos Personales y Privacidad.

[43] El Convenio 108 del Consejo de Europa y la Directiva 95/46/CE se encuentran actualmente bajo revisión.

no necesariamente se produce. En esta línea, la Directiva se consagra una restricción a las exportación de datos fuera del Espacio Económico Europeo, cuyo desarrollo varía entre los Estados Miembros. Con frecuencia estos desarrollos se han traducido en autorizaciones administrativas y notificaciones burocráticas cuyo beneficio para los titulares de los datos en cuestión es incierto. Por su parte, el Marco APEC establece flexibilidad en el libre movimiento internacional de datos, sujeta a la protección efectiva y a la responsabilidad de las organizaciones importadoras, para lo cual promueve un modelo de autorregulación. La falta de un mecanismo de supervisión independiente que pueda determinar cuándo esta protección efectiva se produce ha sido una de las fuentes principales de criticismo hacia este marco. Por su parte, la Resolución de Madrid ha sido uno de los esfuerzos internacionales más recientes en la armonización de posturas en materia de privacidad a nivel global, incluyendo los movimientos internacionales de datos.

Mientras tanto, más de 70 países han adoptado sus marcos normativos nacionales de privacidad o protección de datos que expresamente regulan las transferencias internacionales de datos.[44]

Actualmente, los flujos transfronterizos se negocian en tres acuerdos comerciales de distinta índole:

[44] Sobre los distintos marcos nacionales, véase DLA Piper: "Data Protection Laws of the World". 2013. Disponible en: http://dlapiperdataprotection.com/

- Los EE.UU. y la UE negocian el Comercio y la Inversión de Asociación Transatlántica (T-TIP).[45]
- Los EE.UU. negocian la Asociación Transpacífico con países de la región de Asia Pacífico (T-PP).[46]
- Los EE.UU. y Australia negocian el Acuerdo del Comercio en Servicios con 49 países que representan el 70 por ciento del comercio mundial (T-ISA).[47]

A pesar de la importancia de los flujos de datos transfronterizos, muchos gobiernos no han respondido positivamente a la idea de facilitar el libre flujo de información. Se ha afirmado que la preocupación por la capacidad de controlar o limitar los flujos de información por parte de los Estados ha sido producto de su preocupación por la dependencia de las empresas de Estados Unidos para proporcionar tecnología, y con el deber de estas compañías de cumplir con sus normas nacionales en materia de privacidad y seguridad nacional.[48]

[45] Por sus siglas en inglés, Transatlantic Trade and Investment Partnership. https://ustr.gov/ttip

[46] Transpacific Partnership. Disponible en: https://ustr.gov/tpp

[47] Trade in Services Agreement. Disponible en: http://servicescoalition.org/negotiations/trade-in-services-agreement

[48] Aaronson, Susan: "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security". APSA 2014 Annual Meeting Paper. Disponible en SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2453025

3.4. Enfoque Europeo de Regulación

3.4.1. Convenio 108 del Consejo de Europa

a) El nacimiento del concepto de protección de datos

El concepto de protección de datos se acuñó hace más de tres décadas con el fin de proporcionar protección legal a los individuos frente al uso inadecuado de las tecnologías de información para el tratamiento de información concerniente a ellos. Así, en el año 1981 aparece el Convenio 108[49] del Consejo de Europa con el objeto de hacer frente a una naciente realidad denominada el "Poder de la Información" habilitado por la tecnología. Hubo una convicción temprana y acertada de que el uso extensivo de la tecnología de la información podría tener efectos de largo alcance para los derechos e intereses de los individuos.

Antes de 1981, los Estados Miembros no carecían totalmente de reglas que pudieran ayudar a lograr los objetivos del Convenio 108, en aquél momento, algunos ya contaban con leyes sobre la privacidad y la confidencialidad de la información

[49] El Convenio 108 es el único instrumento internacional existente con poder vinculante en el área de la protección de datos. La mayoría de los signatarios del Convenio también son Estados miembros del Consejo de Europa. El Convenio también está abierto a países no pertenecientes al Consejo de Europa. Hasta la fecha, Mauricio, Marruecos Senegal y Uruguay lo han suscrito en calidad de no miembros, este último también ha procedido a ratificarlo.
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG

sensible, sin embargo, carecían de normas generales sobre el almacenamiento y uso de los datos de carácter personal y, en particular, sobre la cuestión de cómo los individuos podían ejercer un **control** sobre la información relativa a ellos mismos que era recogida y usada por otros.

El Convenio 108 trajo consigo una responsabilidad *ex ante* para actores público y privados, pues se introdujo por primera vez el deber de mantener la buena calidad de la información bajo su custodia, abstenerse de almacenar de información que no fuera necesaria para un propósito específico, protegerla contra la divulgación no autorizada, y proteger los datos, hardware y software contra daños físicos,[50] entre otros.

b) Las primeras restricciones a los movimientos internacionales de datos

Las restricciones a los movimientos de datos fuera de un territorio están ligadas al nacimiento del concepto de protección de datos y a su regulación en el Convenio 108. Así, el artículo 12.2 del Convenio establece que "Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra

[50] Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), Informe Explicativo, 1981. http://conventions.coe.int/Treaty/en/Reports/Html/108.htm

Parte". Por interpretación en contrario, se establecen de esta manera las bases para las restricciones de los flujos de datos originados en Estados Parte del Convenio hacia el territorio de Estados que no lo son.

La motivación predominante para imponer dichas restricciones fue el temor de que sin ellas el tratamiento de datos se trasladaría a países sin leyes adecuadas de protección de datos con el objetivo de evitar la aplicación de ley Europea,[51] lo que se traduciría en detrimento de los derechos de los individuos. No obstante, para algunos el intento europeo de restringir los flujos de información buscaba además la protección de la economía local frente a las compañías estadounidenses que empezaban a jugar un papel predominante en el ámbito tecnológico.[52] Bortnick resumió esta última cuestión en 1979 de la siguiente manera: "EE.UU. mantiene un liderazgo sustancial en el campo de la computación y las comunicaciones, con equipos y software estadounidenses dominando los mercados mundiales. Numerosas preocupaciones han aflorado por parte tanto de países desarrollados como en vías de desarrollo como resultado de su uso de medios computacionales de propiedad y operados por compañías estadounidenses multinacionales. Estos países han puesto el foco sobre el hecho de que una parte sustancial de datos personales

[51] KUNER, Christopher "Transborder Data Flows and Data Privacy Law", United Kingdom, 2013, p.158.

[52] En este sentido, puede consultarse Bortnick, Jane: "International Data Flows Issues". Issue brief number IB81040. 1983. Disponible en http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=577604

de sus ciudadanos, información comercial, y datos económicos nacionales están siendo procesados y almacenados en sistemas de información automatizados fuera de sus países. Por su parte, EE.UU se ha manifestado preocupación de que las compañías estadounidenses sean tratada de forma desleal en el uso de los servicios de comunicaciones ofrecidos por gobiernos extranjeros para la transmisión de datos, en particular en relación con políticas y precios discriminatorios, así como la monitorización de flujos de información". Muchos de los elementos de este debate siguen vigentes hoy día.

No obstante, cabe destacar que el concepto de protección de datos no fue diseñado para evitar el tratamiento de dicha información o limitar el uso de la tecnología de la información *per se*. En cambio, se diseñó para proporcionar garantías cuando las tecnologías de información se utilizan para el procesamiento de la información concerniente a los individuos.[53]

3.4.2. Directiva 95/46/CE

La Directiva 95/46/CE constituye el marco de referencia de la protección de datos en Europa y posiblemente el instrumento de referencia en la materia más importante a nivel mundial en la actualidad. La Directiva establecen ciertos principios que los

[53] HUSTINX, Peter, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2014 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf

Estados Miembros han tenido que transponer en sus respectivos ordenamientos, a saber: información, consentimiento, finalidad, calidad, seguridad; derechos de acceso, rectificación, cancelación y oposición (en adelante, derechos ARCO), autoridad de control independiente, y limitación a las transferencias internacionales de datos. A nivel global existe un acuerdo bastante uniforme en relación con estos principios, a excepción de los derechos ARCO, las restricciones a los movimientos internacionales de datos y la existencia de una autoridad de control independiente.

Estos principios han servido también como fuente de inspiración para otras legislaciones, principalmente de corte continental, que han incorporado en cierta medida estos principios, en primer lugar en aras de proteger los derechos de sus ciudadanos, pero también, para favorecer el tráfico económico con los países miembros de la Unión Europea. Argentina, Chile y Colombia, México y Uruguay son algunos ejemplos en este sentido, aunque solo Argentina y Uruguay han conseguido la declaración de "nivel adecuado de protección" por parte de la Comisión Europea para ser importadores de datos provenientes del Espacio Económico Europeo en las mismas condiciones que un Estado Miembro, es decir, sin restricciones.

De conformidad con el artículo 25.1 de la Directiva, "Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales (...) únicamente pueda efectuarse cuando (...) el país tercero de que se trate garantice un nivel de protección adecuado."

Por su parte, el artículo 25.2 dispone que "El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países". La Comisión podrá hacer constar que un país tercero garantiza un nivel de protección adecuado con arreglo a estos extremos, a la vista de su legislación interna o de sus compromisos internacionales. En este caso, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión (Art. 26.6).

Hay quienes opinan que la intención de esta restricción fue la ejercer cierta presión sobre terceros países fuera del Espacio Económico Europeo para que estos adoptasen estándares de protección de datos similares a los de la UE.[54] Lo cierto es que, 20 años después, solo una lista reducida de 11 países ha recibido una decisión de adecuación por parte de la Comisión Europea:

[54] HON W. Kuan, MILLARD Christopher: "DATA EXPORT IN CLOUD COMPUTING – HOW CAN PERSONAL DATA BE TRANSFERRED OUTSIDE THE EEA? THE CLOUD OF UNKNOWING, PART 4", 2012, p.30. Disponible en: http://script-ed.org/wp-content/uploads/2012/04/hon.pdf

- Suiza, en virtud de la Decisión 2000/518/CE.
- Canadá, en virtud de la Decisión 2002/2/CE.
- Argentina, en virtud de la Decisión 2003/490/CE.
- Guernesey, en virtud de la Decisión 2003/821/CE.
- Isla de Man, en virtud de la Decisión 2004/411/CE.
- Jersey, en virtud de la Decisión 2008/393/CE.
- Islas Feroe, en virtud de la Decisión 2010/146/CE.
- Andorra, en virtud de la Decisión 2010/625/CE.
- Israel, en virtud de la Decisión 2011/61/CE.
- Uruguay, en virtud de la Decisión 2012/484/CE.
- Nueva Zelanda, en virtud de la Decisión 2013/65/CE.

Del mismo modo, sin perjuicio de lo anterior la Comisión haciendo uso de sus poderes ejecutivos podrá determinar que un tercer país no garantiza un nivel de protección adecuado, en cuyo caso los Estado miembros deberán adoptar las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate (Art. 25.4).

Ahora bien, el artículo 26 de la Directiva contempla una serie de excepciones a la restricción y consagra mecanismos de autorización para la realización de transferencias internacionales a terceros países que no han recibido las adecuación

respectiva por parte de la Comisión.[55] En materia de excepciones, el apartado 1 establece que se podrán transferir datos a un país que no garantice un nivel adecuado de protección bajo alguno de los siguientes supuestos:

a) Cuando el interesado haya dado su consentimiento inequívocamente,

b) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado,

c) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero,

d) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial,

e) Cuando la transferencia sea necesaria para la salvaguardia del interés vital del interesado,

f) Cuando la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o

[55] En virtud de sus normas de transposición, Francia, Portugal y España también pueden emitir decisiones de adecuación, sin embargo, ninguno de ellos lo ha hecho hasta el momento.

por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

La utilización de estas excepciones se restringe prácticamente a las relaciones cesiones o comunicaciones de datos que involucran *vis a vis* a dos responsables de tratamiento y no a las relaciones de encargo del tratamiento, por lo que su aplicación en el ámbito del Cloud Computing resulta prácticamente nula.

No obstante, en materia autorizaciones, el artículo 26.2 establece las bases que han permitido, junto con las decisiones de adecuación contempladas en artículo 25, dar encaje a los flujos internacionales de datos que se producen en el ámbito del Cloud Computing. El Artículo 26 dispone que los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado (i) cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas (26.2) (ii) cuando la Comisión decida que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes (26.4).

a) Transferencias Internacionales de Datos excluidas de la Directiva

En relación con la naturaleza tratamiento de datos personales, y por tanto los movimientos de datos regulados por la Directiva, la misma establece determinados supuestos que quedan excluidos que su ámbito de aplicación (Art 3.2). Así, se rigen por sus disposiciones específicas aquellos tratamiento de datos personales que se lleven a cabo fuera del ámbito de aplicación del Derecho Comunitario como los realizados en el marco del Segundo y Tercer pilar de la UE,[56] es decir, política exterior y de seguridad común, y cooperación policial y judicial en materia penal, respectivamente, los tratamientos que tengan por objeto la seguridad pública, la defensa, la Seguridad del Estado y las actividades del Estado en materia penal.[57]

b) ¿Qué se considera una Transferencia Internacional de Datos?

La Directiva no define las transferencias internacionales de datos, sin embargo, algunas normas de transposición sí lo han hecho. En España, el RLOPD define estas transferencias como aquel *"***tratamiento** de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un

[56] Títulos V y VI del Tratado Único Europeo.

[57] ARENAS RAMIRO, Mónica: "El Derecho Fundamental a la Protección de Datos en Europa". Tirant Lo Blanche. Valencia, 2006. p. 301.

tratamiento de datos por cuenta del responsable del fichero establecido en territorio español".[58]

A la luz de la Directiva, constituye **tratamiento de datos** prácticamente cualquier acción que se pueda llevar a cabo con los mismos, específicamente "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".[59]

Siguiendo esta definición de tratamiento de datos, la restricción a las transferencias internacionales aplicaría tanto cuando los datos se transmiten para ser **almacenados** fuera del Espacio Económico Europeo, como cuando los mismos son consultados de forma remota a través de Internet desde fuera de dicho espacio. Esto implica que las restricciones aplican en situaciones cotidianas de nuestro entorno como cuando un empleado accede a su correo electrónico o a una aplicación corporativa que contiene datos personales desde un país fuera del Espacio Económico Europeo, que no esté en la lista blanca de Comisión Europea citada *supra*. Por tanto, para la legitimidad de la

[58] RLOPD. Art. 5 (s).

[59] Directiva 95/46/CE. Art. 2(b).

acción, la organización en cuestión tendría que ajustarse a algunos de los mecanismos de autorización previstos en el artículo 26 de la Directiva desarrollado por las normas nacionales de transposición que resulten aplicables. Como se ha indicado, en España resultan de aplicación la LOPD y el RLOPD. A este respecto, la Agencia Española de Protección de Datos ha considerado que esta restricción aplica tanto en los casos en los que los datos se tratan dentro de un mismo grupo empresarial, como cuando se transfieren a un tercero.[60]

3.4.3. ¿Son realistas las restricciones a los movimientos de datos?

El marco europeo de protección de datos fue diseñado en un momento en el tiempo en el que Internet estaba apenas en fase de gestación, y en el que no se preveía el uso ubicuo de la información. El modelo de "restricción por defecto" se diseñó en un momento en el que las compañías manejan bases de datos centralizadas y movían información de un punto a otro, de forma similar a la que movían paquetería de una dirección a otra;[61] y en el que las transferencias internacionales eran una

[60] AEPD, Informe Jurídico 2001-000. http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/transferencias_internacionales/common/pdfs/2001-0000_Transferencias-Internacionales-de-datos-para-la-realizaci-oo-n-de-un-tratamiento-por-cuenta-del-responsable-del-fichero.pdf

[61] SCHWARTZ M., Paul: "Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment". UC Berkeley School of Law. USA. 2009. http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf, prefacio.

circunstancia excepcional. En consecuencia, la limitación de los flujos transfronterizo no solo atendía a un objetivo legítimo, sino que era compatible contexto tecnológico y aplicable en la práctica.

El legislador procedió a restringir el libre movimiento de la información de las fronteras sobre la base de cuatro premisas que han cambiado profundamente:

a) **Carácter excepcional de las transferencias:** En primer lugar, el sistema parte de la idea de que el tratamiento de datos ocurre dentro de unas fronteras determinadas, y de que las transferencias internacionales de datos son una cuestión excepcional. Esta premisa no resulta válida, en un entorno hiperconectado donde las transferencia internacionales de datos no son la excepción sino la regla. En nuestra era los datos atraviesan las fronteras jurisdiccionales millones de veces constantemente, seamos conscientes de ellos o no. Asimismo, los servicios de Cloud Computing están virtualmente al alcance de cualquier ciudadano y de cualquier empresa, a diferencia de lo que ocurría hace más de tres décadas cuando el coste del almacenamiento y transferencia de datos era tan elevado que su uso estaba casi exclusivamente acotado a grandes corporaciones y gobiernos.[62]

[62] FISHMAN, William L. Introduction to transborder data flows. Reprinted from Stanford journal of international law. v. 16, Summer 1980, p.21.

b) Carácter intencional: En segundo lugar, el sistema presupone que las transferencias sólo ocurren como consecuencia de una intención explícita de enviar información fuera de las fronteras de un territorio. Esta premisa tampoco resulta válida en la era del Cloud Computing, sin perjuicio de las particularidades de la arquitectura de Internet[63] y del enrutamiento de su tráfico, existe una casuística variadísima que se puede dar en función de los servicios que utilizan las partes para comunicarse, pensemos en algunos ejemplos que pueden darse en un servicio de correo electrónico SaaS:

- El remitente envía información a una persona que reside dentro de su mismo país, no obstante, los servidores de correo electrónico de dicha persona (el destinatario) están ubicados en un país tercero al que la Comisión no ha otorgado el "nivel adecuado de protección", por ejemplo, en la India.

- El remitente envía información a una persona que reside dentro de su mismo país, los servidores de correo electrónico de dicha persona (el destinatario) también están ubicados dentro las fronteras del país en cuestión, no obstante, el destinatario accede a sus correo electrónico

[63] Las comunicaciones entre partes ubicadas dentro del mismo territorio pueden hacer su tránsito a través de otros países debido a razones puramente técnicas, sin que las partes sean conscientes de ello.

mientras se encuentra de viaje en un país tercero al que la Comisión no ha otorgado el "nivel adecuado de protección", por ejemplo, en la India.[64]

c) **Comunicaciones punto a punto:** Las transferencias internacionales se entienden como una conexión limitada entre dos extremos ubicados en dos territorios distintos. Hoy en día las comunicaciones son ubicuas y multidireccionales, son un proceso continuo, también lo son las transferencias internacionales de datos. En los entornos de Cloud Computing, los datos no solo están siendo transmitidos activamente por razones de rendimiento cuando se encuentran en estado de almacenamiento, sino que estos están a disposición para su acceso por parte de las organizaciones, a través de sus usuarios en cualquier lugar del mundo donde exista una conexión a Internet, desde cualquier dispositivo. Tal y como apunta SCHWARTZ: "En el pasado reciente, las empresas en general, trabajaban con conjuntos modestos de datos y procesos localizados. En dicho modelo, un flujo internacional de datos era un evento ocasional, una excepción y no la regla, y los sistemas de procesamiento de datos se basaban generalmente a nivel nacional. Por otra parte, desde una perspectiva contemporánea, las últimas transferencias eran eventos relativamente estáticos, es decir que no se producen de forma

[64] Como se ha señalado anteriormente, se ha interpretado que de conformidad con la Directiva 95/46/CE, el acceso remoto a los datos constituye una transferencia internacional de datos.

> continua, y también involucraban un número bastante limitado de participantes en el procesamiento".[65]

Hoy día, en el ámbito corporativo las transferencias internacionales de datos juegan como es de esperarse un papel crucial. La falta de certeza provocada por la obsolescencia de las normas en Europa, la falta de una regulación uniforme a nivel de los Estados Miembros, y la imposibilidad de llevar a la práctica, genera serias dificultades. El cumplimiento en el terreno de los movimientos internacionales de datos el ámbito del Cloud Computing conlleva importantes retos a la luz de la Directiva (y sus normas de transposición) teniendo en cuenta que misma cuenta con un enfoque eminentemente territorial que presuponen que el tratamiento de la información se va a producir dentro de las fronteras de una jurisdicción concreta, lo cual no se corresponde con realidad de Internet y de los servicios en la nube.

No obstante, el panorama legislativo obsoleto, la Comisión Europea y los Estados Miembros han desarrollados distintos mecanismos complementarios para legitimar ciertos movimientos internacionales de datos fuera del Espacio Económico Europeo, siempre que los mismos aseguren un "nivel adecuado protección" para los derechos de los ciudadanos en el marco de la Directiva de protección de datos, si bien estos

[65] SCHWARTZ M., Paul: "Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment". UC Berkeley School of Law. USA. 2009. http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf, p.5.

mecanismos han permitido habilitar la adopción de servicios de Cloud Computing por parte de organizaciones europeas, la falta de uniformidad en el reconocimiento y la aplicación de dichos mecanismos a nivel de la UE constituye una barrera para su pleno desarrollo.

Precisamente, con el objeto adaptar la normativa a los desarrollos tecnológicos y a la globalización, Europa emprendió en 2012 una reforma de protección de datos. Así, la Comisión Europea presentó en enero de 2012 dos propuestas de nuevos instrumentos normativos, a saber: Un Reglamento General de Protección de Datos[66] y una Directiva de protección de datos en materia de cooperación policial y judicial.[67] Ambos textos se están tramitando actualmente mediante el procedimiento legislativo ordinario, con participación del Consejo y del Parlamento Europeo. Las partes esperan que el Reglamento se apruebe antes de finales de 2015, mientras que el debate sobre la Directiva de protección de datos en materia de cooperación policial y judicial se encuentra todavía en sus fases iniciales.

[66] En el apartado 2.4.4 se explican las principales novedades del proyecto de Reglamento en materia de transferencias internacionales de datos.

[67] Los documentos relativos a la reforma del marco legal de protección de datos en la UE pueden ser consultados en el siguiente enlace: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

3.4.4. Mecanismos legales disponibles al Cloud Computing

a) Los Principios de Safe Harbor

Tras la aprobación de la Directiva, reguladores y *policy makers* europeos se encontraron con un Internet en pleno desarrollo, y con la necesidad de facilitar el comercio internacional basado en el intercambio de datos más allá de las fronteras del Espacio Económico Europeo. Así, en el julio de 2000 la Comisión Europea, haciendo uso de los criterios de adecuación previstos en el art 25.2 de la Directiva, emitió la Decisión 2000/520/CE sobre la adecuación conferida de los principios de Safe Harbor aprobados por la Federal Trade Commission (FTC).[68] A estos principios pueden adherirse las empresas estadounidenses que quieran importar datos personales provenientes de los Estados miembros de la Unión Europea. La Decisión establece que se alcanza el "nivel adecuado" de protección de la transferencia de datos desde la UE EE.UU si las entidades adheridas a Safe Harbor cumplen los principios de puerto seguro para la protección de la vida privada, con objeto de proteger los datos personales transferidos de un Estado miembro a EE.UU.[69]

[68] Los principios de Safe Harbor fueron publicados por la FTC unos meses antes en el año 2000.

[69] Considerando (5).

La adhesión a Safe Harbor pretende asegurar la aplicación, por parte del importador, de unos niveles de protección que sean equiparables a los establecidos por la Directiva de protección de datos europea. En particular, con la adhesión el importador se obliga a observar los siguientes principios rectores en el tratamiento de los datos personales: Notificación e información; derecho de oposición a la comunicación de datos o a los usos incompatibles con el objeto inicial de la recogida, transferencias ulteriores, seguridad, calidad de los datos, reconocimiento de los derechos de acceso y rectificación a los afectados, y necesidad de adoptar mecanismos que brinden garantías para la aplicación de los principios.[70]

Los principios en su conjunto aplican cuando el importador actúa en calidad de responsable del tratamiento, es decir, cuando éste decide sobre la finalidad, contenido y uso de los datos, teniendo una relación directa con el titular de los mismos. En contraste, cuando el importador de datos actúa en calidad de encargado del tratamiento para prestar un servicio en nombre y por cuenta del responsable, como es el caso del Cloud Computing, resultan aplicables los principios de transferencias ulteriores, seguridad, y necesidad de adoptar mecanismos que brinden garantías para la aplicación de los principios. Por su parte, los derechos de acceso y rectificación a los afectados se garantizan a través de la incorporación de capacidades tecnológicas que garantizan que los mismos puedan ser accesibles, y ser

[70] Los principios se encuentran disponibles en: http://www.export.gov/safeharbor/eu/eg_main_018475.asp

rectificados o borrados por los propios usuarios y/o por el responsable del tratamiento a través del administrador de los servicios, sin que sea necesaria la intervención del proveedor de Cloud en la gran mayoría de los casos.

Este mecanismo de cumplimiento está disponible para los importadores de datos con sede en EE.UU. La lista de entidades adheridas a los principios de Puerto Seguro está disponible en http://www.export.gov/safeharbor. Las entidades participantes se someten a la jurisdicción de la FTC, quien aplica las normas que prohíben actos o prácticas desleales o fraudulentas en el comercio o en relación con él.

Esta Decisión representó la transición desde un modelo europeo de protección de datos basado únicamente en la protección territorial, hacia un modelo basado también en el cumplimiento de una serie de principios por parte de las entidades importadoras de datos de carácter personal. Las transferencias bajo el esquema de Safe Harbor no requieren autorización por parte de las autoridades nacionales, sin perjuicio de las obligaciones de notificación que puedan aplicar según el derecho interno.[71]

Resulta importante resaltar que Safe Harbor regula el intercambio de datos en el ámbito comercial entre entidades privadas, no regula, en modo alguno, el

[71] El texto de la Decisión se encuentra disponible en:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:ES:PDF

intercambio de información en el marco de la cooperación policial y judicial.[72] Tampoco regula lo relativo al tratamiento de datos con fines de seguridad nacional e inteligencia por parte de las autoridades.[73] De hecho, la UE como tal carece de competencias en este ámbito, siendo las mismas atendidas en exclusiva por los Estados Miembros a nivel nacional.[74] No obstante, a raíz de las revelaciones de Edward Snowden sobre las actividades de vigilancia masiva desplegadas por la NSA dentro y fuera del territorio de los EE.UU.[75], distintos actores a nivel europeo, incluido el Parlamento Europeo llamó a la suspensión de Safe Harbor.[76] Por su parte, la Comisión Europea, quién tendría poderes ejecutivos para derogar la Decisión de adecuación sobre Safe Harbor, se ha manifestado a favor no de la suspensión del programa, sino de la restauración de la confianza en el mismo[77] a través de la implementación de una serie de recomendaciones[78] que incluyen una supervisión más estricta de las compañías participantes por parte la FTC, y la lucha las auto-certificaciones certificaciones de auto falsas. Actualmente se está negociando

[72] Esta se regula a través de otros instrumentos como el Acuerdo de Asistencia Judicial entre la UE y EE.UU, que se estudiará en la Sección 8.4.

[73] Sobre el acceso gubernamental a datos con fines de seguridad e inteligencia, véase la Sección 4.2.

[74] Títulos V y VI del Tratado Único Europeo.

[75] Vid Capítulo IV.

[76] http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-526.085&format=PDF&language=EN&secondRef=02

[77] http://ec.europa.eu/justice/newsroom/data-protection/news/131127_en.htm

[78] http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

este nuevo esquema de Safe Harbor entre la Comisión y la International Trade Administration (ITA).[79]

b) Las Cláusulas Contractuales Tipo

En febrero de 2010, la Comisión Europea adoptó la Decisión 2010/87/UE, y con ella, un conjunto de cláusulas contractuales tipo para transferencias entre responsables y encargados del tratamiento, respectivamente, con el objeto de responder a la

[79] El 07 de octubre de 2015, el Tribunal de Justicia de las Comunidades Europeas anuló la Decisión de adecuación Safe Harbor en el marco del caso *Schrems vs Facebook*. Tras la Decisión, la herramienta utilizada más de 4.000 compañías para importar datos desde la Unión Europea, queda invalidada, sobre la base de que no ofrece *per se* garantías suficientes frente a actividades de vigilancia gubernamentales por parte de la NSA, ni posibilidad de obtener tutela para lo ciudadanos europeos. *A priori*, llaman la atención tres cuestiones:

1) Safe Harbor regulaba exclusivamente el intercambio de datos en el ámbito comercial entre entidades privadas, no tocando lo relativo al tratamiento de datos con fines de aplicación forzosa de la ley en el ámbito criminal seguridad nacional por parte de las autoridades.

2) No se entra a valorar las políticas, los contratos, o las acciones de Facebook, sino que se rompe la presunción prácticamente *iure et de iure* que establece la Decisión, y abre la posibilidad de que las autoridades de protección de datos de los Estados Miembros investiguen.

3) Las intrusiones por parte de la NSA fueron ilegales (al menos en su mayoría) tal y como se ha declarado por parte de la justicia federal y por parte del propio Gobierno de los EE.UU. y Gran parte de estas actividades se produjeron de hecho fuera del territorio de los EE.UU. Asimismo, las intrusiones reveladas por Snowden parecía tener como principal aliado un Estado Miembro de la Unión Europea como el Reino Unido. Por lo anterior, la solución al problema parece ser política más que jurídica.

Desde el punto de vista político, la Decisión del Tribunal constituye un elemento de presión para las negociaciones de un posible nuevo Safe Harbor, y para el gobierno de los EE.UU. sobre el control que debe ejercer sobre sus agencias de seguridad e inteligencia de cara al restablecimiento de la confianza por parte de las autoridades europeas en el intercambio de datos trasatlánticos y de seguir gozando de una posición privilegiada en la economía digital europea a través de sus compañías.

expansión de actividades de tratamiento y en particular, la aparición de nuevos modelos de negocio para el tratamiento internacional de datos personales.[80]

A la luz de esta Decisión, cuando las transferencias de datos se realicen entre un responsable y un encargado del tratamiento, se considera que reúnen las garantías adecuadas los contratos que incluyan las cláusulas contractuales tipo aprobadas. Del conjunto de cláusulas, resultan especialmente relevantes en el ámbito del Cloud Computing las siguientes:

- Ley aplicable: En lo relativo a la protección de datos, aplicará la legislación del Estado Miembro en el que está establecido el exportador de datos (Cláusulas 1 y 9).

- Responsabilidad: El importador (proveedor de Cloud) será responsable subsidiario de los daños y perjuicios a los titulares de los datos como resultado del incumplimiento de las obligaciones contenidas en las cláusulas (Cláusula 6).

- Seguridad: El importador de datos (proveedor de Cloud) ofrecerá garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas específicas detalladas y especificadas en un anexo al contrato. (Cláusula 4 c, d, e).

[80] Decisión 2010/87/UE. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32010D0087

- Auditoría: el importador de datos (proveedor de Cloud) ofrecerá a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las cláusulas. Esta será realizada por el exportador de datos o por un organismo de inspección, compuesto por miembros independientes con las cualificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos y, cuando corresponda, de conformidad con la autoridad de control (Cláusula 5.f).

  En el ámbito del Cloud Computing esta cláusula resulta problemática en la práctica, permitir la auditoría por parte de múltiples (miles o millones de clientes) puede precisamente poner en riesgo la seguridad de los sistemas y de los datos en vez de fortalecerla. Sobre este particular, el Grupo Trabajo del Artículo 29 ha establecido que en el ámbito de la nube, la auditoría de una tercera parte independiente podrá considerarse adecuada, en lugar de la auditoría individual por parte de cada responsable del tratamiento.[81]

- Subcontrataciones: La subcontratación de las operaciones de procesamiento requerirán de dos requisitos: (i) previo consentimiento por escrito del

[81] Este criterio fue reflejado en su Opinión 05/2012 sobre Cloud Computing, p.22.

exportador de datos (ii) que el subencargado del tratamiento que se contrata garantice que proporcionará, al menos, el mismo nivel de protección de los datos personales y los derechos de los interesados que el importador de datos proporciona en virtud de las cláusulas (Cláusulas 4 y 11.i).

En el ámbito del Cloud Computing la aplicación de esta cláusula también resulta problemática: Recabar el consentimiento individual de múltiples (miles o millones de clientes) ante todas y cada una de las subcontrataciones (ya que no se distinguen las subcontrataciones sustanciales de las no sustanciales) que puedan producirse a lo largo de la vida de un contrato puede ser difícil de materializar en la práctica. Sobre este particular, el Grupo Trabajo del Artículo 29 ha establecido que, en estos casos, un consentimiento general por escrito al inicio de la relación es suficiente, siempre y cuando el exportador sea notificado de eventuales nuevos subcontratistas, caso en el cual dicho exportador tendrá derecho o bien a objetar la nueva subcontratación, o a terminar el contrato.[82]

- Jurisdicción competente: El importador se somete a la jurisdicción del exportador de datos (cliente de Cloud) a los efectos de cualquier reclamación

[82] Este criterio fue reflejado en su Opinión 05/2012 sobre Cloud Computing p.10.

por daños y perjuicios por parte de los titulares de los datos (Cláusulas 4 y 11.i).

- Deber de cooperación: Las partes acuerdan que la autoridad de control está facultada para auditar al importador (proveedor de Cloud), o a cualquier subencargado, en la misma medida y condiciones en que lo haría respecto del exportador de datos conforme a la legislación de protección de datos aplicable (Cláusula 8).

A diferencia de Safe Harbor, las cláusulas están disponibles para importadores ubicados en todo el mundo. De este modo continúa la transición europea desde un modelo basado a únicamente en protección territorial, hacia un modelo basado en compromisos contractuales. A diferencia de Safe Harbor, las cláusulas no tienen una aplicación uniforme en los Estados Miembros. Si bien en la mayoría de los Estados Miembros las cláusulas tienen un reconocimiento directo y no necesitan de la autorización de las autoridades de protección de datos locales para su utilización, algunos países han optado por requerir el trámite de autorización. España se encuentra en este grupo de países junto a Austria, Alemania, Eslovenia Francia, Italia, Lituania, Luxemburgo, Malta, Portugal y Rumanía.[83] Polonia reformó recientemente

[83] Para consultar un resumen de estos regímenes de TID, véase DLA Piper: "Data Protection Laws of the World". Marzo 2013. Disponible en: http://dlapiperdataprotection.com/

su ley de protección de datos para eliminar el requerimiento de autorización previa.[84]

c) Normas Corporativas Vinculantes para Encargados del Tratamiento o PBCRs[85]

En 2012, el Grupo de Trabajo del Artículo 29 publicó un esquema para facilitar el uso de normas corporativas vinculantes o *binding corporate rules* por parte de encargados del tratamiento, un instrumento que desde 2008 se venía utilizando para transferencias entre responsables del tratamiento.[86]

Las PBCRs se proponen por el Grupo de Trabajo como una herramienta que ayudaría a enmarcar las transferencias internacionales de datos personales que se procesan inicialmente por un importador de datos en nombre del exportador, y cuyo tratamiento está subcontratado dentro de la organización del encargado del

[84] Entró en vigor el 25 de diciembre de 2014. Según el instrumento, no se requiere el consentimiento del regulador para la transferencia que un responsable del tratamiento y un encargado del tratamiento basado en un tercer país, cuando se suscriben entre las partes las la cláusulas contractuales tipo aprobado por la Comisión Europea.
Véase más en:
https://www.huntonprivacyblog.com/2014/12/02/poland-amends-personal-data-protection-act/

[85] Processor Binding Corporate Rules.

[86] ARTICLE 29 DATA PROTECTION WORKING PARTY: "Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules". Bruselas, Junio 2012. Disponible en:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

tratamiento.[87] Bajo las PBCRs, las entidades del grupo del encargado del tratamiento se comprometen a respetar los principios contenidos en dichas PBCRs, y se hacen responsables vis- à-vis frente al responsable del tratamiento en caso de incumplimiento.

Para el Grupo de Trabajo, mientras que las cláusulas contractuales tipo parecen ser eficaces para enmarcar transferencias no masivas realizadas por un exportador de datos situado en la UE a un importador de datos que se encuentra fuera de la UE, la industria ha solicitado un nuevo instrumento jurídico que permita una enfoque global de la protección de datos en el negocio de la externalización, así como el reconocimiento oficial de las reglas internas que las organizaciones pueden haber implementado. Este nuevo instrumento jurídico sería eficiente para enmarcar transferencias masivas hechas por un encargado del tratamiento a sub-encargados del tratamiento de su misma organización, que actúa en nombre y bajo las instrucciones de un responsable del tratamiento. Por tanto, las PBCRs deberían entenderse como garantías adecuadas previstas por el encargado del tratamiento al responsable (Art. 26.2 de la Directiva de la UE 95/46) que permiten al exportador cumplir con la ley de protección de datos de la UE.

[87] ARTICLE 29 DATA PROTECTION WORKING PARTY: "Explanatory Document on the Processor Binding Corporate Rules". Bruselas, Abril 2013 (rev. May 2015). Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf

Se suma de esta forma un mecanismo adicional de cumplimiento a las opciones existentes (Safe Harbor y Cláusulas Contractuales Tipo). A diferencia de las cláusulas contractuales tipo, BCRs y PBCRs son esencialmente adaptables a la operativa empresarial de una compañía multinacional. Esta flexibilidad puede resultar positiva desde el punto de vista práctica, no obstante, añade incertidumbre sobre los criterios tener en cuenta por las autoridades competentes para su aprobación. Asimismo, a diferencia de las cláusulas tipo, el procedimiento tiene una complejidad considerable.

En la actualidad, ni BCRs y PBCRs cuentan con un alto nivel de adopción, quizás esto se deba a que las mismas tienen poco reconocimiento en las normativas nacionales de protección de datos, las cuales se aprobaron antes de que el concepto se empezará a desarrollar en el seno del Grupo de Trabajo del Artículo 29. El nuevo Reglamento Europeo de Protección de Datos pretende corregir esta situación, haciendo un reconocimiento expreso de las normas corporativas vinculantes.[88]

d) Otras Garantías

[88] Vid. Art. 42 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

Los Estados miembros, a través de sus autoridades nacionales de protección de datos, conservan la potestad de autorizar transferencias a terceros países que no está incluidos en la lista blanca de la Comisión Europea cuando el responsable del tratamiento ofrezca, a su juicio, garantías suficientes para cumplir con la ley de protección de datos del Estado Miembro en cuestión.

3.4.5. Regulación en España

Las transferencias internacionales de datos se regulan en los artículos 33 y 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y en el Título VI del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD).

Como regla general, para la realización de transferencias internacionales de datos se requiere previa Autorización por parte Director de la Agencia Española de Protección de Datos (AEPD) salvo cuando el Estado en el que se encuentre el importador ofrezca un nivel adecuado de protección a la luz del esquema de Safe Harbor, que el mismo se encuentre en uno de los países aprobados por la Comisión Europea, o que la

misma se haga con arreglo a las excepciones establecidas en los apartados 34 de la LOPD.[89]

Con respecto a las transferencias apoyadas en Cláusulas Contractuales Tipo, se establece que su utilización deberá ser aprobada por el Director de la AEPD. La autorización también podrá ser otorgada bajo Otras Garantías, es decir, fórmulas contractuales alternativas en las que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales, y se garantice el ejercicio de sus respectivos derechos.[90] En cualquier caso, se deberán notificar las transferencias internacionales de datos al Registro General de Protección de Datos. Con independencia de la legitimidad de las transferencias internacionales de datos, de conformidad con la LOPD, toda prestación de servicios que implique el tratamiento[91] datos de carácter personal, constituye un acceso a datos por cuenta de terceros o encargo del tratamiento, y deberá estar regulada en un contrato por escrito, de conformidad con el art. 12 de la LOPD. Este contrato debe recoger los siguientes aspectos:

---

[89] Tras la anulación de la Decisión sobre Safe Harbor, este supuesto desaparece, tal y como indica la AEPD en su página web:
https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

[90] Art. 70.2 RLOPD.

[91] El Art. 5.1.t del RLOPD define el tratamiento de datos de carácter personal como: "cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de **datos** que resulten de comunicaciones, consultas, interconexiones y transferencias".

1. Objeto de la prestación del servicio.

2. Prohibición de ceder los datos a terceros, ni siquiera para su conservación, salvo para el cumplimiento de obligaciones legales.

3. Obligación del prestador de tratar los datos de acuerdo con las instrucciones dadas por el Responsable del Tratamiento.[92]

4. Medidas de seguridad que el prestador de servicios deberá aplicar al tratamiento de los datos realizados.

5. Obligación de devolver o destruir los datos, soportes generados, documentación, etc., cuando haya concluido la prestación de servicios., sin perjuicio de que pueda conservar debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con el Responsable del Fichero.

El responsable del tratamiento deberá, establecer estas estipulaciones o bien dentro del contrato principal de Cloud Computing, o bien en un anexo del mismo, además de suscribir estas estipulaciones, el responsable deberá velar por que el encargado del tratamiento reúna las garantías necesarias para el cumplimiento de las mismas (Art. 20.2 del RLOPD).

[92] El Art. 5.1(q) del RLOPD define el Responsable del fichero o del tratamiento como: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

El incumplimiento de las obligaciones establecidas en el contrato por parte del proveedor de servicios, le convertirán responsable del tratamiento a efectos de asumir las infracciones derivadas de su comportamiento (Art. 12.4 de la LOPD). Por su parte, el prestatario del servicio será responsable de las infracciones cometidas por el proveedor en materia de comunicaciones de datos, cuando éste actúe de acuerdo con sus instrucciones (Art. 20.3 del RLOPD).

De conformidad con el art. 21 del RLOPD, el proveedor no podrá llevar a cabo la subcontrataciones totales o parciales del servicio, a menos que el responsable del tratamiento hubiera otorgado su autorización para ello en el propio contrato, o en un instrumento posterior. Conviene mencionar esta circunstancia expresamente, ya que en la industria de servicios TIC, la subcontratación de servicios es muy habitual, por lo que la AEPD ha tomado el mismo enfoque que el Grupo Trabajo del Artículo 29 sobre este particular, estableciendo que el consentimiento general por escrito al inicio de la relación es suficiente, siempre y cuando el exportador sea notificado de eventuales nuevos subcontratistas, caso en el cual dicho exportador deberá tener derecho a objetar la subcontratación en cuestión, o a terminar el contrato.[93]

[93] AEPD. Resolución Nº Expediente: TI/00032/2014 de declaración de adecuación de garantías para las transferencias internacionales de datos a los Estados Unidos con motivo de la prestación de servicios de computación en nube. Disponible en: https://on.uclm.es/pdf/TI-00032-2014_Resolucion-de-fecha-09-05-2014_de-MICROSOFT-CORPORATION_a-Estados-Unidos.pdf

3.4.6. Proyecto de Reglamento Europeo de Protección de Datos

El proyecto de Reglamento Europeo de Protección de Datos propuesto por la Comisión[94] regula las Transferencias Internacionales de Datos en su Capítulo V. Como principio general, se establece que podrá realizarse una transferencia cuando la Comisión haya decidido que un tercer **país**, un **territorio**, **sector** de tratamiento de datos en ese tercer país o territorio, una **organización** internacional, garanticen un nivel de protección adecuado. Dichas transferencias no requerirán autorización (Art. 40). El principal cambio con relación a la Directiva es que no se parte de una prohibición, sino más bien de una autorización siempre que se cumpla con los criterios de adecuación de la Comisión. Se mantiene el concepto de "nivel adecuado de protección", no obstante, como principal novedad se recoge expresamente que la adecuación podrá recaer no sólo sobre un tercer país, o territorio, sino también sobre sectores u organizaciones. Si bien en la práctica la Comisión ha venido adoptando este enfoque con decisiones como Safe Harbor y las Cláusulas Contractuales tipo, el borrador de Reglamento da mayor uniformidad y seguridad jurídica al recoger estos extremos expresamente.

[94] Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012PC0011&from=ES

3.5. Marco de Privacidad APEC[95]

El Marco de Privacidad APEC, aprobado en el año 2005, tiene como objetivo proporcionar orientación y dirección a empresas dentro de las Economías de APEC, sobre asuntos comunes de privacidad, teniendo en cuenta las expectativas razonables del consumidor moderno de que las empresas reconocerán sus intereses de privacidad de forma consistente con los principios establecidos en el Marco, [96] a saber: prevención del daño, aviso, limitaciones a la recolección, usos de la información personal, elección, integridad de la Información personal, medidas de seguridad, acceso y rectificación, y responsabilidad.

Existe una simetría importante con la sustancia de los principios de protección de datos personales consagrados en la Directiva Europea, no obstante, existen grandes diferencias en los relativo a las transferencias internacionales de datos, que en el modelo APEC no se ven restringidas. Asimismo, en el modelo europeo, las autoridades de protección de datos tienen la potestad de verificar regulan y verificar el cumplimiento *ex ante* de dichos principios por parte de las organizaciones,

[95] De las siglas en inglés de Asia-Pacific Economic Cooperation. Foro de Cooperación Económica Asia-Pacífico. Forman parte de ella Australia (1989) Brunei (1989) Canadá (1989) Chile (1994) China (1991) Hong Kong (1991) Indonesia (1988) Japón (1989) Malasia (1989) México (1993) New Zealand (1989) Papúa New Guinea (1993) Perú (1998) Filipinas (1989) Russia (1998) Singapur (1989) Corea del Sur (1989 Tailandia (1989) Estados Unidos (1989) y Vietnam (1998).

[96] Una traducción al español del Marco se encuentra disponible en: https://www.sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf

mientras que en el modelo APEC se establece un mecanismos de autorregulación, bajo el que estas tareas corresponden a la propia organización.

3.6. Directrices de las Naciones Unidas

Las Directrices de las Naciones Unidas para la Regulación de Tratamientos de Datos Automatizados fueron emitidas en el año 1990 por la Asamblea General de las Naciones Unidas. En materia de movimientos internacionales de datos, se establece que, cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca garantías comparables para la protección de la privacidad, la información debe ser capaz de circular tan libremente como en el interior de cada uno de los territorios de los Estados en cuestión. De no haber garantías recíprocas, las limitaciones a la circulación no se pueden imponer indebidamente sino sólo en la medida en que protección de la privacidad lo demande.[97]

3.7. Directrices de la OCDE

Las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE fueron adoptadas en 1980 como una recomendación del

[97] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 1990. Principio 9. Disponible en: http://www.refworld.org/docid/3ddcafaac.html

Consejo de la OCDE, apoyado en los tres principios que aglutinan a los países de la OCDE, a saber: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas. Las directrices fueron revisadas en 2013.

Se consagran una serie de principios básicos, a saber: principio de limitación de recogida, principio de calidad de los datos, principio de especificación del propósito, principio de limitación de uso, principio de salvaguardia de la seguridad, principio de transparencia y principio de participación individual y principio de responsabilidad. En relación con las transferencias internacionales de datos, las directrices establecen en su Parte Cuarta[98] que:

- El responsable del tratamiento sigue siendo responsable de los datos personales bajo su control con independencia de la ubicación de los datos.

- Los países miembros deben abstenerse de restringir los flujos transfronterizos de datos personales cuando (i) el otro país observa sustancialmente las directrices OECD (ii) existen suficientes garantías, incluyendo mecanismos de aplicación eficaces y medidas apropiadas puestas en marcha por el responsable del tratamiento, para garantizar un nivel de protección continuo y consistente con las directrices establecidas.

[98]The OECD Privacy Framework, 2013
http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

- Todas las restricciones a los flujos transfronterizos de datos personales deben ser

  proporcionales a los riesgos presentados, teniendo en cuenta la sensibilidad de los datos, el propósito y el contexto del procesamiento.

3.8. Resolución de Madrid

La Resolución de Madrid[99] sobre Estándares Internacionales sobre Protección de Datos Personales y Privacidad fue el producto de la labor conjunta de los garantes de la privacidad de casi cincuenta países coordinado por la AEPD. Su texto intenta plasmar los múltiples enfoques que admite la privacidad a nivel global, integrando legislaciones de los cinco continentes.

En particular por objeto "*Definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación*

[99] Estándares Internacionales sobre Protección de Datos Personales y Privacidad, Resolución de Madrid. Madrid, 2009: https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

con el tratamiento de datos de carácter personal; y Facilitar los flujos internacionales de datos de carácter personal, necesarios en un mundo globalizado".[100]

El relación con las transferencias internacionales de datos se establece los siguiente: "Como regla general, podrán realizarse transferencias internacionales de datos de carácter personal cuando el Estado al que se transfieran dichos datos ofrezca, cuando menos, el nivel de protección previsto en el presente Documento (...) Será posible realizar transferencias internacionales de datos de carácter personal a Estados que no ofrezcan el nivel de protección previsto en el presente Documento, cuando quien pretenda transferir dichos datos garantice que el destinatario ofrecerá dicho nivel de protección; dicha garantía podrá derivarse, por ejemplo, de cláusulas contractuales apropiadas. En particular, cuando la transferencia se lleve a cabo en el seno de organizaciones o de grupos multinacionales, dicha garantía podrán consistir en la existencia de normas internas de privacidad cuya observancia resulte vinculante (...).[101]

Aunque no tiene un carácter vinculante, estos Estándares establecen un compromiso político de quienes lo han suscrito, en el sentido de servir como referencia a los Estados que en la actualidad no hayan legislado sobre la materia, y de facilitar la armonización de la normativa existente, en aras de que la normativa sobre

[100] Principio 1.

[101] Principio 15.

protección de datos y la privacidad no se constituya un obstáculo al comercio internacional, facilitando el flujo de los datos de carácter personal.

4. CAPÍTULO III. LEY APLICABLE Y JURISDICCIÓN COMPETENTE

4.1. Ley aplicable al contrato de Cloud Computing

En principio, la ley aplicable a la prestación de servicios de Cloud Computing es de libre elección por las partes contratantes, no obstante, cuando los elementos relevantes a la relación jurídica estén conectados con sólo un país, la elección de las partes no puede perjudicar la aplicación de las leyes que según el ordenamiento de ese país no puedan ser derogadas por contrato.[102]

En este sentido, el Artículo 10.5 del Código Civil español establece que se aplicará a las obligaciones contractuales la Ley a que las partes se hayan sometido expresamente, siempre que tenga alguna conexión con el negocio de que se trate; en su defecto, se aplicará la Ley nacional común a las partes; a falta de ella, la de la residencia habitual común, y, en último término, la Ley del lugar de celebración del contrato.

Las partes serán libres de elegir la legislación aplicable a la prestación de servicios de Cloud Computing, siempre que se respete el cumplimiento de las normas que no pueden derogarse por contrato, es decir, las normas de orden público, y que la

[102] VAN OUDENHOVE, Bart: "The formation of Contracts through the Internet, A decade of Research @ the Crossroads of Law and ICT". Bruselas, 2001, p. 398.

legislación escogida tenga alguna conexión con la relación jurídica en el momento de dicha elección, por ejemplo, el domicilio del prestatario, el domicilio del prestador, el lugar de ubicación geográfica de la infraestructura TIC desde donde se prestarán los servicios de computación en la nube, etc.

La elección de la ley aplicable afecta a la relación entre las partes, esto es, al cumplimiento de las obligaciones, la interpretación del contrato, la responsabilidad contractual, entre otras. No obstante, las partes contratantes seguirán obligadas por las normas que les apliquen sus los activos de información en virtud de su ubicación geográfica, actividad de negocio, o participación en un mercado concreto. Asimismo se verán afectadas por las reglas aplicables en materia de responsabilidad extracontractual. La ley aplicable será determinante, entre otras cosas, a la hora de establecer responsabilidades entre las partes, ante incidentes relacionados con la seguridad de la información tratada por el proveedor.

4.2. Ley aplicable a la información en la Nube

En una relación *Business to Business* (B2B), la articulación jurídica de la prestación de servicios de Cloud Computing es en principio libre, en virtud de la autonomía de la voluntad que rige la contratación, no conociendo al menos en el ordenamiento jurídico español, otras limitaciones que las señaladas en el capítulo anterior. No

obstante, dependiendo del tipo de organización contratante y de la información que se vea involucrada en el ámbito de los servicios, es muy probable que existan requerimientos legales y regulatorios específicos, que deben ser tenidos en cuenta en el diseño del marco contractual que rige la relación de prestación de servicios.

Estos requerimientos legales y regulatorios, lógicamente variarán dependiendo de factores como la ubicación geográfica y el sector de actividad del prestatario, entre otros, o simplemente dependerán de su participación en un mercado concreto. Algunos ejemplos los encontramos en normas como el Esquema Nacional de Seguridad[103], Sarbanes Oxley[104], HIPAA[105] o GLBA.[106] Asimismo, en caso de que los servicios de Cloud impliquen el tratamiento de datos de carácter personal (lo cual sucede en la mayoría de los casos) entran en juego las normas que regulan la

[103]El Esquema Nacional de Seguridad español que tiene por objeto establecer la política de seguridad para la Administración en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

[104] La Ley Sarbanes Oxley (Sarbanes-Oxley Act, Pub. L. 107-204, 116) de 2002, también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista, es una ley Estadounidense que más allá del ámbito nacional, involucra a todas las empresas que cotizan en NYSE (Bolsa de Valores de Nueva York), así como a sus filiales. Esta norma impone requisitos que afectan directamente a la seguridad de la información, en particular, a la integridad de la misma.

[105] La Ley HIPAA (Health Insurance Portability and Accountability Act, Pub.L.104-191) de 1996, es también una es una ley que se aplica a todos los actores vinculados al sistema sanitario estadounidense, y que establece requisitos específicos de privacidad y seguridad para los datos de salud.

[106] GLB (Gramm–Leach–Bliley Act, Pub. L. 106-102, 113) de 1999 obliga a todas las instituciones financieras a aplicar unos estándares apropiados de seguridad, para proteger los datos de los clientes contra amenazas y accesos no autorizados internos y externos que se producen a través de redes y sistemas en línea.

privacidad y la protección de datos de carácter personal aplicables al prestatario del servicio de Cloud y/o al prestador, y que varían en función de la jurisdicción en la que se encuentren, respectivamente.

En materia de protección de datos personales, en España resultan de aplicación la LOPD y el RLOPD[107] instrumentos que restringen los movimientos internacionales de datos personales, salvo que se las mismas se amparen en alguna de las excepciones contempladas, o se acredite que se reúnen las garantías adecuadas.

Como punto de partida para la contratación, la organización contratante deberá conocer muy bien sus obligaciones. Sin ello no será posible cumplirlas y menos aún, verificar si los compromisos contractuales y la tecnología del proveedor se ajustan a estos requisitos.

Estas obligaciones pueden provenir de fuentes internas y externas.

Las fuentes externas se refieren al derecho positivo y/o al conjunto de normas jurídicas que aplican a la entidad contratante y que afectan a sus activos de información, fundamentalmente en virtud de su localización geográfica o jurisdicción

[107] Instrumentos de transposición de la Directiva 95/46/CE en del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

a la que está sometida y de su sector de actividad. Por su parte, las fuentes internas se refieren a las normas internas, políticas corporativas y obligaciones contractuales que debe cumplir la organización por haberse obligado a ello de forma voluntaria. En muchos casos, estas normas y políticas ordenan la adopción de estándares existentes, como la norma ISO/IEC: 27001, o el estándar PCI-DSS.[108]

4.3. Jurisdicción competente

El término jurisdicción tiene en la actualidad tres acepciones genéricas: a) como poder del Estado; b) como complejo orgánico (órganos públicos a los que se les encomienda la función jurisdiccional; c) como uno de los presupuestos del proceso judicial.[109] En este apartado nos referiremos a la jurisdicción como poder del Estado. En el ámbito del derecho internacional público,[110] dicha jurisdicción puede tener tres manifestaciones, a saber:

a) Jurisdicción Prescriptiva

[108] PCI DSS (Payment Card Industry Data Security Standard) es el estándar de seguridad de datos para la industria de tarjeta de pago. Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más relevantes a nivel global como una guía de seguridad para las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes, con el fin de prevenir los fraudes en materia de tarjetas bancarias débito y crédito.

[109] TAPIA F, Isabel: "Lecciones de Derecho Procesal". Volumen 1. Universitat Illes Balears, 2010, p.27.

[110] En contraposición al ámbito del derecho internacional privado, cuando se trata de conocer cuestiones civiles por parte de un tribunal.

En su sentido más amplio, la jurisdicción prescriptiva se refiere a la competencia de un Estado para legislar *vis a vis* frente a otros Estados.[111] Se refiere a la compartición del espacio legislativo entre los Estados con arreglo al principio de *juste partage de souveraineté* o distribución justa de la soberanía. Concretamente, el concepto de jurisdicción prescriptiva atañe a la autoridad soberana que tiene un Estado para extender la aplicación de su legislación a las actividades, relaciones, el estatus de las personas o los intereses estas sobre determinadas cuestiones; ya sea por disposición legal, por un acto ejecutivo, por disposición de una regla administrativa, o por determinación de un tribunal.[112]

b) Jurisdicción Adjudicativa

La jurisdicción adjudicativa se refiere a la autoridad soberana de un Estado para someter a personas o entidades a los procedimientos de sus tribunales con el propósito de determinar si el derecho de prescripción ha sido contravenido o incumplido.[113]

[111] KOHL, Uta: "Jurisdiction and the Internet: Regulatory Competence over Online Activity". Cambridge Univ. Press, 2007, p.14.

[112] Restatement (Third) of Foreign Relations Law of the United States, S 401 (1987).

[113] JENNINGS, Robert. WATTS, Arthur, OPPENHEIM Lawrence: "Oppenheim's international law". Essex, 1992, p. 456.

c) Jurisdicción Ejecutiva

Por su parte, la jurisdicción ejecutiva o por imposición se refiere a la autoridad soberana que tiene un Estado para inducir u obligar al cumplimiento, o para castigar y sancionar el incumplimiento de sus leyes o reglamentos, ya sea a través de los tribunales o del uso ejecutivo, administrativo o policial y otras acciones no judiciales. [114] En general, se supone que un Estado no puede hacer cumplir sus reglas a menos que tenga jurisdicción para prescribir dichas reglas.[115] En consecuencia, un Estado podrá emplear medidas judiciales o extrajudiciales para obligar al cumplimiento o castigar el incumplimiento de sus leyes o reglamentos, siempre que tenga jurisdicción para prescribir.[116]

La consideración de los diversos tipos de jurisdicción tiene especial relevancia en el ámbito penal por dos razones. En primer lugar, el ejercicio válido internacionalmente de la jurisdicción prescriptiva en la adopción de una ley es un requisito previo para el ejercicio válido de la jurisdicción adjudicativa o ejecutiva con respecto a esa ley.[117] Si

[114] American Law Institute: "Restatement (Third) of the Foreign Relations Law of the United States". Nota introductoria Parte IV.

[115] En éste sentido véase United Nations: "Report of the International Law Commission", 2006, p.518 citando a OXMAN Bernard H.

[116] American Law Institute: "Restatement (Third) of the Foreign Relations Law of the United States" 1987. Nota introductoria Parte IV.

[117] United Nations: "Report of the International Law Commission", United Nations Publications, 2006, p.518 pp.

la competencia sobre el fondo va más allá de los límites legales, cualquier ejercicio de jurisdicción ejecutiva sería ilegal.[118] En segundo lugar, la posible injerencia resultante del ejercicio extraterritorial de la jurisdicción en materia legislativa es menor que la resultante del ejercicio extraterritorial de la jurisdicción en materia adjudicativa o ejecutiva.[119]

4.4. Jurisdicción civil vs jurisdicción penal en el Cloud Computing

Dado el carácter eminentemente transnacional de los servicios de Cloud Computing, no sorprende que tengamos que acudir a las reglas de derecho internacional para analizar los distintos escenarios jurisdiccionales en la nube.

El Derecho Internacional privado será relevante en materia civil, en relación con los eventuales conflictos entre partes contratantes ubicadas en distintas jurisdicciones (proveedor, cliente y usuario del servicio de Cloud, respectivamente), mientras que el Derecho Internacional Público determinará la jurisdicción penal (p.ej. Qué autoridades judiciales o administrativas pueden investigar y perseguir un delito, y por tanto obligar a un proveedor de Cloud Computing a revelar datos).

[118] United Nations: "Report of the International Law Commission", United Nations Publications, 2006, P.518, citando a Brownlie.

[119] United Nations: "Report of the International Law Commission", United Nations Publications, 2006, p. 534.

La determinación de la jurisdicción civil internacional se apoya principalmente en dos instrumentos supranacionales, a saber, el Convenio de Lugano y el Reglamento de Bruselas. En el ámbito civil, la determinación de la jurisdicción competente no conlleva de modo automático la aplicación del derecho sustantivo del foro, debido a la normativa especial en materia de conflicto de leyes y las técnicas de reenvío. Asimismo, la inicial determinación de la jurisdicción civil en atención a criterios territoriales (el lugar de celebración del contrato, el lugar donde la obligación debe llevarse a cabo, el lugar donde se produce el hecho dañoso) y personales (el domicilio del demandado, o su lugar de su establecimiento o centro de operaciones) pueden ser objeto de modificación, por ejemplo, en virtud del as reglas de sumisión expresa y tácita o a través de la *derogatio fori*, conforme a las cuales las partes pueden excluir mediante acuerdos o mediante determinados actos, la competencia de los tribunales de un determinado Estado.[120]

[120] En este sentido, véase ORTIZ PRADILLO, J.: "Problemas Procesales de la Ciberdelincuencia", Colex. Madrid, 2013 p.38.

En contraste, en el ámbito de la jurisdicción penal[121] no existen instrumentos supranacionales de referencia que sirvan para determinar la jurisdicción. La ausencia de unas reglas claras de distribución de la competencia judicial en materia penal, a nivel internacional, ni en el marco del espacio Judicial Europeo dificultan la tarea de conocer *a priori* en qué jurisdicción se enjuiciarán determinados delitos que intersectan con el Cloud Computing. Ello tiene importantes repercusiones en razón de que la determinación de la jurisdicción competente para el enjuiciamiento del delito es condición *sine qua non* para la determinación del Derecho Penal aplicable, tanto en el plano sustantivo como en el plano procesal. A diferencia de la jurisdicción civil, la jurisdicción penal conlleva de modo automático la aplicación del derecho sustantivo del foro.[122] Dada la importancia y la complejidad del asunto, las siguientes páginas de este Capítulo se centrarán principalmente en la jurisdicción penal.

4.5. Retos de la jurisdicción penal ante el Cloud Computing

[121] En el ámbito penal, esta jurisdicción puede envolver, conjunta o separadamente, las siguientes facultades:

a) Investigación: Realizar investigaciones y obtener evidencias, incluyendo actividades de inteligencia, a través de sus fuerzas y cuerpos de seguridad.
b) Persecución: Perseguir un delito mediante el ejercicio de la acción penal pública dentro de un proceso a través sus órganos competentes (por ejemplo, el ministerio público) y presentar evidencias las pruebas ante el juez para que ese delito se castigue.
c) Juzgamiento: Juzgar un hecho delictivo, así como obtener datos, (que pueden encontrarse dentro o fuera del territorio nacional en el marco de un procedimiento judicial.

[122] En algunos casos, pueden existir restricciones a la aplicación íntegra del Derecho del foro, por ejemplo en materia de extradición de nacionales se puede imponer restricciones en cuanto a la cuantía de la pena.

En el ámbito del Cloud Computing, la propia naturaleza de las transacciones internacionales puede despertar el interés jurisdiccional de varios Estados surgen dos cuestiones fundamentales: En primer lugar, cuándo un Estado puede afirmar válidamente jurisdicción. En segundo lugar, qué reglas rigen el ejercicio de esa jurisdicción.

La importancia de estas cuestiones no es baladí, en razón de que, como se ha reiterado, a diferencia de lo que ocurre en con la jurisdicción civil, la jurisdicción penal escapa de la autonomía de la voluntad de las partes.

Los Principios de Harvard de 1935[123] sobre la competencia judicial con respecto a la delincuencia de 1935 sugieren, por primera vez, unas reglas internacionales de jurisdicción con respecto al crimen. Se trata de un Proyecto de Convención que resultó del análisis por un grupo de abogados internacionalistas de los distintos códigos de Derecho Penal modernos de aquél entonces, a la luz de la doctrina, de resoluciones de conferencias internacionales y la opinión de sociedades científicas, complementado por el examen de algunas decisiones de tribunales nacionales.

Aunque el Proyecto de Convención no fue adoptado formalmente por los Estados, dicho instrumento ha probado ser una guía influyente en el debate acerca de los

[123] Harvard Research Draft Convention on Jurisdiction with respect to Crime, 1935.

factores de conexión legítimos para afirmar la existencia de jurisdicción.[124] Dicho análisis reveló los cinco principios generales con arreglo a los cuales los Estados afirman una jurisdicción penal más, o menos extensa,[125] a saber:

1. **Principio territorial:** determina la jurisdicción por referencia al lugar donde el delito se ha cometido.

2. **Principio de la nacionalidad:** determina la jurisdicción por referencia al carácter nacional de la persona que ha delinquido.

3. **El principio de la personalidad pasiva:** determina la jurisdicción por referencia al carácter nacional de la persona que ha sido lesionada por el delito.

4. **El principio de protección:** determina la jurisdicción por referencia al interés nacional lesionado por el delito en cuestión.

5. **El principio de universalidad:** determina la jurisdicción por referencia al carácter de delito en cuestión, cuando la ofensa es contraria al interés de la comunidad internacional, todos los Estados tienen jurisdicción con

[124] GARDINER, Richard. K.:"International Law". Harlow Pearson, 2003, p.312.

[125] Véase comentario introductorio del Proyecto de Convención.

independencia del lugar de la comisión del delito, o de la nacionalidad de los sujetos del delito.

Los principios de Harvard han modelado la forma en la que pensamos sobre la jurisdicción en los últimos 80 años.[126] Tal y como se desprende de ellos, la territorialidad resulta insuficiente para regular la extensión de la jurisdicción penal de un Estado, por esta razón se han establecido elementos extraterritoriales de conexión que legitiman la jurisdicción teniendo en cuenta elementos distintos al territorio.[127]

Más recientemente, el Informe de la Comisión de Derecho Internacional de las Naciones Unidas sobre la jurisdicción extraterritorial reafirmó estos principios afirmando que: "Cualquier ejercicio de la jurisdicción extraterritorial debe basarse, indiscutiblemente, en al menos uno de los principios antes mencionados para ser válida en virtud del Derecho Internacional. Más de uno de los principios anteriores pueden ser relevantes en la determinación de la validez de la jurisdicción extraterritorial en un caso particular, dependiendo de las circunstancias"[128] y señaló

[126] SVANTESSON, Dan B: "Law enforcement internet jurisdiction". Intervención en CDPD 2015, min. 36. https://www.youtube.com/watch?v=NL4nNlzyqmQ

[127]SANZ H., Ágata: "Extraterritorialidad de la Ley Penal y Jurisdicción". Madrid 1999. Disponible en https://www.uclm.es/area/procesal/Extraterritorialidad.htm#_ftn36

[128] UNITED NATIONS: "Report of the International Law Commission". New York, 2006. Anexo E. p. 516 y ss http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf

que para que un Estado pueda afirmar válidamente su jurisdicción sobre una persona física o jurídica, propiedad situación, debe tener alguna conexión válida con esa persona, propiedad o situación.[129]

El ordenamiento jurídico español recoge expresamente cuatro de los cinco Principios de Harvard a través del artículo 23 de la Ley Orgánica del Poder Judicial (LOPJ) [130], a saber, el territorio (Art. 23.1), la nacionalidad del sujeto activo del delito[131] (Art. 23.2), la protección de los intereses nacionales (Art. 23.3) y la consecución de la justicia universal (Art. 23.4).

En relación con la protección de los intereses nacionales, tal y como señala FLORES, la legislación penal nacional puede extenderse sobre conductas realizadas fundamentalmente en otros estados, pero cuyas consecuencias se extienden hasta

[129] Cuando se habla de extraterritorialidad se hace referencia referencia a la zona más allá del territorio de un Estado, incluyendo su tierra, aguas interiores, mar territorial, así como el espacio aéreo adyacente. Dicha área podría entrar o bien dentro del territorio de otro Estado, o bien fuera de la jurisdicción territorial de algún Estado.

[130] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

[131] En el orden penal corresponderá a la jurisdicción española el conocimiento de los delitos que hayan sido cometidos fuera del territorio nacional, siempre que los criminalmente responsables fueren españoles (Siempre que el hecho sea punible en el lugar de ejecución, salvo que, en virtud de un Tratado internacional o de un acto normativo de una Organización internacional de la que España sea parte, no resulte necesario dicho requisito, cuando el agraviado o el Ministerio Fiscal interpongan querella ante los Tribunales españoles y el delincuente no haya sido absuelto, indultado o penado en el extranjero, o, en este último caso, no haya cumplido la condena. Si sólo la hubiere cumplido en parte, se le tendrá en cuenta para rebajarle proporcionalmente la que le corresponda.

nuestras fronteras.[132] Y es que de conformidad con el art. 24.3 LOPJ sólo podrán ser perseguidos por la jurisdicción española en virtud del principio de justicia universal los siguientes delitos:

a) Genocidio y lesa humanidad.

b) Terrorismo.

c) Piratería y apoderamiento ilícito de aeronaves.

d) Delitos relativos a la prostitución y corrupción de menores e incapaces.

e) Tráfico ilegal de drogas psicotrópicas, tóxicas y estupefacientes.

f) Tráfico ilegal o inmigración clandestina de personas, sean o no trabajadores.

g) Los relativos a la mutilación genital femenina, siempre que los responsables se encuentren en España.

h) Cualquier otro que, según los tratados y convenios internacionales, en particular los Convenios de derecho internacional humanitario y de protección de los derechos humanos, deba ser perseguido en España.

Sin perjuicio de lo que pudieran disponer los tratados y convenios internacionales suscritos por España como requisito adicional, la LOPJ establece que para que puedan conocer los Tribunales españoles de los anteriores delitos deberá quedar acreditado que sus presuntos responsables se encuentran en España o que existen víctimas de nacionalidad española, o constatarse algún vínculo de conexión relevante

[132] FLORES PRADA, Ignacio "Criminalidad Informática aspectos sustantivos y procesales". Tirant Monografías 818, Valencia 2012. p. 314.

con España y, en todo caso, que en otro país competente o en el seno de un Tribunal internacional no se ha iniciado procedimiento que suponga una investigación y una persecución efectiva, en su caso, de tales hechos punibles. De modo que, España puede requerir a los proveedores de Cloud Computing bajo su jurisdicción la cesión o revelación de información custodiada cuando ejerza dicha potestad con fundamento en alguno de los factores de conexión señalados.

El caso ***Estados Unidos vs Ivanov***[133] abordó el principio de personalidad pasiva o de protección de los intereses nacionales, en particular, la existencia o no jurisdicción sobre delitos informáticos cometidos fuera del territorio de los EE.UU, por parte ciudadanos extranjeros, en contra de empresas e infraestructuras estadounidenses ubicadas en los EE.UU. Ivanov, ciudadano de nacionalidad rusa fue acusado de los delitos de fraude informático y posesión de dispositivos ilegales de acceso, entre otros, en contra de la Oficina de Información en Línea (OIB) de los EE.UU. cuyo negocio e infraestructura están ubicados en el Estado de Connecticut. Ivanov, quien se trasladó a lo Estados Unidos para defenderse, alegó que el tribunal estadounidense carecía de jurisdicción en virtud de que éste se encontraba ubicado físicamente en Rusia cuando se cometieron los delitos, y por tanto, no podía ser acusado de violaciones de la ley de los EE.UU. El tribunal rechazó estos argumentos, en primer lugar, porque los efectos perjudiciales previstos y reales de las acciones de Ivanov en Rusia se produjeron dentro de los Estados Unidos, y en segundo lugar,

[133] *United States vs. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001)
http://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/

porque las leyes en virtud de las cuales Ivanov fue acusado de un delito de fondo, estaban destinadas por el Congreso de los EE.UU. a ser aplicadas extraterritorialmente.

4.6. Ubicación física, jurisdicción y extraterritorialidad

a) Ubicación física de equipos no equivale necesariamente a jurisdicción

El hecho de que los activos de información (o parte de ellos) residan en un centro de datos ubicado en determinado Estado no implica necesariamente que dicho Estado tenga un interés jurisdiccional legítimo en dichos datos en materia penal.[134] Existen un problema subyacente fundamental que es la fusión de la ubicación física de los datos con el acceso y/ o jurisdicción legal.[135]

Los datos se almacenan cada vez más en múltiples jurisdicciones, y se mueven rápidamente entre ellas. Parece arbitrario los usuarios estén sujetos a leyes

[134] SVANTESSON, Dan B: "Law enforcement internet jurisdiction". Intervención en CDPD 2015, min. 36. https://www.youtube.com/watch?v=NL4nNlzyqmQ

[135] HON, W. Kuan. MILLARD, Christopher. REED, Chris. SINGH, Jatinder. WALDEN, Ian. CROWCROFT, Jon: "Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Queen Mary School of Law Legal Studies Research Paper 191/2015. London, 2015 Disponible en SSRN: http://ssrn.com/abstract=2527951 p.8.

diferentes dependiendo de donde sus datos se encuentren en un momento determinado en el tiempo. Para algunas empresas, incluso puede ser difícil determinar dónde se encuentran los datos. Se ha argumentado que si las empresas tomaran decisiones sobre dónde almacenar los datos basadas puramente en consideraciones jurídicas en lugar de los requisitos técnicos, podría ponerse en peligro la capacidad de proporcionar e productos fiables y rápidos a los consumidores.[136]

Por otro lado, la ubicación física de los datos en un determinado territorio no implica necesariamente que desde ese territorio se tenga acceso lógico e inteligible a esos datos.[137] Por ejemplo, las personas a cargo de operar las instalaciones físicas de un centro de datos (electricidad, temperatura, cableado) pueden no tener acceso lógico alguno a los sistemas o datos en sí mismos, ya que la gestión y el mantenimiento de los sistemas se podría hacer en remoto desde otra jurisdicción. El enfoque en la ubicación física de los datos oscurece el problema de fondo, a saber, el acceso inteligible a datos, y la importancia de las medidas de seguridad que protegen los

[136] WESTMORELAND, Kate: "Jurisdiction over user data - what is the ideal solution to a very real world problem". Julio, 2014. The Center for Internet and Society at Stanford Law School. Disponible en: http://cyberlaw.stanford.edu/blog/2014/07/jurisdiction-over-user-data-what-ideal-solution-very-real-world-problem afirmando que Google subrayó esté argumento en sus objeciones a la propuesta establecer una ley de localización de datos en Brasil.

[137] HON, W. Kuan. MILLARD, Christopher. REED, Chris. SINGH, Jatinder. WALDEN, Ian. CROWCROFT, Jon: "Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Queen Mary School of Law Legal Studies Research Paper 191/2015. London, 2015 Disponible en SSRN: http://ssrn.com/abstract=2527951 p.10.

datos. Parece que hay una suposición implícita de que la ubicación física permitirá datos inteligibles para ser accedidos por cualquiera que tenga acceso a esa ubicación física, cuestión que no es correcta.[138]

b) La jurisdicción debe ejercerse dentro del territorio

Del mismo modo, un Estado puede tener interés jurisdiccional legítimo sobre datos que encuentran ubicados fuera de su territorio. No obstante, la primera y más importante restricción impuesta por el derecho internacional a un Estado es que, a falta de la existencia de una norma permisiva en contrario, no puede ejercer su poder en forma alguna en el territorio de otro Estado.[139] La utilización del criterio de la territorialidad tiene como base el principio de soberanía, la cual se ejerce dentro de unas fronteras determinadas.[140] En este escenario, el Estado en cuestión tendría que acudir a los mecanismos de cooperación internacional para el ejercicio de esta jurisdicción, salvo que una norma de Derecho Internacional autorice lo contrario.

[138] HON, W. Kuan. MILLARD, Christopher. REED, Chris. SINGH, Jatinder. WALDEN, Ian. CROWCROFT, Jon: "Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Queen Mary School of Law Legal Studies Research Paper 191/2015. London, 2015 Disponible en SSRN: http://ssrn.com/abstract=2527951 p.13.

[139] La Convención de Budapest es ciertamente la muestra más representativa de una convención no territorial.

[140] La noción jurídica de territorio comprende todos los lugares o espacios a los cuales se extiende la soberanía del Estado.

De conformidad con la Carta de las Naciones Unidas[141] el ejercicio de jurisdicción extraterritorial está sujeto a limitaciones basadas en ciertos principios fundamentales del Derecho Internacional, tales como la igualdad soberana de los Estados, el principio de la integridad territorial de un Estado y el principio de no intervención en los asuntos internos de otros Estados. Consideraciones de cortesía también se deben tener en cuenta en la aplicación de las afirmaciones de la jurisdicción extraterritorial.[142] Como principio general, un Estado no puede imponer su ley penal, es decir, investigar los delitos o detener a los sospechosos en el territorio de otro Estado sin el consentimiento de ese otro Estado.

En el caso de ejercicio de la jurisdicción extraterritorial por un Estado que otro Estado considere no válida en virtud del derecho internacional, los Estados tienen la obligación general de cooperar para resolver la disputa.[143] Un instrumento jurídico sobre este tema también debe prever un procedimiento para resolver tal controversia incluiría: dar aviso de que el ejercicio de la jurisdicción se considera no válida; la revisión de la validez del ejercicio de jurisdicción por parte del Estado actuante la luz de los principios fundamentales, y teniendo en cuenta las objeciones

[141] Carta de las Naciones Unidas http://www.un.org/es/documents/charter/index.shtml

[142] UNITED NATIONS: "Report of the International Law Commission". New York, 2006. Anexo E, p. 531.http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf

[143] UNITED NATIONS: "Report of the International Law Commission". New York, 2006. Anexo E, p. 536 .http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf

del Estado afectado.[144] Estos conceptos parecen estar vinculados a acciones en el plano físico (p. ej. territorio, detención) que tienen difícil aplicación en Internet; no parece razonable equiparar la detención de un sujeto en territorio extranjero al acceso a datos de este sujeto en una web alojada en territorio extranjero.

A la luz de lo anterior, está claro que un Estado no puede proceder a registrar un servidor que se encuentra ubicado fuera de su territorio con para acceder a datos en el marco de una investigación criminal. Ahora bien ¿qué ocurre cuando un Estado emite una orden para obligar a sujetos que están dentro de su jurisdicción a revelar información que no está almacenada dentro de su territorio? En estos casos ¿ocurriría la búsqueda y registro en el territorio donde se ubican los centros de datos en cuestión, o donde el proveedor de servicios de Cloud tiene control? ¿Qué pasa si existen copias en distintos territorios, incluido en el del Estado requirente? En el siguiente apartado se analizan estas cuestiones.

En este sentido, el Informe de la Comisión de Derecho Internacional sobre la jurisdicción extraterritorial ha sugerido la conveniencia de crear disposiciones específicas para abordar este tipo de cuestiones especiales, que no pueden ser tratadas adecuadamente a través de principios y reglas generales.

[144] UNITED NATIONS: "Report of the International Law Commission". New York, 2006. Anexo E, p. 536 .http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf

c) El ejercicio territorial de la jurisdicción puede tener efectos extraterritoriales

A diferencia del mundo físico, el mundo digital permite el acceso remoto a información. Esta posibilidad ha abierto nuevos escenarios en los que un Estado con jurisdicción sobre una persona jurídica establecida dentro de un territorio determinado puede compeler a dicha entidad a entregar o hacer accesibles datos que se encuentran almacenados o replicados en otras jurisdicciones ¿se considera éste un ejercicio válido de la jurisdicción?

Si bien los Principios de Harvard dibujaron los principios que rigen la **existencia** o afirmación válida de jurisdicción, el punto de partida para el examen de las normas del Derecho Internacional que rigen el **ejercicio** extraterritorial de la jurisdicción se estableció por la Corte Permanente de Justicia Internacional en 1927 en el marco del caso Lotus.[145]

La Corte estableció que la jurisdicción de un Estado es de naturaleza territorial y un Estado no puede ejercer su jurisdicción fuera de su territorio en ausencia de una norma del derecho internacional permisiva a tal efecto. Sin embargo, la Corte

[145] Caso Lotus (Francia vs. Turquía) Corte Permanente de Justicia Internacional, Ser. A, No. 10, 1927. Disponible en: http://www.dipublico.org/10984/s-s-lotus-1927-corte-permanente-de-justicia-internacional-ser-a-no-10/

distinguió entre el ejercicio de la jurisdicción por un Estado **fuera de su territorio** y el ejercicio de la jurisdicción por un Estado **dentro de su territorio** con respecto a las personas, los bienes o actos que se encuentra **fuera de su territorio**. El Tribunal indicó que los Estados tienen amplia discreción con respecto al ejercicio de la jurisdicción, y que todo lo que puede requerirse a un Estado es que no debe sobrepasar los límites que el derecho internacional impone sobre su jurisdicción.[146]

Tal y como apunta Ortiz Pradillo,[147] ha habido debate sobre cómo ha de interpretarse o no la actual concepción de la territorialidad y de la jurisdicción cuando nos referimos al ciberespacio, y en particular, cuando tratamos la obtención de prueba electrónica por parte de las autoridades encargadas de la investigación criminal.

Cada vez es más frecuente la obtención de prueba electrónica (por ejemplo, el registro e incautación de datos almacenados en equipos informáticos, la cesión directa de los datos de tráfico de las comunicaciones electrónicas, la monitorización de cuentas bancarias, etc.) presenta una importante peculiaridad: puede resultar posible su obtención directa en el territorio de otro Estado sin necesidad de que ocurra un desplazamiento físico a dicho Estado.

[146] Caso Lotus (Francia vs. Turquía) Corte Permanente de Justicia Internacional, Ser. A, No. 10, 1927. Disponible en: http://www.dipublico.org/10984/s-s-lotus-1927-corte-permanente-de-justicia-internacional-ser-a-no-10/

[147] ORTIZ PRADILLO, J.: "Problemas Procesales de la Ciberdelincuencia", Colex. Madrid, 2013, p.206.

d) Internet necesita un nuevo enfoque

El sistema internacional está saturado de retos a los enfoques tradicionales sobre el ejercicio de la jurisdicción y de casos reflejando las dificultades actuales. Y es que en el mundo digital la territorialidad ya no proyecta necesariamente una imagen fidedigna de la realidad.[148]

Para algunos, la territorialidad históricamente se estableció atendiendo entre otras a razones prácticas como son el aseguramiento de la eficacia penal por la proximidad de juzgar el hecho cerca de donde se ha realizado; la mayor facilidad para la obtención de las pruebas[149.] no obstante, en el ciberespacio este criterio con frecuencia no aporta valor en el orden práctico.

El ejercicio de la jurisdicción extraterritorial por un Estado con respecto a las personas, los bienes o actos fuera de su territorio se ha convertido en un fenómeno cada vez más común, en gran parte como consecuencia del aumento de la circulación de las personas más allá de las fronteras nacionales, el creciente número de

[148] MICHAELS, Ralf: "Territorial Jurisdiction After Territoriality" en Globalisation and Jurisdiction" editado por SLOT, Pieter J. BULTERMAN, Mielle K. Kluwer Law International, Países Bajos 2004, p.113.

[149] MORILLAS CUEVA, Lorenzo: "Curso de Derecho penal español. Parte general", Madrid, Marcial Pons, 1996, p. 120. Citado por SANZ HERMIDA, Ágata: "Extraterritorialidad de la Ley Penal y Jurisdicción" Madrid, 1999. Disponible en: https://www.uclm.es/area/procesal/Extraterritorialidad.htm#_ftn36

empresas multinacionales, la globalización de la economía mundial, el aumento de las actividades delictivas transnacionales y el uso de Internet.[150] Cuando las autoridades competentes buscan evidencias que se encuentran o podrían encontrarse en servicios de Cloud Computing (p. ej. mensajes de correo electrónico, código malicioso, documentos, identidades, etc.) el tratamiento global de información, hace extremadamente complicado determinar a *priori* el lugar donde la información reside.

Los principios de Harvard resultan insuficientes para regular las cuestiones jurisdiccionales inherentes a Internet y al Cloud Computing. Por una lado, el objetivo de la investigación de Harvard era proponer "los factores de conexión legítimos para afirmar la existencia de jurisdicción" y no para proponer cómo se debía ejercer dicha jurisdicción. Por otro lado, esta última cuestión era apenas relevante el 1935, cuando no era siquiera previsible la existencia de Internet y de un mundo global e interconectado, en el que las evidencias necesarias para la persecución y castigo de los delitos no se encontrarían, por regla general, en el territorio del Estado que afirma la jurisdicción.

[150] UNITED NATIONS: "Report of the International Law Commission". New York, 2006. Anexo E. p. 516 y ss. Disponible en: http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf

Con miras a una posible solución, resulta particularmente interesante la propuesta de Svantesson[151] sobre los tres principios básicos, o más bien, requisitos, que deberían reemplazar los principios de Harvard como punto de partida:

1. Que haya una **conexión sustancial** entre el asunto y el Estado que buscar ejercer jurisdicción;
2. Que el Estado que buscar ejercer jurisdicción tenga un **interés legítimo** en el asunto;
3. Que el ejercicio de la jurisdicción sea **razonable**, dada la **proporcionalidad** entre el interés legítimo del Estado reclamante y los intereses en competencia de otros Estados.

La propuesta de Svantesson está formada principalmente por conceptos jurídicos indeterminados, que si no se acompañan de algunos criterios objetivos podrían crear una inseguridad jurídica indeseable, no obstante, si estos conceptos se utilizan para complementar los principios de Harvard en vez de para reemplazarlos podrían obtenerse guías razonables para determinar cuándo el ejercicio de la jurisdicción en Internet es legítimo.

[151] SVANTESSON, Dan B: "A new legal framework for the age of cloud computing". The conversation, 2015. https://theconversation.com/a-new-legal-framework-for-the-age-of-cloud-computing-37055

4.7. La lucha por la soberanía sobre los datos

Alrededor del mundo, algunos gobiernos han reaccionado a algo que se percibe como pérdida de soberanía sobre los datos de sus ciudadanos principalmente de dos maneras (i) requiriendo la localización de los datos de sus ciudadanos dentro de sus fronteras nacionales (ii) otorgando un efecto extraterritorial a su ley, estableciendo que esta se aplicará a los datos de sus ciudadanos con independencia de la ubicación de dichos datos.

a) Localización forzada

- En agosto de 2014, Rusia aprobó una ley de localización de datos[152], que obliga a las empresas a almacenar los datos personales de los ciudadanos rusos en el territorio de la federación rusa, al menos en primera instancia, sin perjuicio de que puedan almacenarse copias de respaldo o réplicas en el territorio de otros Estados. La norma, cuya entrada en vigor se produjo el 1 de Septiembre de 2015, en principio obligaría a los clientes de Cloud Computing a utilizar proveedores con infraestructura local, lo cual podría repercutir en el tipo y nivel de servicios, así como su coste para los usuarios finales. De conformidad

152 http://www.hldataprotection.com/2015/08/articles/international-eu-privacy/russia-update-regulator-publishes-data-localization-clarifications/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ChronicleOfDataProtection+%28HL+Chronicle+of+Data+Protection%29

con la guía no oficial del Ministerio de Comunicaciones ruso, las restricciones a la localización aplicarían únicamente a la información en reposo o en almacenamiento por cuanto "la ley permite acceder a los datos desde cualquier parte del mundo".[153] Se ha expresado que la norma sólo busca fortalecer las capacidades de los servicios nacionales de inteligencia a nivel local y los poderes de investigación de la justicia criminal rusa sobre los datos de sus ciudadanos, las cuales normalmente debían iniciar procedimientos asistencia judicial para la obtención de datos almacenados por proveedores de servicios de Cloud Computing ubicados en otros Estados, sin tener ningún beneficio específico para la privacidad.[154]

- En 2013, Brasil decidió abandonar su propuesta de ley de localización de datos sobre la base de que "obligar a los proveedores a construir o usar centros de datos o servidores en Brasil incrementaría significativamente los costes para los usuarios, ahuyentaría a las compañías de Internet, no garantizaría la protección contra los agentes maliciosos par quienes ubicación de los ordenadores conectados a Internet es irrelevante, y que pueden interceptar

[153] EUROPEAN Commission: "Trusted Cloud Europe". Bruselas, 2014. https://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

[154] KUNER, Christopher: "Requiring local storage of Internet data will not protect privacy", Oxford University Press 2013. Disponible en: http://blog.oup.com/2013/12/data-security-privacy-storage-law/#sthash.L9zl47Bl.Dc8nkwDS.dpuf

> datos enrutados a través de Internet; y haría la vigilancia de los ciudadanos brasileños más fácil para la policía y los servicios de inteligencia locales".[155]
>
> En su lugar, Brasil aprobó la ley conocida como Marco Civil de Internet, que introdujo un principio de aplicación extraterritorial de la norma, extendiendo la jurisdicción de Brasil, incluyendo los requisitos para cumplir con las peticiones de cumplimiento forzoso de la ley, a las organizaciones no brasileñas en relación con los datos de los ciudadanos brasileños, donde quiera que dichos datos se encuentren. La extensión del alcance territorial de las leyes nacionales en materia de cooperación penal ha sido implementada también por el Reino Unido.[156]

La localización forzada también se ha propuesto como medida para contrarrestar los riesgos de intrusiones indebidas en la privacidad por parte de gobiernos extranjeros. En Europa, tras las filtraciones de Snowden se propuso el establecimiento de una nube Schengen y más allá, de un Internet Schengen que involucraría restricciones en

[155] WESTMORELAND, Kate: "Jurisdiction over user data - what is the ideal solution to a very real world problem". Julio, 2014. The Center for Internet and Society at Stanford Law School. Disponible en: http://cyberlaw.stanford.edu/blog/2014/07/jurisdiction-over-user-data-what-ideal-solution-very-real-world-problemhttps://www.leviathansecurity.com/blog/the-value-of-cloud-security/

HON, W. Kuan. MILLARD, Christopher. REED, Chris. SINGH, Jatinder. WALDEN, Ian. CROWCROFT, Jon: "Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Queen Mary School of Law Legal Studies Research Paper 191/2015. London, 2015 Disponible en SSRN: http://ssrn.com/abstract=2527951 p.18.

[156] A través de su ley DIRPA.

el enrutamiento de las comunicaciones y en el almacenamiento de los datos de los residentes europeos. Se sostuvo que esta idea pretendía "mantener a los usuarios de los ciudadanos más seguros y fuera de las manos de piratas informáticos, servicios de inteligencia extranjeros y autoridades extranjeras sin intermediación de autoridades locales a través de los canales de asistencia mutua." [157]

La propuesta fue criticada tanto desde la perspectiva técnica, como jurídica por las siguientes razones.

- Desde el punto de vista de la seguridad, resulta difícil ver cómo técnicamente una nube Schengen ayudaría a resolver el problema del intento de acceso ilegal por parte Estados extranjeros. Exactamente como ocurre con la ciberdelincuencia ordinaria, los ciberataques patrocinados por los Estados pueden iniciarse en cualquier lugar del mundo donde haya una conexión a Internet, y pueden dirigirse a cualquier infraestructura u organización conectadas a Internet con independencia de su ubicación. La localización forzada no es necesaria o suficiente para asegurar que los datos estarán

[157] http://www.euractiv.com/infosociety/merkel-hollande-lay-foundation-p-news-533560

protegidos y que son tratados adecuadamente.[158] Los datos pueden residir exclusivamente en Europa y no contar con medidas técnicas apropiadas.

- Desde la perspectiva jurídica, la localización forzada tampoco es necesaria o suficiente para garantizar que los datos son tratados en conformidad con las normas europeas sobre protección de datos. Asimismo, en los escenarios de acceso gubernamental legítimo o amparado en ley,[159] claramente las preocupaciones tiene que ver con que un Estado con jurisdicción sobre un proveedor de Cloud Computing no europeo (por ejemplo, los EE.UU. sobre proveedores establecidos en su territorio) pueda obligar al proveedor, directamente y sin hacer uso de mecanismos de asistencia judicial, a revelar los datos a los tiene acceso a través de los servicios de Cloud,[160] aun cuando estos datos residan fuera de los EE.UU., por ejemplo en Europa, el proveedor estará obligado a cumplir con su ley nacional y a responder frente a las

[158] HON, W. Kuan. MILLARD, Christopher. REED, Chris. SINGH, Jatinder. WALDEN, Ian. CROWCROFT, Jon: "Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Queen Mary School of Law Legal Studies Research Paper 191/2015. London, 2015 Disponible en SSRN: http://ssrn.com/abstract=2527951 p.13.

[159] Sobre el acceso gubernamental legítimo en contraposición a acceso ilegal véase el Capítulo IV.

[160] Hon, W. Kuan and Millard, Christopher and Reed, Chris and Singh, Jatinder and Walden, Ian and Crowcroft, Jon, Policy, Legal and Regulatory Implications of a Europe-Only Cloud (November 21, 2014). Queen Mary School of Law Legal Studies Research Paper 191/2015. Disponible en SSRN: http://ssrn.com/abstract=2527951 p.10.

autoridades competentes, no siendo la ubicación de los datos una excepción válida que exonere del cumplimento en la actualidad.[161]

- En el plano tecnológico, eventuales restricciones de enrutamiento necesitan implementarse a nivel de la infraestructura de comunicaciones, no al nivel de IaaS, PaaS o SaaS. Dada la arquitectura abierta de Internet, existe una imposibilidad práctica de imponer barreras al enrutamiento.[162] La infraestructura principal de Internet consiste en cables de fibra óptica de alta capacidad desplegados bajo los océanos y mares del mundo, y los cables terrestres asociados y routers. Los cables más importantes de Europa son los que funcionan desde Europa continental hasta Reino Unido, y desde hasta los EE.UU. pasando por el Océano Atlántico. Dado que dominio de Internet y de la nube por empresas estadounidenses, estos cables gestionados por dichas empresas llevan una gran parte de todo el tráfico de Internet y datos de comunicación basados en Internet, incluyendo casi todos los datos hacia y desde Europa.[163] Del mismo modo, la iniciativa de Internet Schengen va en

[161] Un análisis sobre este tema puede verse en el caso Microsoft.

[162] Hon, W. Kuan and Millard, Christopher and Reed, Chris and Singh, Jatinder and Walden, Ian and Crowcroft, Jon, Policy, Legal and Regulatory Implications of a Europe-Only Cloud (November 21, 2014). Queen Mary School of Law Legal Studies Research Paper 191/2015. Disponible en SSRN: http://ssrn.com/abstract=2527951 p.10.

[163]KORFF, Douwe. V: "The rule of law on the Internet and in the wider digital world", p.8. Disponible en:http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/70114_Rule%20of%20Law%20on%20the%20Internet_web.pdf, Consejo de Europa, 2014, p.124.

contra de la forma en la actualidad funciona el tráfico global de Internet a nivel comercial. El tráfico pasa de una red a otra bajo acuerdos gratuitos o de pago, sin consideración ninguna de las fronteras nacionales. A nivel internacional no existen precedentes en los que el tráfico de Internet de un país desarrollado evite o haga *bypass* a los servidores de otro país. [164] A propósito de la propuesta de creación de una Internet local en Alemania, el presidente ejecutivo de Deutsche Telekom afirmó que "proponer una Internet alemana sería como proponer un Sol alemán".[165] Asimismo, de poder existir un enrutamiento alemán, los servicios secretos de los Estados fuera de esta área encontrarían más difícil (pero no imposible) acceder ilegalmente a este tráfico de datos. Por tanto la solución al problema subyacente no sería técnica, sino política.[166]

- Se ha sugerido que otros motivos de esta propuesta podrían haber sido facilitar el acceso de las propias autoridades nacionales a los datos.[167]

[164] KORFF, Douwe. V: "The rule of law on the Internet and in the wider digital world". Disponible en:http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/70114_Rule%20of%20Law%20on%20the%20Internet_web.pdf, Consejo de Europa, 2014, p.8.

[165] KORFF, Douwe. V: "The rule of law on the Internet and in the wider digital world". Disponible en:http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/70114_Rule%20of%20Law%20on%20the%20Internet_web.pdf, Consejo de Europa, 2014, p.8.

[166] The Washington Post, citando a Norbert Pohlmann , director del Instituto para la Seguridad en Internet de la Universidad de Ciencias Aplicadas de Westfalia en Gelsenkirche.

[167] HON, W. Kuan. MILLARD, Christopher. REED, Chris. SINGH, Jatinder. WALDEN, Ian. CROWCROFT, Jon: "Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Queen Mary School of Law

- También se advirtieron implicaciones de libre comercio. La medida fue valorada por algunos como proteccionismo económico o de ayudas estatales hacia proveedores de Cloud Computing locales.[168]

En materia de localización se han manifestado preocupaciones sobre los impacto negativo para Internet per se. Si más Estados se aíslan a sí mismos, esto podría conducir a una "Balcanización" de Internet, paralizando la apertura y la eficiencia que han hecho de la web una fuente de crecimiento económico pueden crearse regulaciones que bloqueen el comercio en los servicios de la sociedad de la información, pero esto habría grandes sacrificios de la eficiencia económica.[169]

extranjeros y capacidades de acceso que se pueden utilizar contra los proveedores de nube fuera de la República Federal de Alemania"[170].

Legal Studies Research Paper 191/2015. London, 2015 Disponible en SSRN: http://ssrn.com/abstract=2527951 p.6.

[168] SCHWARTZ M., Paul: "Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment". UC Berkeley School of Law. USA. 2009, p16.

[169] HON, W. Kuan. MILLARD, Christopher. REED, Chris. SINGH, Jatinder. WALDEN, Ian. CROWCROFT, Jon: "Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Queen Mary School of Law Legal Studies Research Paper 191/2015. London, 2015 Disponible en SSRN: http://ssrn.com/abstract=2527951 p.14.

[170] http://www.euractiv.com/sections/infosociety/germany-set-bundescloud-316939

Debido a la imposibilidad de derogar normativa aplicable por vía contractual[171] parece que la nube gubernamental alemana solo quedaría abierta en términos de mercado a aquellos operadores establecidos en Alemania, y que no están establecidos y por tanto sujetos a las normas de otro Estado.

Desde la perspectiva de la seguridad, estos requerimientos de localización resultan cuestionables. Incluso si los datos son almacenados exclusivamente en Alemania, cuando se transmiten a través de Internet, pueden ser interceptados por actores extranjeros, que pueden ser Estados. Asimismo, las buenas prácticas ordenan que al menos una copia de los datos se deba almacenar en una zona geográfica distinta a efectos de continuidad del negocio y de la recuperación ante desastres. De nuevo, la localización no garantiza que la información sea inmune a ataques desde cualquier ubicación por actores maliciosos, incluidos actores estatales. La ubicación física de los datos es irrelevante desde la perspectiva técnica cuando hablamos de seguridad ante ataques bien por parte de actores privados o de actores. Sobre los requisitos de localización, el documento "Política de Establecimiento de una Nube de Confianza para Europa" elaborado por el Consejo Directivo de la Asociación Europea de Cloud Computing de la Comisión Europea[172] expresó una visión clara sobre el tema "a menudo es posible y aconsejable sustituir requisitos formales legales (como la

[171] En este sentido, véase el Capítulo IV.

[172] The European Cloud Partnership Steering Board: "Establishing a Trusted Cloud Europe". Brussels 2014. p.19. Disponible en: https://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

ubicación geográfica de los datos) por los requisitos funcionales correspondientes (tales como garantizar la accesibilidad y la seguridad de los datos).Asimismo, de acuerdo con la estrategia de mercado único digital de la Comisión "los requisitos de datos de localización pueden, de hecho, limitar los beneficios que ofrece servicios digitales, como la computación en nube, ya que crean barreras para las transferencias de datos de la UE transfronterizas, lo que limita la elección de competencia entre los proveedores y el aumento de los costos al obligar organizaciones y empresas para almacenar datos en servidores ubicados físicamente dentro de un determinado Estado miembro".

No obstante lo anterior, las nuevas normas alemanas para el Cloud Computing en el ámbito gubernamental establece que datos oficiales sólo pueden ser procesados en Alemania, además los proveedores deberían "firmar un acuerdo de no divulgación, según el cual estos datos no pueden terminar en obligaciones de información estatales.

Desde la perspectiva jurídica, cuando se trata de acceso gubernamental a la información amparado en la ley, la ubicación física de los datos es irrelevante si un tercer Estado tiene jurisdicción sobre el proveedor o sobre el cliente de servicios de Cloud Computing, y puede realizar un ejercicio válido de la misma encaminado a solicitar dicha información. Si bien la localización forzada de datos no es una solución

que haya demostrado tener beneficios concretos para la seguridad y la privacidad de los datos, los equipos y centros de datos deberían estar situados en países donde imperen el Estado de Derecho y los valores democráticos.[173]

[173] "Derecho y Cloud Computing" coordinado por MARTINEZ, Ricard, Civitas, Madrid, 2012, p.34.

5. CAPÍTULO IV. ACCESO GUBERNAMENTAL A LA INFORMACIÓN EN LA NUBE

La información tratada por un proveedor de servicios de Cloud Computing en nombre y por cuenta de una organización puede llegar a ser relevante en el marco de un litigio entre particulares, o para la prevención o persecución de actividades delictivas, exactamente del mismo modo en que puede serlo la información almacenada localmente en un servidor, en un ordenador portátil, o en los archivos de la gestoría externa que se encarga de la llevanza de la contabilidad de dicha organización.

La sujeción de la información a la ley y a los poderes de investigación del Estado (o los Estados) con jurisdicción sobre el cliente de cloud, con independencia de si dicha información se encuentra bajo la custodia directa del sujeto obligado, o de un tercero prestador de servicios no es una cuestión nueva.

No obstante, no existe claridad sobre si el uso de servicios de Cloud Computing produce necesariamente un incremento de la exposición jurisdiccional de la información.[174] Como se ha visto en el Capítulo anterior, el carácter transnacional de

[174] WESTMORELAND, Kate: "Jurisdiction over user data - what is the ideal solution to a very real world problem". Julio, 2014. The Center for Internet and Society at Stanford Law School. Disponible en: http://cyberlaw.stanford.edu/blog/2014/07/jurisdiction-over-user-data-what-ideal-solution-very-real-world-problemhttps://www.leviathansecurity.com/blog/the-value-of-cloud-security/

los servicios de Cloud Computing plantea en primer lugar dudas sobre los poderes de investigación de las autoridades del país o países terceros donde el proveedor de Cloud Computing posee u opera centros de datos que almacenan la información de titularidad del cliente. Como se ha apuntado, en el Cloud Computing no puede fusionarse la ubicación geográfica con la jurisdicción.[175] En segundo lugar, existen dudas sobre la eventual exposición a la jurisdicción del Estado donde el proveedor de Cloud Computing está establecido (que suele ser un país tercero), especialmente en los supuestos en los que el proveedor tendría la obligación legal de colaborar con las autoridades revelando información[176] sin que el cliente tenga control u oportunidad procesal *ex ante* de oponerse o controlar dicha solicitud de información.

Mientras en el ámbito de las disputas civiles y mercantiles no se contempla en principio la obtención procesal de pruebas en secreto,[177] en el ámbito penal sí que se permiten las investigaciones subrepticias en determinados casos, cuando se pueda poner en peligro el resultado de una investigación. Ante estos supuestos, la notificación al cliente de Cloud estaría prohibida o solo se autorizaría *a posteriori* una

[175] Vid 3.6 (a).

[176] Sobre el uso de los servicios servicios, como la última vez que un usuario se conecta, o sobre el contenido almacenado en los servicios, así como los mensajes de correo electrónico, o documentos.

[177] En España, por ejemplo, la LEC de 2000 no contempla ningún supuesto de autorización de intervención de comunicaciones de las partes por hechos relevantes para el proceso civil, tal y como apunta MONTERO AROCA, J.: "La prueba en el proceso civil", Ed. Civitas, 5ª ed., Madrid 2007, p. 162. Citado por BELLIDO PENADÉS, R.: "La Prueba Ilícita y su control en el Proceso Civil". Revista Española de Derecho Constitucional ISSN: 0211-5743, núm. 89, mayo-agosto (2010), p. 86.

vez que la entrega de la información se ha producido. Estas prohibiciones son frecuentes en investigaciones en el ámbito de la lucha contra el terrorismo y relacionadas con la seguridad nacional.[178]

Los pactos contractuales para evitar estas situaciones no parecen una solución jurídicamente viable. Como principio general, los distintos ordenamientos jurídicos, incluido el español,[179] precluyen a las partes de establecer pactos, cláusulas o condiciones contrarias a normas de orden público tales como las impuestas por el Derecho Penal. Asimismo, la violación del deber de secreto en un procedimiento penal constituye normalmente una infracción penal en sí misma.

En el ámbito del Cloud Computing es frecuente que el país del establecimiento principal del cliente y del proveedor de cloud respectivamente, sean distintos, y por tanto el derecho sustantivo y procesal rector también sea distinto. Desde la perspectiva de la gestión del riesgo legal, en estos casos el cliente de Cloud Computing debe determinar si la ley a la que está sujeto el proveedor en función de

[178] Con relación a los delitos se refiere a investigaciones para la protección contra el terrorismo internacional y las actividades clandestinas de inteligencia, 18 U.S. Code § 2709 permite al FBI prohibirle al destinatario de una NSL divulgar su recepción, si el FBI certifica que tal hecho podría "poner en peligro la seguridad nacional de los Estados Unidos o la vida o la seguridad física de otras personas, o interferir en relaciones diplomáticas o investigaciones criminales o investigaciones destinadas a combatir el terrorismo u operaciones de inteligencia".

[179] Artículo 1.255 del Código Civil.

su establecimiento, ofrece un nivel de protección equiparable al de su ordenamiento jurídico no, y en su caso, si hay un conflicto entre los mismos.

En Europa, actualmente el acceso de autoridades a la información en la nube se percibe como uno de los principales riesgos inherentes a la adopción de los servicios de Cloud Computing, particularmente en relación con las autoridades de los Estados Unidos, en un mercado global de Cloud Computing en el que la los proveedores de cloud estadounidenses en la actualidad dominan. Estas preocupaciones crecieron exponencialmente tras las filtraciones de información clasificada en el año 2013 por Edward Snowden sobre los programas de vigilancia masiva practicados por la NSA.

Son frecuentes los análisis y afirmaciones que parten de premisas incorrectas, por ejemplo, la confusión del acceso gubernamental ilegal[180] con el acceso gubernamental amparado en la ley. Desde la perspectiva de gestión de los riesgos de privacidad y seguridad, se trata de dos amenazas completamente distintas, cuyas medidas de mitigación son también distintas. Asimismo, es importante distinguir el acceso gubernamental con fines de cumplimiento forzoso de la ley o de *law enforcement* del acceso con fines de seguridad nacional e inteligencia. En este capítulo se aportan algunas notas distintivas útiles que sirven para valorar

[180] Por ejemplo, a través de técnicas de intrusión física o de intrusión informática.

adecuadamente el riesgo, apoyar procesos de contratación de servicios de Cloud Computing.

El acceso gubernamental a la información en la nube es tema en plena ebullición y controvertido sobre el que no existe un acuerdo global. Cuando un Estado tiene jurisdicción para perseguir un delito con arreglo a los principios analizados en el Capítulo III ¿cómo puede ejercerla cuando los datos están "en la nube"? En este capítulo se analizará esta cuestión de forma general y a la luz de las reglas para su ejercicio en España, los EE.UU. y el Reino Unido.

5.1. Posición jurídica de las partes contratantes en el Cloud Computing

5.1.1. Responsable vs custodio de la Información

El contrato de Cloud Computing puede definirse como un contrato informático en virtud del cual el prestador pone a disposición del prestatario, aplicaciones informáticas, infraestructura de almacenamiento y/o plataformas para el desarrollo de aplicaciones informáticas, bajo demanda y a través de Internet, a cambio de una contraprestación que estará determinada por los recursos que se consuman en cada

momento por el prestatario, o en su caso, de la aceptación de unas condiciones determinadas bajo la fórmula de la adhesión.[181]

No existe una transferencia de titularidad o control de la información, el proveedor de servicios de cloud es un mero prestador de servicios de tecnología, que no cuenta con la titularidad o poder de decisión alguna sobre los activos de información alojados en sus servicios. En ocasiones puede no llegar a tener siquiera acceso inteligible a la información de alojada en sus servicios.[182] En consecuencia, es el cliente de cloud en calidad de titular de la información y en su caso, de responsable del tratamiento de datos de carácter personal quien se configura como sujeto principal legitimado para recibir, valorar, atender, o en su caso, impugnar dichas solicitudes por parte de autoridades gubernamentales.

5.1.2. El rol del responsable de la información

Por regla general, los contratos de Cloud Computing en el ámbito B2B establecen al cliente como principal responsable de atender a eventuales solicitudes de

[181] REY, Nathaly: "La Contratación de Servicios de Cloud Computing: Consideraciones sobre la Seguridad de la Información". Tesina de Doctorado, Universidad Complutense de Madrid, 2013.

[182] Esta situación se daría, por ejemplo, en los casos en las que la información se encuentra cifrada y las llaves de dicho cifrado son gestionadas por el cliente de servicios de Cloud Computing.

información por parte de las autoridades.[183] Esta configuración del cliente de cloud como legitimado pasivo principal resulta razonable tanto desde la perspectiva sustantiva como de la perspectiva procesal. Es el cliente quien determina quiénes son los usuarios de sus servicios, cómo dichos usuarios pueden utilizar los servicios, y si la información que sus usuarios finales almacenan o tratan en determinados servicios de Cloud Computing está sujeta a determinada ley o regulación específica. Asimismo, desde la perspectiva procesal, es el cliente de cloud quien está en la posición correcta para defensa de sus derechos e intereses en el marco de una investigación por parte de las autoridades competentes.

5.1.3. El rol del custodio de la información

Por su parte, corresponde al proveedor de servicios de Cloud Computing, en calidad de custodio de la información, garantizar que los servicios permitan el cumplimento de dichas solicitudes, a través de la incorporación de herramientas tecnológicas adecuadas para producir información (visualizar, extraer, exportar en formatos estándar) y de dar soporte para la correcta utilización de dichas herramientas.

Ahora bien, ¿Qué ocurre cuando una solicitud se dirige directamente al proveedor de Cloud Computing? En este caso, el proveedor deberá examinar la solicitud a la luz de

[183] En este sentido véanse por ejemplo los términos y condiciones de Servicio de Dropbox para empresas https://www.dropbox.com/business_agreement, Google Apps para empresas http://www.google.com/apps/intl/en-GB/terms/premier_terms_ie.html, y Microsoft 365 para empresas http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=7703.

las normas que aduce la autoridad solicitante en cuestión, y en su caso, a la luz de las normas jurídicas que aplican al propio proveedor en función del lugar de su establecimiento.

Por vía contractual, es habitual la imposición de una obligación de notificación al cliente, salvo que la ley o la propia orden de la autoridad lo impida. Mientras en el ámbito de las disputas civiles la re-dirección o la notificación de la solicitud típicamente resultan posibles, en el ámbito penal existen mecanismos legales que habilitan las actividades investigación subrepticia en conexión con la persecución de delitos graves, que pueden impedir dicha notificación.

Este tipo de investigaciones se encuentra prevista prácticamente en la totalidad de ordenamientos jurídicos avanzados del mundo.[184] Así las cosas, los lineamientos generales reflejados en los contratos de Cloud Computing examinados reflejan lo siguientes: [185]

[184] En este sentido, véase MAXWELL, Winston. WOLF, Christopher: "A Global Reality: Governmental Access to Data in the Cloud". A Hogan Lovells White Paper. París, Washington, 2012. Disponible en: http://www.hoganlovells.com/files/Publication/80a807f2-e619-41dc-98e4-e6a7b5f6c5f8/Presentation/PublicationAttachment/9bab0ead-0b8b-4cdb-bb08-8ba1b95a9df9/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf

[185] En este sentido véanse por ejemplo los términos y condiciones de Servicio de Dropbox para empresas https://www.dropbox.com/business_agreement, Google Apps para empresas http://www.google.com/apps/intl/en-GB/terms/premier_terms_ie.html, y Microsoft 365 para empresas http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=7703.

1) El cliente es el principal responsable ante eventuales solicitudes de información, por tanto, este debe en primer lugar obtener o extraer por sí mismo la información necesaria para responder a una eventual solicitud (por ejemplo, utilizando las funcionalidades de exportación de datos existentes en los servicios) pudiendo solicitar apoyo del proveedor en el caso que no consiga obtener de una manera razonable dicha información.

2) Por su parte, el proveedor se comprometen a:

    a) En la medida permitida por la ley o por las condiciones de la solicitud particular, a informar sin demora al cliente de la recepción de la solicitud, de forma que este pueda interponer los recursos que estime oportuno.
    b) Proporcionar al cliente la información o las herramientas necesarias para que este responda a la solicitud.
    c) apoyar al de forma razonable al cliente en sus esfuerzos para oponerse a la solicitud.

En la práctica, las peticiones de información en el ámbito B2B suelen dirigirse directamente al cliente de Cloud Computing por una razón de orden práctico, por ejemplo, cuando la justicia criminal investiga a un empleado de la organización X, y

requiere acceder a las comunicaciones de dicho empleado con el individuo Y en el día Z, las autoridades competentes no tienen conocimiento, al menos *a priori* de si los servicios de correo electrónico de la organización X están gestionados por la propia empresa X en un centro de datos propio, o por un tercero como Acens, Telefónica, Google o Microsoft. Para sus propósitos esto es completamente irrelevante.[186]

En este sentido, resultan ilustrativas las estadísticas publicadas en el último Informe de Transparencia de Microsoft. A nivel Global, Microsoft recibió 52.997 peticiones de información alrededor del mundo, relacionadas con 31.002 usuarios. De este universo, en el ámbito B2B, Microsoft solo recibió tres solicitudes de información. En dos de estos casos, las solicitudes fueron rechazadas o redirigidas con éxito al cliente. En el tercer caso, el cliente fue notificado de la solicitud de información, y Microsoft dirigido por el cliente, proporcionó la información solicitada. Ninguna de ellas se tradujo en la revelación de información de usuarios por parte de Microsoft sin el consentimiento del cliente.[187]

[186] Normalmente, si éste se encuentra en su territorio, podrá dirigir a él directamente, en caso contrario deberá activar los mecanismos de cooperación internacional que resulte relevantes. Sobre estos mecanismos, véase el Capítulo V.
[187] Microsoft Transparecy Hub:
http://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/

5.1.4. La figura del encargado del tratamiento

A la luz de la normativa europea de protección de datos de carácter personal, el proveedor de servicios de Cloud Computing se configura como un encargado del tratamiento. Como tal, su rol se limita a cumplir con las instrucciones del responsable del tratamiento, siendo éste último a quien corresponde determinar las finalidades de dicho tratamiento, incluidas eventuales comunicaciones o cesiones de datos a terceros.

No obstante, existen situaciones en las que el encargado del tratamiento puede verse obligado a realizar una cesión de datos a las autoridades competentes en cumplimiento de una disposición legal. Este escenario se recoge en el art. 16 de la Directiva 95/46/CE, el cual establece el cumplimiento de un imperativo legal como excepción al deber de confidencialidad del encargado de tratamiento. Esta disposición ha quedado traspuesta en el ordenamiento jurídico español a través del artículo 12 la LOPD, en virtud del cual, toda relación de encargo del tratamiento (que deberá estar regulada en un contrato por escrito) debe recoger la prohibición de ceder los datos a terceros, salvo para el cumplimiento de obligaciones legales.[188]

[188] En este sentido, véase el art. 12 de la LOPD.

Los preceptos mencionados en materia de protección de datos resultan ilustrativos sobre los principios que rigen cesión de información a las autoridades competentes en Europa en líneas generales, no obstante, el régimen comunitario de protección de datos no resulta aplicable en el ámbito del ejercicio de la acción penal por el Estado. Esto se subraya en el Considerando 13 de la Directiva 95/46/CE "los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho Comunitario".[189]

5.2. Acceso gubernamental ilegal vs acceso legal

5.2.1. El acceso ilegal a información por parte de gobiernos

La preocupaciones relacionadas con el acceso gubernamental a la información en la nube crecieron exponencialmente tras las filtraciones por parte de Edward Snowden en el año 2013, en las que se revelaron numerosos programas de vigilancia a nivel mundial, muchos de ellos operados por la Agencia de Seguridad Nacional de Estados Unidos (NSA) y los países que conforman la llamada alianza de inteligencia de los Cinco Ojos.[190]

[189] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Considerando 13.

[190] Un resumen ilustrativo puede encontrarse en la siguiente entrada de Wikipedia https://en.wikipedia.org/wiki/Edward_Snowden

Entre otras actividades, se conoció que la NSA irrumpió ilegalmente en los cables privados de operadores distintos servicios de Internet, incluyendo servicios de Cloud Computing como Google y Yahoo, en los EE.UU y fuera.[191] También se conoció la interceptación rutinaria de datos de tráfico telefónicos en todo el mundo utilizando órdenes contra operadores de telecomunicaciones. En mayo de 2015, una corte federal de los EE.UU.[192] determinó que el programa de recogida masiva de datos de tráfico telefónicos, bajo el que NSA recabó en masivamente fue ilegal y no estuvo autorizado por el Congreso de los EE.UU.

La sentencia establece que la ley "Patriot Act", no podía interpretarse en el sentido de permitir a la NSA recoger una cantidad "asombrosa" de registros telefónicos. Tampoco contemplaba esta intrusión en la vida privada para mejorar la lucha contra el terrorismo, y afirma que la recopilación realizada por la agencia supone "una contradicción sin precedentes de las expectativas de privacidad de los americanos". En la sentencia, el juez Lynch también añadió que "quizá esta contradicción es necesaria para mantener la seguridad nacional frente a los peligros contemporáneos del terrorismo interno e internacional". Sin embargo, aclaró que una decisión de esa

191 http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

192 ACLU v. Clapper. Corte de Apelaciones de los Estados Unidos para el Segundo Circuito. NY, Mayo, 2015. Disponible en: http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf

naturaleza debe "ser precedida un fuerte debate, y expresada en un lenguaje inconfundible". Y que "no existe evidencia de tal debate". Patriot Act en cuestión expiró en mayo de 2015, tal y como preveía la propia norma, al no acordar el congreso la prolongación de su vigencia.[193]

La necesidad de asegurar el sometimiento de las actividades de inteligencia alrededor del mundo ha existido de largo tiempo. Los servicios de inteligencia, en cierta medida, han operado siempre al margen de la ley.[194] Las revelaciones sobre la NSA, GCHQ y los Cinco Ojos así como la puesta en conocimiento público de otros de programas de vigilancia de internet desplegados por España, Alemania[195] o Francia,[196] por citar algunos, han puesto sobre la mesa el debate sobre la vigilancia digital masiva y la necesidad de establecer una justa ponderación entre dos bienes fundamentales para las sociedades como son la privacidad y la seguridad. Este equilibrio debe marcarse por leyes producto de procesos democráticos, y no por parte de agencias o gobiernos de forma unilateral.

[193] Sobre el régimen de vigente en los EE.UU. se hablará en el Capítulo VI.

[194] HORNLE, Julia-Queen Mary University of London CPDP 2015: Law enforcement Internet Jurisdiction. Disponible en: https://www.youtube.com/watch?v=NL4nNlzyqmQ

[195] http://www.telegraph.co.uk/technology/10421835/Germany-France-and-Spain-were-all-spying-on-citizens.html

[196] http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

Y es que para algunos, en general las autoridades gubernamentales sostienen que no están accediendo a datos de forma ilegal en otros Estados, pero de hecho todas lo están haciendo.[197]

En el plano legal, en cuanto a las facultades de investigación de las autoridades gubernamentales, fuera de los Estados Unidos se ha observado una tendencia general a la ampliación de los poderes de investigación las autoridades y de los deberes de cooperación por parte de los actores privados, lo que pone de manifiesto la necesidad de las autoridades acceder a más información para garantizar el orden público. Como ejemplos pueden mostrarse las reformas impulsadas por Irlanda,[198] España,[199] Alemania[200] y Francia.[201]

[197] VELASCOS, Cristos, CPDP 2015: "Law enforcement internet jurisdiction". Disponible en: https://www.youtube.com/watch?v=NL4nNlzyqmQ

[198] http://www.irishtimes.com/business/technology/state-sanctions-phone-and-email-tapping-1.2027844

[199] http://politica.elpais.com/politica/2014/12/05/actualidad/1417793649_334772.html

[200] http://uk.reuters.com/article/2013/06/16/us-germany-spying-idUKBRE95F0EU2013061

[201] http://www.rt.com/op-edge/256049-france-new-spying-rules-law/

Resulta esencial distinguir entre el acceso gubernamental ilegal[202] del acceso gubernamental amparado en el Derecho de un Estado, o en el Derecho Internacional. Aunque frecuentemente se perciben como amenazas equivalentes, se trata de cuestiones fundamentalmente distintas desde la perspectiva jurídica y de seguridad, por tanto, los riesgos asociados a cada una de estas actividades necesitan valorarse y gestionarse de forma distinta.

5.2.2. El acceso legal como necesidad y deber del Estado

Los gobiernos tienen la obligación positiva de proteger a la sociedad frente al crimen a través de la aplicación forzosa de la ley cuando sea necesario. La creciente dependencia de las sociedades de las tecnologías de información y las comunicaciones viene acompañada del aumento de delitos en contra y por medio de sistemas de computación, sistemas que cada vez más adoptan forma de nubes.

Un objetivo principal de la aplicación forzosa de la ley o *law enforcement* es el aseguramiento de las pruebas. En relación con los delitos informáticos propiamente

[202] La investigación del Comité de Libertades Civiles del Parlamento Europeo señaló que las actividades de la NSA y su homólogo británico, GCHQ , parecían ser ilegales y que sus operaciones han "profundamente conmovido " la confianza entre los países que se consideraban aliados. http://www.theguardian.com/world/2014/jan/09/nsa-gchq-illegal-european-parliamentary-inquiry

dichos, y otros tipos de delincuencia que intersectan con la nube, el material probatorio toma la forma de pruebas electrónicas.[203]

Cuando se trata de peticiones de información amparadas en la ley, si bien los distintos ordenamientos difieren en su enfoque, las economías avanzadas cuentan facultades de aplicación de la ley y protecciones fundamentalmente similares. La posibilidad acceso gubernamental a la información almacenada en la nube, incluyendo el acceso transfronterizo, se contempla en una buena parte de los ordenamientos jurídico avanzados del mundo.[204] No obstante Las autoridades se enfrentan a desafíos complejos de legislación, jurisdiccionales y procedimentales al investigar y recopilar información cuando la información relevante para la investigación penal se encuentra o puede llegar a encontrarse en servicios de Cloud Computing.

La nube representa la manifestación de un entorno transnacional en el que las autoridades tienen que operar hoy en día, en el cual se presenta un panorama

[203] CYBERCRIME CONVENTION COMMITTEE (T-CY): "Transborder access to data and jurisdiction: Options for further action by the T-CY", p. 5. Estrasburgo, 2013. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)28_Plen10AbrRep_V3.pdf

[204] MAXWELL, Winston. WOLF, Christopher: "A Global Reality: Governmental Access to Data in the Cloud". A Hogan Lovells White Paper. 2012. Disponible en: http://www.hoganlovells.com/files/Publication/80a807f2-e619-41dc-98e4-e6a7b5f6c5f8/Presentation/PublicationAttachment/9bab0ead-0b8b-4cdb-bb08-8ba1b95a9df9/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf

multicolor de reglas aplicables. La comunidad internacional ha reconocido que es un reto acceder a datos almacenados en otra jurisdicción, y aun cuando los datos se encuentran almacenados en su jurisdicción, es un reto acceder a datos en poder de una entidad cuya sede se encuentra en otra jurisdicción.[205]

5.3. Seguridad nacional e inteligencia vs. aplicación forzosa de la ley

La separación entre el acceso gubernamental con fines de inteligencia y aquél para la aplicación forzosa de la ley queda plasmada que forma clara en la Convención de Budapest[206]. La inteligencia se basa en la obtención de "señales",[207] mientras que la aplicación de la ley busca la obtención de datos específicos por parte las autoridades de justicia criminal de cara a la investigación y persecución de hechos delictivos concretos. La Convención es un Tratado de Derecho Penal diseñado para su utilización en el marco de investigaciones penales específicas, no constituye un tratado en materia seguridad nacional que pueda utilizarse con fines de vigilancia de

[205] WALDEN, Ian: "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent". Queen Mary School of Law Legal Studies Research Paper No. 74/2011. November 14, 2011, p.2. Disponible en SSRN: http://ssrn.com/abstract=1781067

[206] Convención de Budapest. Convenio número 185, del Consejo de Europa, sobre Ciberdelincuencia, de 23 de noviembre de 2001. Disponible en: http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm

[207] Véase por ejemplo la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

masiva por las autoridades de inteligencia. La Convención de Budapest no permite la recogida o transferencia masiva de datos.[208]

En la actualidad no existen reglas basadas en tratados internacionales que gobiernen las acciones de las agencias de seguridad e inteligencia de los Estados y la base sobre la que operan e intercambian datos entre sí. En Europa la legislación comunitaria excluye expresamente la seguridad nacional de las competencias de la Unión.

Los Principios de Johannesburgo sobre Seguridad Nacional, Libertad de Expresión y Acceso a la Información, propuestos por la ONG del Artículo 19 y apoyados por diversos foros internacionales, aportan algunas guías parciales para ponderar las actividades de seguridad nacional por parte de los Estados. Estos Principios establecen que los Estados sólo pueden invocar la seguridad nacional como una razón para interferir con la libertad de expresión en relación con los asuntos que amenazan "la existencia del Estado o su integridad territorial"[209] básicas de la nación. Cuando las ofensas no alcanzar este nivel se deben tratar con reglas de aplicación forzosa de la ley en contraposición a la seguridad nacional. Aunque los principios

[208] CYBERCRIME CONVENTION COMMITTEE (T-CY): "Transborder access to data and jurisdiction: Options for further action by the T-CY", p. 5. Estrasburgo, 2014. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf

[209] ONG Article 19: "The Johannesburg Principles on National Security, Freedom of Expression and Access to Information" U.N. Doc. E/CN.4/1996/39, Londres, 1996. Principio 2. Disponible en: https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pd f

tratan en particular de la libertad de expresión, algunos han sugerido que podrían servir como guías en el ámbito de la privacidad y el secreto de las comunicaciones.[210]

A la luz de lo anterior, a los efectos del análisis de riesgos relacionados con el acceso gubernamental, se deben analizar, por un lado, las reglas que rigen la aplicación forzosa de la ley, para lo cual existen instrumentos internacionales de amplio alcance como la Convención de Budapest, que aporta principios comunes, así como la legislación aplicable a las partes en función de su establecimiento.[211] Por su parte, las reglas que rigen la seguridad nacional y la inteligencia se deben analizar a nivel local y de forma comparativa al no existir instrumentos internacionales de referencia.

[210] KORFF, Douwe. V: "The rule of law on the Internet and in the wider digital world". Disponible en: http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/70114_Rule%20of%20Law%20on%20the%20Internet_web.pdf, Consejo de Europa, 2014.

[211] Por ejemplo, las obligaciones de cesión de datos contenidas en el llamado *Marco Civil da Internet* de Brasil y la DIRPA del Reino Unido parecen aplicar a los datos de ciudadanos de Brasil y del Reino Unido, respectivamente, con independencia del establecimiento del proveedor.

6. CAPÍTULO V: COOPERACIÓN PENAL INTERNACIONAL Y CLOUD COMPUTING

El fundamento de la cooperación internacional se encuentra en la limitación territorial de la jurisdicción del Estado, y en consecuencia, en la imposibilidad jurídica para las autoridades de un Estado de practicar pruebas fuera su territorio, lo cual exige la colaboración de las autoridades del Estado extranjero donde las pruebas han de realizarse. Para justificar la cooperación internacional se invocan principios de Derecho Público, principalmente la soberanía de los Estados, la cortesía internacional y la reciprocidad. [212]

Las reglas de cooperación internacional se enfrentan a una realidad que diluye sustancialmente la limitación territorial de la jurisdicción como es Internet. Un Estado puede obtener desde de su territorio, sin necesidad de desplazarse físicamente obtener pruebas digitales que se encuentran almacenadas fuera del mismo (p.ej. en tránsito a través de los cables de Internet, en aguas internacionales, o almacenados en equipos que se encuentran terceros Estados).

[212] GARCIMARTIN ALFÉREZ, Francisco J.: "Sobre el fundamento de la cooperación jurídica internacional", Cooperación jurídica internacional, Colección Escuela Diplomática núm. 5, Madrid, 2001, pp. 61-68.

6.1. La Convención de Budapest[213]

La Convención de Budapest[214] del año 2001 se constituye como el primer tratado internacional de Derecho Penal contra la criminalidad informática. Se trata de una Convención Europea[215] abierta también terceros Estados no europeos para su firma. Hasta la fecha ha sido ratificada por 41 Estados, incluidos los EE.UU., España[216] y el Reino Unido.

La Convención tiene por objeto completar otros tratados internacionales de cooperación en el ámbito penal, con el fin de hacer más eficaces las investigaciones y procedimientos penales para perseguir y castigar las infracciones vinculadas a sistemas informáticos e información (delitos informáticos propiamente dichos) así como permitir la recogida de pruebas electrónicas relacionadas con una infracción penal cometida a través de medios informáticos.[217]

[213] Convenio número 185, del Consejo de Europa, sobre Ciberdelincuencia, de 23 de noviembre de 2001 http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm

[214] El Convenio y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa abierto a firma el año 2001. El instrumento entró en vigor el 1 de julio de 2004.

[215] Estados no miembros como Canadá, Japón, Sudáfrica y Estados Unidos participaron en su redacción.

[216] España ratificó la Convención mayo de 2010.

[217] Vid. Exposición de Motivos de la Convención de Budapest.

En la parte sustantiva, la Convención exige a los Estados Parte tipificar ciertas conductas como delitos en sus respectivos ordenamientos nacionales.[218] La importancia de la armonización en la tipificación de delitos se ha demostrado en innumerables casos, el denominado I love you virus[219], que causó múltiples y cuantiosos daños alrededor en sistemas y equipos alrededor del mundo. El código malicioso o malware fue creado y distribuido por un ciudadano filipino, quien fue identificado por las fuerzas y cuerpos de seguridad de Filipinas. No obstante, no pudo ser detenido ni procesado dichas autoridades por carecer Filipinas de una norma de Derecho Penal que tipificara la elaboración y distribución de código malicioso como delito. Por lo tanto, aunque la conducta de este individuo habría sido castigada en otros países donde el virus causó daños, sólo las fuerzas y cuerpos de seguridad de Filipinas tenían jurisdicción para detenerlo y procesarlo en el territorio, y ante la falta de un tipo penal, fueron incapaces de proceder. Tras el incidente se promulgó en Filipinas una ley que criminaliza la distribución de malware.

Si alguno de los Estados afectados por el virus hubiera solicitado la extradición de su autor, probablemente esta se hubiera denegado por Filipinas al no cumplirse el requisito de la doble criminalidad. Sin embargo, si el ciudadano filipino se hubiera

[218] A saber, el acceso ilegal a sistemas informáticos, la interceptación ilegal de comunicaciones electrónicas, la distribución de malware, las violaciones de derechos de autor, la producción o difusión de pornografía infantil, la difusión de material racista y xenófobo (discurso del odio).
http://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html

[219] http://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html

desplazado a uno de los territorios donde I Love You produjo daños, muy probablemente se habría producido un resultado similar al del caso *Ivanov.*[220] En la actualidad, la mayoría de los países han actualizado normas internas para tipificar ciertos delitos informáticos. Sin duda, La Convención de Budapest ha sido un instrumento político y jurídico de armonización valiosísimo. En la parte procesal, la Convención cuenta con una amplia provisión para la cooperación internacional en la lucha contra los delitos informáticos en sentido amplio, incluida la asistencia jurídica mutua en la investigación y conservación de pruebas.

En relación con las evidencias electrónicas, la convención contempla su recogida en el marco de cualquier delito, y no solo de relacionados con delitos informáticos propiamente dichos.[221]

6.1.1. Registro de sistemas fuera del territorio

En relación con los datos almacenados, la regla general establecida por la Convención es la de colaboración y asistencia mutua de los Estados Parte para procurar el acceso a los mismos por parte del Estado requirente. Cualquier Estado podrá solicitar a otro el registro o acceso de otro modo, el decomiso u obtención por

[220] Vid. Capítulo III.

[221] Vid. Art. 14.

otro medio, o la comunicación de datos almacenados en un sistema informático que se encuentre en su territorio (Art. 31).

6.1.2. Acceso remoto a sistemas fuera del territorio

La Convención de Budapest autoriza el Acceso Transfronterizo, que significa acceder de manera unilateral los datos informáticos almacenados en el territorio de otra Parte sin la utilización de procedimientos de asistencia judicial. En particular, el artículo 32 contempla el acceso remoto unilateral desde el territorio de un Estado Parte en dos circunstancias:

a) Cuando se trata de datos de libre acceso al público (fuentes abiertas), independientemente de la localización geográfica de esos datos;

b) Cuando se obtiene el consentimiento "legal y voluntario de la persona autorizada para divulgarlos" a través de un sistema informático.

La Convención de Budapest ha dado una solución parcial al problema jurisdiccional de Internet, legitimando el ejercicio extraterritorial de la jurisdicción cuando los datos están disponibles al público (en Internet) con independencia de que estos se encuentren almacenados en el territorio de otro Estado. Asimismo, ha autorizado expresamente la cesión de datos por parte de "la persona autorizada para

divulgarlos" a las autoridades competentes, de nuevo, con independencia del territorio de la autoridad requirente y del territorio de ubicación de los datos, siempre que ambos sean Estados Parte. Ahora bien, ¿Quién es "la persona autorizada" para divulgar los datos en un relación de Cloud Computing? ¿Qué se considera consentimiento legal?

En línea con los argumentos señalados en el Capítulo IV parece evidente que esta autoridad recae sobre el cliente de servicios de Cloud Computing. No obstante, también podría interpretarse que los proveedores de Cloud Computing ubicados en el territorio de los Estados Partes de la Convención están facultados a facilitar el acceso o entregar, datos a las autoridades de cumplimiento forzoso de la ley del Estado solicitante, siempre que éstas acceden a través de un sistema informático situado en el territorio del Estado Requirente. En este escenario no estaría claro a qué base legal se refiere el artículo 32 para determinar qué es un "consentimiento legal", pero podrían interpretarse que se refiere a la ley aplicable al proveedor en virtud de su establecimiento. Precisamente estas dudas suscitaron la necesidad de elaborar una guías de interpretación de este polémico Art. 32 por parte del Comité de la Convención contra la Ciberdelincuencia (T-CY), tal y como se verá en los siguientes apartados, dichas guías apuntaron que resulta "poco probable" que un proveedor pueda considerarse como sujeto legitimado para obtener un consentimiento legal.

6.1.3. Revisión de la Convención de Budapest

La clasificación de los ciberdelitos contenida en la Convención de Budapest es sin duda un modelo de referencia para la adopción de legislación sustantiva y procesal sobre el cibercrimen a nivel internacional. No obstante, hay quienes apuntan a la necesidad de actualizarla.[222]

Asimismo, el citado artículo 32 sobre el acceso a los datos situados en el territorio de otros países sin el consentimiento de esos otros países ha sido muy controvertido, para algunos resulta contrario al derecho internacional público, en particular a los principios de territorialidad y no intervención. Para otros, resulta insuficiente y sus provisiones deberían ampliarse.

En consecuencia, en el año 2011, T-CY acordó establecer un grupo transfronterizo *ad-hoc* (en adelante, grupo transfronterizo) sobre jurisdicción y acceso transfronterizo a datos. En 2012, el grupo transfronterizo presentó un informe completo, denominado "El Acceso Transfronterizo a los Datos y la Jurisdicción: ¿cuáles son las opciones?" [223] subrayando la necesidad de que exista un acceso

[222] Entre otros aspectos, para incluir nuevos tipos que han ido apareciendo. VELASCO, Cristos: "La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet. Tirant lo Blanch, Valencia Mayo 2012, p. 383.

[223] El Informe completo se puede consultar en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

transfronterizo por parte de las autoridades, pero notando también las preocupaciones y riesgos que éste puede suponer para las garantías procesales de los individuos afectados y la protección de datos de carácter personal, entre otros. El grupo consideró que estos riesgos debían ser abordados si los poderes de acceso transfronterizo contenidos en la Convención se incrementaran.

El informe propuso tres acciones concretas para abordar la cuestión, a saber: (i) El uso más eficaz de disposiciones sobre cooperación internacional que ya se establecen en la Convención (ii) La elaboración de una Nota de orientación sobre el contenido del artículo 32 de la Convención (ii) La creación de un protocolo adicional a la Convención que regule específicamente el acceso transfronterizo a las evidencias electrónicas.

En 2013, el grupo transfronterizo presentó un nuevo informe señalando que si bien la Convención es un tratado de Derecho Penal que abarca las investigaciones penales específicas dentro del ámbito del artículo 14, el contexto de las denuncias sobre vigilancia masiva por parte de las agencias nacionales de seguridad podría afectar negativamente la negociación de un protocolo adicional a la Convención. Además, apuntó que la reflexión y el diálogo con las autoridades de protección de datos, la sociedad civil y las organizaciones del sector privado, con miras conciliación de

acceso transfronterizo a los datos con las garantías y condiciones adecuadas para proteger los derechos de las personas y evitar el mal uso serían necesarios.

6.1.4. El Art. 32 de la Convención de Budapest

En el año 2014, el grupo transfronterizo finalmente publicó su Nota sobre la interpretación del Art. 32 b) de la Convención[224] estableciendo los siguientes criterios:

a) Los conceptos de "Acceso transfronterizo" y "Ubicación"

La Nota aclara que Acceso Transfronterizo significa "acceder de manera unilateral los datos informáticos almacenados en otra Parte sin buscar asistencia mutua"[225] y que la medida se puede aplicar entre las Partes. Asimismo, aclara que el Art. 32 b) se refiere a datos informáticos localizados en el territorio de otro Estado Parte y que si bien puede hacerse uso del mismo cuando se sabe dónde se encuentran los datos, éste no cubriría aquellas situaciones en que los datos *no* se almacenan en otra Parte, o en las que *es incierto* donde se encuentran los datos.

[224] CYBERCRIME CONVENTION COMMITTEE (T-CY): "Transborder access to data and jurisdiction: Options for further action by the T-CY", p. 5. Estrasburgo, 2014. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf

[225] Párrafo 293 del Informe explicativo de la Convención de Budapest.

El primer problema que se plantea con esta interpretación es que las autoridades normalmente no saben *a priori* donde se encuentran los datos. Los datos tratados en servicios de Cloud Computing pueden encontrarse fragmentados en distintas jurisdicciones, y copiados en otras adicionales. Asimismo, los datos pueden encontrarse en un formato ininteligible, por ejemplo, cifrados. Los datos pueden encontrarse en determinada jurisdicción y las llaves de cifrado correspondientes en otra distinta. Cuando los servicios de Cloud Computing ofrecen alguna opción de localización, la misma se realiza normalmente a nivel de regiones y no países. La Nota no aporta luces sobre estas realidades.

A la luz de lo anterior, la interpretación ofrecida por el grupo transfronterizo pareciera reducir significativamente en la práctica la aplicación del Art. 32 b) de la Convención en el ámbito del Cloud Computing, no obstante, resulta interesante que el documento continúa matizando que la Convención "no autoriza ni impide otras situaciones, por lo tanto, en situaciones donde se desconoce si, o no existe la certeza de que los datos estén almacenados en otra Parte, las Partes pueden tener que valorar la legitimidad de un registro u otro tipo de acceso a la luz de su derecho nacional, los principios de derecho internacional pertinentes o consideraciones de las relaciones internacionales" dejándonos prácticamente en el mismo punto de partida.

b) Requisitos del "acceso sin la autorización de otra Parte"

El Artículo 32 b) no requiere de la activación de los mecanismos de asistencia mutua, y la Convención de Budapest no requiere de la notificación a la otra Parte, aunque tampoco la prohíbe. Por tanto, la Parte que realiza el acceso podrá proceder a la notificación, si así lo estima oportuno.

c) La Noción de "consentimiento"

El consentimiento debe ser legal y voluntario, lo que significa que los datos no pueden obtenerse por fuerza o engaño. El grupo transfronterizo habla sobre el consentimiento de menores y particulares, sin embargo, no hace referencia al consentimiento prestado por personas jurídicas en el marco de relaciones contractuales B2B como las de Cloud Computing analizadas en la presente investigación.

d) Sobre la ley aplicable

En todos los casos, las autoridades policiales deben aplicar sus normas nacionales para realizar el acceso. Si el acceso o la divulgación no se permitirían internamente tampoco se permitirían bajo el Art. 32 b) de la Convención.

Esta orientación tiene implicaciones muy significativas, puesto que indica que las normas que deben regir el acceso son las normas del Estado que realiza el acceso en cuestión, sin que éste deba tener en consideración las normas del Estado o los Estados Parte donde la información se encuentra almacenada.

e) ***Sobre la persona que puede proporcionar acceso o divulgar datos***

La guía trae a colación dos ejemplos, reconociendo que el concepto de persona que está "legalmente autorizada" para realizar una cesión de datos puede variar a la luz de los distintos ordenamientos jurídicos aplicables:

a) En primer lugar, destaca que esta persona puede ser una persona física o jurídica que proporciona acceso sus los datos, por ejemplo, a su cuenta de correo electrónico u otra información que se encuentran almacenada en el extranjero.

b) En segundo lugar, hace referencia a los proveedores de servicios afirmando que es “poco probable” que estos tengan capacidad de dar su consentimiento válida y voluntariamente para ceder datos de usuarios a las autoridades al amparo del artículo 32 de la Convención. El documento resalta que, normalmente los proveedores de servicios sólo actúan como custodios de los

datos,[226] no controlan o son titulares de los mismos, por tanto, no están en condiciones de otorgar un consentimiento válido.

La Nota también aclara que las autoridades pueden adquirir datos transnacionalmente utilizando otros métodos, tales como los mecanismos de asistencia judicial o los procedimientos para situaciones de emergencia judicial recíproca.

Por último, en relación con la posibilidad de elaborar protocolo adicional a la Convención para desarrollar específicamente el acceso transfronterizo a datos, el documento establece que aunque dicho protocolo es necesario, "las condiciones de consenso requeridas para llegar a un acuerdo no están dadas". Muy probablemente esta afirmación se refiere al clima político y las tensiones existentes a ambos lados del atlántico en materia de acceso gubernamental a información. Si más, el documento refleja la creación de un nuevo grupo de trabajo por un período de los dos años. Hasta la fecha, el grupo no ha publicado su propuesta en este sentido.

[226] En el ámbito de protección de datos, ocupan la figura del encargado del tratamiento. Sobre esta distinción de roles, véase el Capítulo IV.

6.2. Comisiones Rogatorias

Las comisiones rogatorias son instrumentos a través de los cuales la autoridad judicial de un Estado (Estado requirente) solicita de la autoridad competente de otro Estado (Estado requerido) la ejecución, dentro del territorio de su jurisdicción, de un acto de instrucción o de otros actos judiciales, especialmente la práctica de una diligencia probatoria.[227] Este mecanismo se utiliza por los tribunales para solicitar formalmente información, asistencia y cooperación en un procedimiento judicial cuando las partes involucradas están ubicadas en distintas jurisdicciones.

Cuando no existe un tratado de asistencia judicial entre dos Estados, la asistencia internacional está gobernada por las normas domésticas respectivas en materia de asistencia mutua. En este sentido, el Derecho interno de los países suele incluir las comisiones rogatorias como una de las figuras que habilitan la colaboración. Asimismo, las comisiones rogatorias son el método consuetudinario internacional por excelencia para obtener asistencia y evidencias de otros Estados en ausencia de un tratado.[228]

[227] AGUILAR, Mariano: "Comisiones rogatorias y obtención de pruebas en el extranjero" Boletín del Ministerio de Justicia, ISSN-e 0211-4267, Año 55, Nº 1905. Madrid, 2001, p. 3635.

[228] ITU: "Global Cybersecurity Agenda". Ginebra, 2008, p. 54. Disponible en: https://ccdcoe.org/sites/default/files/documents/ITU-080801-HLEGreport.pdf

No obstante, se trata de un mecanismo voluntarios que no obligan a la parte requerida a su ejecución y cumplimiento. Las comisiones rogatorias usualmente se transmiten mediante canales diplomáticos, un proceso que carece de celeridad.[229] Asimismo, se considera generalmente que los cuerpos diplomáticos son libres de no actuar ante una comisión rogatoria, si a su parecer la asistencia que persigue no fuera consistente con las políticas públicas del Estado requerido.

Cuando la comisión rogatoria es aceptada por el Estado requerido, esta se traslada a un juez nacional para que ordene su ejecución. Por su parte, el juez no está obligado a ejecutar lo solicitado, y en caso de haber ejecución, la misma se debe realizar de conformidad con el Derecho Interno del Estado requerido. Esto puede añadir otro nivel de inseguridad al proceso, debido a que la ley del Estado requerido puede ser muy diferente a la ley del Estado requirente (en asuntos tales como la autenticación de la evidencia, los mecanismo de recogida y preservación, etc.), lo cual puede poner en riesgo la utilización de la misma en el marco de un proceso judicial. Tras este proceso y una vez que el requerimiento se ha ejecutado, (o negado su ejecución) los resultados se devuelven al juez solicitante, de nuevo normalmente a través de los canales diplomáticos.[230]

[229] ITU: "Global Cybersecurity Agenda". Ginebra, 2008, p. 191. Disponible en: https://ccdcoe.org/sites/default/files/documents/ITU-080801-HLEGreport.pdf

[230] VELASCO, Cristos Op. Cit, p. 287.

6.3. Investigaciones Conjuntas

Los Equipos Conjuntos de Investigación son un instrumento cooperación internacional que consiste en la formación de grupos internacionales operativos de investigadores, constituidos por acuerdo de las autoridades competentes de dos o más Estados para llevar a cabo coordinadamente investigaciones penales en el territorio de todos o alguno de ellos en relación con unos hechos delictivos determinados y por un periodo de tiempo limitado.[231]

En el ámbito de Naciones Unidas, el art. 19 del Convenio contra la Delincuencia Organizada Transnacional de 2000 prevé las investigaciones conjuntas a través de acuerdos bilaterales o multilaterales entre los países que lo suscriban o de acuerdos específicos casos concreto. Asimismo, el Convenio de la Naciones Unidas contra la Corrupción de octubre de 2003 recoge las investigaciones conjuntas como métodos de investigación de estos delitos acuerdos.

Tanto el Tratado de Asistencia Judicial en materia penal entre la UE y los EE.UU. como el Tratado de Asistencia Judicial en materia penal entre España y los EE.UU. contemplan esta técnica de investigación.

[231] Informe del Consejo Fiscal en relación con la problemática relativa a los Equipos Conjuntos de Investigación, Madrid 2014. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/23_09_2014_Informe_CF_sobre_Equipos_Conjuntos_de_Investigacion.pdf?idFile=a3b90dca-8134-4343-ad3a-316573c83e3f

6.4. Peticiones de Emergencia

Típicamente los distintos ordenamientos jurídicos permiten a proveedores de servicios la cesión voluntaria de información de los usuarios a las autoridades, cuando se cree que ello es necesario para evitar la muerte o daño físico serio de una persona.[232] La ley normalmente permite hacer estas excepciones al deber de confidencialidad, en casos como secuestros o amenazas terroristas inminentes. Las peticiones de emergencia deben contener una descripción de la situación de emergencia y una explicación de cómo la información solicitada podría prevenir el daño. La información proporcionada en respuesta a la solicitud se debe limitar a lo se cree que ayudaría a prevenir el daño en cuestión.

6.5. Tratados de Asistencia Mutua (MLATs)[233]

Los MLATs son tratados que se suscriben entre los Estados con la finalidad de proveerse mutuamente asistencia en la obtención de evidencias relacionan con la investigación y/o persecución criminal. Un MLAT establece una obligación inequívoca para los Estados Parte, de proveer formas específicas de asistencia en conexión con investigaciones criminales. Por ejemplo, un MLAT da derecho al Estado requirente a recibir asistencia en la adquisición de registros bancarios y otra información financiera; la realización de inspecciones e incautaciones, entre otros. Cada Estado

[232] Por ejemplo, en España la LOPD.

[233] Del inglés Mutual Legal Assistance Treaty.

debe designar a una autoridad central competente responsable de la transmisión y ejecución de solicitudes de asistencia judicial mutua (por lo general, un Ministerio de Justicia o la Oficina del Fiscal General). Un MLAT también puede permitir cualquier otra forma de asistencia no prohibida por la legislación del Estado requerido. Motivos habituales que permiten la denegación asistencia tienen que ver con delito políticos, o delitos militares no reconocidos por el derecho penal ordinario, o cuando la solicitud violaría la constitución o el ordenamiento jurídico del Estado requerido, la seguridad nacional o el orden público. La mayoría de MLATs hoy día afirman que la doble incriminación no puede servir de base para denegar la asistencia.

Las propuestas para procurar la celeridad en los procesos de asistencia judicial, incluidos los MLATS sugieren la creación de órdenes internacionales (i) que puedan ser servidas a las autoridades de otros Estados directamente i.e prescindiendo de los canales diplomáticos (ii) que puedan ser servidas al proveedor que tiene los datos en otro país signatario de la convención.[234]

[234] En este sentido véase::
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/3021_art15Conf_Conclusions_v1e.pdf

7. CAPÍTULO VI: REGLAS DEL ACCESO GUBERNAMENTAL EN LA NUBE: ESPAÑA, EE.UU Y REINO UNIDO

En esta sección se examinan los regímenes que regulan el acceso gubernamental a la información en materia criminal aplicables en España, EE.UU y el Reino Unido Reino, así como las principales reglas de cooperación internacional en vigor entre dichos Estados.

En el año 2012, Hogan Lovells publicó un White Paper en el que se hacía una comparación de los distintos regímenes jurídicos en 10 de las economías más importantes, incluidos España, EE.UU y el Reino Unido. En dicho documento se señaló que "basándose en la experiencia práctica y anecdótica, parece que las empresas a menudo asumen el conocimiento de las leyes regulan el acceso gubernamental a los datos en sus propias jurisdicciones, y hacen otras hipótesis sobre el regímenes jurídicos en el extranjero, donde los proveedores de servicios de nube pueden estar ubicados. Por ejemplo, especialmente en Europa, Patriot Act se ha invocado como una especie de taquigrafía para expresar la creencia de que los Estados Unidos gobierno tiene mayores poderes de acceso a los datos personales en la nube que los gobiernos de otros lugares".[235]

[235] MAXWELL, Winston. WOLF, Christopher: "A Global Reality: Governmental Access to Data in the Cloud". A Hogan Lovells White Paper. París, Washington, 2012,p.1. Disponible en: http://www.hoganlovells.com/files/Publication/80a807f2-e619-41dc-98e4-e6a7b5f6c5f8/Presentation/PublicationAttachment/9bab0ead-0b8b-4cdb-bb08-8ba1b95a9df9/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf

Por tanto, parece importante realizar un análisis del régimen jurídico de los EE.UU al que está sujetos varios de los proveedores más relevantes en la actualidad, y compararlo con regímenes europeos como el de España y el Reino Unido, donde también existen jugadores importantes en la provisión de servicios de Cloud Computing, y donde además hay un nivel de adopción creciente de estos servicios por parte de organizaciones, e instituciones públicas y privadas.

En el Capítulo III se analizaron los principios y las reglas que rigen la jurisdicción en la nube. Una vez que un Estado afirma jurisdicción, buscará ejercerla. Se estudiarán las reglas que rigen el ejercicio de esta jurisdicción en los tres países mencionados con relación al acceso a datos en la nube, señalando cómo el Estado que investiga o que persigue un delito podrá solicitar información a un proveedor servicios de Cloud Computing sobre sus usuarios.

Las normas de Derecho Procesal resultan esenciales pues no solamente representan el fundamento para fijar los límites de la competencia de los tribunales para conocer sobre una determinada petición o causa, sino que también establecen derechos y garantías de los individuos en el marco del debido proceso.

7.1. Estados Unidos

7.1.1. Marco Legal

En los Estados Unidos, las potestades que las autoridades gubernamentales pueden utilizar para obligar a los proveedores de servicios de Cloud Computing a ceder información sobre sus usuarios, así como los límites de dichas potestades se encuentran en dos fuentes principales, a saber, la Cuarta Enmienda de la Constitución y La Ley de Privacidad de las Comunicaciones Electrónicas (en adelante, ECPA).[236]

La Cuarta Enmienda de la Constitución federal establece que "No se violará el derecho del pueblo a la seguridad en sus personas, hogares, documentos y pertenencias, no se harán allanamientos e incautaciones fuera de lo razonable, y no se emitirá ningún mandamiento judicial al efecto, si no es en virtud de causa probable, respaldada por Juramento o promesa, y con la descripción en detalle del lugar que habrá de ser allanado y de las personas o efectos que serán objeto de detención o incautación".[237]

[236] Electronic Communications Privacy Act.

[237] El texto de la enmienda se puede consultar en: http://iipdigital.usembassy.gov/st/spanish/publication/2008/09/20080915145501pii0.1888391.html#axzz3XkbAISlc

El objetivo de esta disposición es proteger el derecho de las personas a la privacidad y la libertad de las intrusiones gubernamentales arbitrarias.[238] Por su parte, ECPA[239] es la principal ley federal que regula el acceso gubernamental a las comunicaciones electrónicas. La norma fue promulgada en 1986 para proporcionar protecciones adicionales a Cuarta Enmienda de la Constitución, así como para llenar algunos de los vacíos dejados por la Cuarta Enmienda a raíz de decisiones judiciales que tenían difícil encaje en las nuevas tecnologías,[240] en particular, para para extender las restricciones del gobierno sobre escuchas telefónicas a las comunicaciones electrónicas.

ECPA consta de tres partes:[241]

1. La primera parte (codificada en 18 U.S. Code § 2510 y ss.) se refiere a las comunicaciones electrónicas en tránsito, declarando ilegal su interceptación no autorizada. Por regla general, se requiere de autorización judicial para

[238] Legal Information Institute, Cornell University: "Fourth Amendment".Disponible en: https://www.law.cornell.edu/wex/fourth_amendment

[239] Disponible en: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

[240] Véase SOLOVE, Daniel: "Surveillance Law in Dire Need of Reform: The Promise of the LEADS Act", blogpost. Disponible en: https://www.linkedin.com/pulse/surveillance-law-dire-need-reform-promise-leads-act-daniel-solove

[241] DOYLE, Charles: "Privacy: An Overview of the Electronic Communications Privacy Act" Congressional Research Service, Octubre 2012. Disponible en: https://www.fas.org/sgp/crs/misc/R41733.pdf

permitir tales interceptaciones con fines de justicia criminal y de seguridad nacional.

2. La segunda parte (codificada en U.S. Code 18 § 2701 y ss.) se centra en la protección de las comunicaciones electrónicas almacenadas, y en cómo las autoridades pueden tener acceso a dichas comunicaciones electrónicas. En general, los ISPs tienen prohibido divulgar **voluntariamente** a cualquier persona o entidad el contenido de cualquier comunicación que se lleva o se mantiene en ese servicio. Sin embargo, a los proveedores se les permite (más no están obligados) a revelar contenidos a una entidad gubernamental, si el proveedor en cuestión, de buena fe, considera que una emergencia relacionada con peligro de muerte o lesiones físicas graves a una persona requiere la revelación sin demora de las comunicaciones relativas a la situación de emergencia, entre otras.[242] También se les permite revelar datos que no sean de contenido, tales como los datos de registro y el nombre y dirección de correo electrónico del destinatario en respuesta a un requerimiento informal (§ 2702). Por regla general, se requiere de mandamiento judicial para requerir a un proveedor revelar comunicaciones

[242]18 U.S. Code § 2702 - Voluntary disclosure of customer communications or records. Disponible en: https://www.law.cornell.edu/uscode/text/18/2702

almacenadas con fines de justicia criminal y de seguridad nacional.[243] Por su parte, los datos de suscripción pueden obtenerse mediante orden administrativa.

3. La tercera parte (codificada en U.S.Code 18 § 3121 y ss.) crea un procedimiento para la instalación y uso de registros de llamadas para recabar datos de tráfico de las comunicaciones, asimismo regula los dispositivos de "trampa y traza"[244] prohibiendo su instalación o uso, excepto con fines policiales e investigaciones de inteligencia en el extranjero.

7.1.2. Mecanismos jurídicos para la obtención de datos en la nube[245]

a) Citación ECPA: La citación o *subpoena* contempla el umbral más bajo o la forma menos rigurosa para la obtención de ciertos datos por parte de una autoridad gubernamental en los EE.UU. A través de una citación[246] las autoridades pueden obligar a un proveedor de servicios de Cloud a la cesión

[243] En relación con los email, el mandamiento judicial siempre se requiere. Véase la decisión en el caso *U.S. v. Warshak* https://www.eff.org/files/warshak_opinion_121410.pdf

[244] En este sentido, véase:
https://www.eff.org/files/filenode/spanish-lessonsfromtheunitedstates_0.pdf

[245] Google Transparency Report. Disponible en:
https://www.google.com/transparencyreport/userdatarequests/legalprocess/

[246] Las citaciones pueden ser utilizados por el gobierno en ambos casos penales y civiles.

de datos identificativos como el nombre suministrado al crear una cuenta vinculada a servicios de Cloud Computing, las direcciones IP desde las que se haya creado dicha cuenta, e iniciado y cerrado la sesión, respectivamente, así como sus fechas y horas. Bajo el sistema federal de los Estados Unidos no se requiere la supervisión judicial de estas citaciones.

- **Orden Judicial ECPA:** Por virtud de una orden judicial ECPA, las autoridades pueden obtener información más detallada sobre el uso de una cuenta vinculada a servicios de Cloud Computing. Esta información podría incluir la dirección IP asociada a un correo electrónico enviado, y/o la utilizada se para cambiar la contraseña, con sus respectivas fechas y horas, así mismo, las partes que no conforman en contenido de mensajes de correo electrónico, tales como "de", "para" y "fecha". Las órdenes judiciales ECPA sólo están disponibles para las investigaciones penales. A diferencia de la citación ECPA, la obtención de una orden judicial ECPA implica la revisión por parte de un tribunal. Para recibir una orden judicial ECPA, una la autoridad competente debe presentar hechos **específicos** que demuestren que la información solicitada es **pertinente** y material a una investigación penal en curso.[247]

[247] 18 U.S. Code § 2703 - Required disclosure of customer communications or records. Disponible en: https://www.law.cornell.edu/uscode/text/18/2703

b) **Orden de registro ECPA:** Para obtener una orden de registro ECPA se deben cumplir requisitos adicionales a los de la Orden Judicial ECPA, en particular, la autoridad solicitante debe demostrar que existe la "**causa probable**" que exige la Cuarta Enmienda de la Constitución que lleva a creer que cierta información relacionada con un crimen se encuentra actualmente en el lugar específico en el que se solicita buscar. La orden de registro debe especificar el lugar en el que se debe buscar y lo que se busca en concreto; ésta puede utilizarse para obligar a un proveedor de servicios de Cloud a la divulgación de contenido almacenado en una cuenta (mensajes de correo electrónico, o documentos). Una orden de registro ECPA está únicamente disponible en el ámbito de investigaciones penales. Se discutía si un correo electrónico sin abrir que había estado almacenado durante 180 días o menos, requería de la obtención de una orden de registro, en el marco del caso *U.S. v. Warshak* se estableció *que* el correo electrónico está protegido por la cuarta enmienda de la Constitución y por tanto, la orden de registro se requiere con independencia de la antiguedad de la comunicación.[248] Con relación a otros documentos, bastaría una orden judicial ECPA donde consten "hechos específicos y articulables" combinada con la previa notificación al usuario afectado (§ U.S.C 2702). La notificación se puede retrasar hasta 90 días cuando la misma pueda obstaculizar la instrucción.

[248] https://www.eff.org/files/warshak_opinion_121410.pdf

c) **Orden judicial de registro de comunicaciones entrantes y salientes**[249] En el ámbito de la aplicación forzosa de la ley, una orden judicial de registro de comunicaciones entrantes y salientes obliga a prestadores de servicios a entregar información sobre las comunicaciones de un usuario (sin incluir el contenido de comunicaciones a sí mismos) en tiempo real. Con esa orden, las autoridades pueden obtener datos de tráfico es decir, "marcación, enrutamiento, direccionamiento y la información de señalización." Esto podría incluir las llamadas salientes de un usuario o una dirección IP asignada a un usuario[250].

d) **Orden judicial de intervención de las comunicaciones:** Mediante este mecanismo, en el ámbito de la aplicación forzosa de la ley, las autoridades competentes pueden obtener una orden judicial para la intervención de comunicaciones en tiempo real, éste tipo de órdenes judiciales buscan recopilar información que aún no existe. Para obtener una orden judicial de intervención de las comunicaciones, la autoridad solicitante debe demostrar

[249] ASCENSIO, Hervé: "Extraterritoriality as an instrument". Contribution to the work of the UN Secretary-General's Special Representative on human rights and transnational corporations and other businesses. Diciembre 2010. Disponible en: http://www.univ-paris1.fr/fileadmin/IREDIES/Contributions_en_ligne/H._ASCENSIO/Extraterritoriality__Human_Rights_and_Business_Entreprises.pdf

[250] 18 U.S. Code § 3123 - Issuance of an order for a pen register or a trap and trace device. Disponible en: https://www.law.cornell.edu/uscode/text/18/3123

que: a) alguien está cometiendo un delito de los que figuran en la Wiretap Act,[251] b) la intervención está encaminada a recopilar información sobre ese crimen, y c) el delito implica la cuenta que será intervenida. También se debe demostrar que las maneras ordinarias para investigar el hecho punible han fracasado (o que probablemente fracasaría) o que sería demasiado peligroso intentarlas en primer lugar. Existen límites en la duración de una intervención telefónica, y en la notificación de los usuarios que han sido intervenidas.[252]En el ámbito de la seguridad nacional, en lo relativo a actividades de espionaje o el terrorismo internacional contra los EE.UU, algunas autoridades la interceptación por vía administrativa, con arreglo a las reglas que se indican en las siguientes líneas[253].

ECPA ha sido modificada por varias normas, entre las que destacan:

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) de 2001. USA Patriot Act fue una modificación de las leyes pre-existentes utilizadas por las agencias

[251] Sabotaje de instalaciones nucleares, armas biológicas, espionaje, secuestro, violación de secretos industriales, entre otros delitos considerados graves por el ordenamiento jurídico. El texto puede ser consultado en: https://www.law.cornell.edu/uscode/text/18/2516

[252] 18 U.S. Code § 2518 - Procedure for interception of wire, oral, or electronic communications.

[253] Véase Foreign Intelligence Surveillance Act (FISA) de 1978, modificada en 2008.

del gobierno de los EE.UU.s en materia de seguridad nacional para fortalecer la lucha contra el terrorismo.[254] Patriot Act expiró en Junio de 2015.

Esta norma fue objeto de atención tras las revelaciones de Snowden en el año 2013. Para algunos, las preocupaciones sobre el alcance potencial de las autoridades competentes de Estados Unidos, en particular en el marco de Patriot Act, reflejaba cierta ignorancia generalizada acerca de los poderes que ya estaban disponibles para las agencias locales en muchas, si no la mayoría de las jurisdicciones.[255]

- Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act (USA Freedom Act) de 2015. Es la norma sustitutiva de Patriot Act. La norma está encaminada a garantizar que la vigilancia electrónica está acotada, es transparente y está sujeta a control judicial. La ley que restauró, en distinta forma, varias disposiciones de su antecesora, imponiendo algunos límites adicionales sobre a la recolección de datos de tráfico de las telecomunicaciones por las agencias de inteligencia de Estados Unido, tanto en el ámbito de la aplicación forzosa de la ley, como en

[254] Covington & Burling: "The USA PATRIOT Act and the Use of Cloud Services: Q&A. http://www.insideprivacy.com/PatriotActQA.pdf

[255] WALDEN, Ian: "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent". Queen Mary School of Law Legal Studies Research Paper No. 74/2011. November 14, 2011, p.2. Disponible en SSRN: http://ssrn.com/abstract=1781067

los ámbitos de la seguridad nacional e inteligencia. Se ha destacado que su aprobación constituye un hito, al ser la primera vez en más de treinta años que las dos cámaras del Congreso acuerdan el establecimiento de restricciones reales y supervisión sobre los poderes de vigilancia de la Agencia de Seguridad Nacional.[256]

- Foreign Intelligence Surveillance Act (FISA) de 1978, modificada en 2008[257]

FISA prescribe procedimientos para solicitar autorización judicial para la vigilancia electrónica y la búsqueda física de las personas que participan en actividades de espionaje o el terrorismo internacional contra los EE.UU. en nombre de una potencia extranjera. [258]

Esta norma sigue siendo un foco de atención tras las revelaciones de Snowden, pues establece poderes más amplios de investigación con relación a objetivos de inteligencia fuera de los EE.UU. En particular, la Sección 702 de la norma faculta al Fiscal General y el Director de Inteligencia Nacional para autorizar de manera conjunta, por un período de hasta 1 año la investigación de personas que creen

[256] COHN, Cindy. REITMAN, Rainey: "USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here" EFF, 2015. https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here

[257] Texto disponible en: https://www.govtrack.us/congress/bills/110/hr6304/text

[258] http://fas.org/irp/agency/doj/fisa/

razonablemente se encuentran fuera de los Estados Unidos para adquirir información de inteligencia extranjera, dicha adquisición de inteligencia deberá llevarse a cabo de una manera consistente con la Cuarta Enmienda de la Constitución de los EE.UU, así como someterse al control judicial de la Corte FISA.[259] Por el contrario, las Secciones 703 y 704 requieren de una orden judicial para adquirir esta información personas estadounidenses que creen razonablemente se encuentra fuera de los Estados Unidos.[260] La gran debilidad que tiene esta norma, es que se enfoca en las protecciones a los estadounidenses, dejando en situación de desventaja a los extranjeros.

7.1.3. Secreto de las actuaciones

18 U.S. Code § 2703 contempla los poderes de investigación de las autoridades competentes sobre comunicaciones electrónicas con arreglo a los cuales se puede solicitar a proveedores de Cloud información sobre sus usuarios. La habilidad para notificar estas solicitudes, de forma que el usuario o cliente pueda ejercer las acciones oportunas, es la regla. No obstante, 18 U.S. Code § 2705 establece la posibilidad de retrasar esta notificación cuando se pueda perjudicar la investigación, por ejemplo, cuando se pueda poner en peligro la vida o la integridad física de una

[259] Sección 207, codificada bajo (50 U.S. Code § 1881a y ss). Disponible en: https://www.law.cornell.edu/uscode/text/50/1881a
[260] https://www.lawfareblog.com/update-fisa-amendments-act-reauthorization

persona, escapar del enjuiciamiento, la destrucción o manipulación de pruebas, la intimidación de testigos potenciales, o retrasar indebidamente un juicio.

Asimismo, 18 U.S. Code § 2709 establece la prohibición, a través de las llamadas NSL (National Security Letters) de la divulgación de investigaciones relacionadas con actividades de **terrorismo** y **contraespionaje** en ciertas circunstancias. En estos casos, la notificación por parte de proveedores que resulten requeridos estaría prohibida. Tras un litigio por parte de varios actores de la industria (LinkedIn, Facebook, Yahoo, Google, Microsoft entre otros) acordó por parte del Gobierno permitir a los proveedores la publicación de estadísticas sobre las llamadas NSL que reciben en agregado, esta información suele encontrarse disponible en los respectivos informes de transparencia de las los proveedores.[261]

7.1.4. Registros transfronterizos

En los EE.UU. se ha reconocido jurisprudencialmente la admisibilidad de registros realizados en los EE.UU. aun cuando los datos estuvieran almacenados en equipos situados en un país extranjero, así como su validez probatoria en el posterior proceso judicial en territorio de los EE.UU.[262]

[261] http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf

[262] El caso más emblemático ha sido *United States v. Ivanov.* Véase p.88 y ss.

7.1.5. Recurso Judicial

La reparación judicial con respecto a posibles intrusiones indebidas por parte de las autoridades de EE.UU. está disponible para los ciudadanos de los EE.UU. al amparo de la Ley de Privacidad de 1974, no obstante, los ciudadanos extranjeros no cuentan con legitimación activa para acudir a esta vía con el objeto de obtener tutela. En este sentido, Judicial Redress Act es un proyecto de ley autoriza al Departamento de Justicia (DOJ) de los EE.UU. para designar a los países extranjeros u organizaciones regionales de integración económica, a los efectos de que sus ciudadanos puedan obtener tutela judicial invocando la Ley de Privacidad de 1974 de los EE.UU. contra autoridades del gobierno de EE.UU. con el propósito de acceder, modificar o corregir registros obtenidos indebidamente por una agencia gubernamental. Asimismo, autoriza al Departamento de Justicia (DOJ) con la concurrencia del Departamento de Estado, el Departamento del Tesoro y el Departamento de Seguridad Nacional, para designar a los países u organizaciones cuyos ciudadanos pueden acudir a dichos recursos civiles y obtener reparación, cuando el país o la organización tenga protecciones de privacidad adecuadas para el intercambio de información con los EE.UU. en el marco de la prevención, investigación, detección o persecución de delitos.[263] La Ley de Reparación Judicial extendería ciertos derechos a los ciudadanos de los aliados designados, en particular, a los Estados miembros de la Unión Europea

[263] El texto de la norma se encuentra disponible en:
https://www.congress.gov/bill/114th-congress/house-bill/1428

a los efectos de que estos puedan hacer uso de los beneficios fundamentales que los estadounidenses disfrutan en virtud de la Ley de Privacidad de los EE.UU. con respecto a la información tratada por los Estados Unidos con fines de aplicación forzosa de la ley.[264]

7.1.6. Interoperabilidad práctica del régimen de EEUU con España

a) Asistencia judicial internacional como regla

Tal y como señala VELASCO, muchos proveedores de servicios de Cloud Computing están establecidos en los EE.UU. y los datos que tratan se encuentran ubicados fuera del territorio español, para cuya consecución es prácticamente obligatorio solicitarlos mediante mecanismos de asistencia judicial, cuestión que muchas veces e incluso inutiliza la investigación.[265] Tanto los contenidos almacenados, como los datos de tráfico y de alta del servicio se rigen por la normativa de los EE.UU. para su intervención o cesión, la cual se encuentra recogida en la ECPA. Sobre las

[264] En este sentido, véase la carta dirigida por varios actores de la industria a la Cámara de Representantes, disponible en: http://www.ccianet.org/wp-content/uploads/2015/04/Joint-Letter-re-Judicial-Redress-Act-042815.pdf

[265] VELASCO NUÑEZ, Eloy: "Delitos cometidos a través de internet. Cuestiones procesales". La Ley. Madrid, 2010, p.99.

peculiaridades y retos de ECPA con relación a las investigaciones realizadas en España, VELASCO[266] señala, entre otros.

a) Solicitud directa de información a los proveedores:

"En algunos casos, que suelen coincidir con la radicación de sucursales en España (por el ejemplo en el caso de Microsoft, con su correo electrónico hotmail) las empresas proveedoras, siempre que haya mandamiento judicial español, remiten al juzgado los datos de conexión y los datos del usuario de correo electrónico y contractuales asociados que se les solicita, sin necesidad de emitir comisión rogatoria. No ocurre lo mismo respecto de la intervención del contenido del mensaje, que suele exigir la emisión de comisión rogatoria".

b) Cesión de datos de tráfico

"Para la cesión de datos de tráfico (direcciones IP, emisor, receptor) hay que tener en cuenta que las empresas proveedoras de servicio sólo tienen la obligación de conservarlos por un período que oscila entre los 20 y los 60 días.[267] La "orden de

[266] VELASCO NUÑEZ, Eloy: "Delitos cometidos a través de internet. Cuestiones procesales". La Ley. Madrid, 2010, p.100 y ss.

[267] En España, la Ley 25/2007 obliga a la retención de datos por el período de un año. Esta norma constituye la transposición al ordenamiento jurídico español de la Directiva 2006/24/CE. Esta Directiva fue declarada inválida por el Tribunal de Justicia de la Unión Europea en abril de 2014 (Sentencia en los asuntos acumulados C-293/12 y C-594/12 Digital Rights Ireland y Seitlinger y otros)

preservación" si es aceptada, produce el efecto de que los datos a*d hoc* requeridos se conserven por 90 días más, que pueden prolongarse por otros 80 días adicionales en caso de que lo investigado tenga consideración de hechos graves (crimen organizado, terrorismo). Por el contrario, los hechos leves y medios, entre los que la legislación norteamericana comprende las expresiones vejatorias a través de Internet por obra de su concepción amplia del derecho a la libertad de expresión contemplado en la Primera Enmienda a su Constitución, suelen dar lugar a la no concesión de lo solicitado".[268]

c) Intervención de las comunicaciones

"EEUU. no contempla, en principio, la intervención de un correo electrónico autorizado por la legislación de país extranjero, si con ella se trata de investigar hechos delictivos ocurridos en otro país, a menos que a la vez abra una investigación paralela por lo mismo en su país *(refiriéndose a las investigaciones conjuntas*). Cuando deciden no abrirla, la cooperación judicial penal estadounidense consiste en la aportación del barrido histórico de los mensajes enviados/recibidos en un determinado período de tiempo, sin que se pueda conocer su contenido. En caso positivo, la justicia norteamericana exige comisión rogatoria y mandamiento judicial

no obstante, la Decisión no tiene efectos directos en la Ley española. Se discute que la norma se aplique a servicios de Cloud Computing.

[268] VELASCO NUÑEZ, Eloy: "Delitos cometidos a través de internet. Cuestiones procesales". La Ley. Madrid, 2010, p.100.

(warrant), para cuya consecución los datos consignados en la comisión rogatoria deben ser exhaustivos por parte del juez requirente, ya que los debe trasladar el fiscal americano, para superar el umbral del llamado "probable cause" o juicio suficiente de probabilidad , para que el que se necesita informar suficientemente de los indicios delictivos detectados, su relación probatoria probable con el correo a intervenir y la copia de los preceptos del Código Penal español infringidos, que llevarán o no al juez estadounidense a emitir la orden permitiendo o no la intervención de la cuenta de correo electrónico que, como se ha apuntado, además, deberá haber propiciado una investigación paralela en su territorio".

Esto significa que los países tienen que pasar por el proceso legal MLAT y Estados Unidos. Esto crea una gran carga de trabajo para el Departamento de Justicia (DOJ) el FBI y las compañías estadounidenses, y genera retrasos y frustraciones cuando se trata de la aplicación de la ley extranjera. Son preocupaciones como estas las que fomentan los movimientos de los Estados hacia la localización de datos y la fragmentación de Internet.[269]

[269] VELASCO NUÑEZ, Eloy: "Delitos cometidos a través de internet. Cuestiones procesales". La Ley 2010, Madrid, 2010, p.101 y ss.

7.2. España

7.2.1. Marco legal

En España, las potestades que las autoridades gubernamentales pueden utilizar para obligar a los proveedores de servicios de Cloud Computing a ceder información sobre sus usuarios, así como los límites a dichas potestades se encuentran en las siguientes normas:

- La Constitución Española, Art. 18.3.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en adelante LSSI.
- Ley de Enjuiciamiento Criminal,[270] en adelante LECrim.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, en adelante, la Ley de Conservación de Datos.
- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

El secreto de las comunicaciones es un derecho fundamental consagrado en el artículo 18.3 de la Constitución, conforme al que se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo

[270] Su última revisión entrará en vigor el 28 de Octubre de 2015.

resolución judicial. La doctrina jurisprudencial ha ido delineando el contenido de este derecho de la siguiente manera:

- Desde la perspectiva subjetiva, los titulares pueden ser tanto las personas físicas como las jurídicas, nacionales o extranjeras.[271]

- La protección constitucional abarca todos los medios de comunicación, con independencia de los diferentes sistemas técnicos que puedan emplearse.[272]

- El secreto de la comunicaciones del artículo 18.3 no sólo cubre su contenido, sino que alcanza a los datos de tráfico, esto es la identidad subjetiva de los interlocutores, la propia existencia de la comunicación: su momento, origen, destino duración, así como los referentes al volumen de la información transmitida y el tipo de comunicación entablada.[273]

- Toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas precisa necesariamente de una habilitación legal.[274]

[271] STS 246/1995, de 20 de febrero.

[272] STS 1377/1999, de 8 de febrero.

[273] STS 688/2009, de 18 de junio.

[274] STC 184/2003, de 23 de octubre.

Por su parte, la Carta Europea de Derechos Humanos (CEDH) en su artículo 8.2 señala expresamente los objetivos o fines que pueden perseguir las medida que constituyan una injerencia en el derecho al secreto de las comunicaciones para considerarse admisible son: la seguridad nacional, la seguridad pública y el bienestar económico. En España, los delitos susceptibles de investigación a través de la interceptación de comunicaciones se determinan a través de un sistema abierto en el que la ponderación se realiza en función del tipo de delito, la relevancia jurídico penal, el bien jurídico protegido y la trascendencia social del mismo.[275]

No existe en España una norma específica que regule el acceso a las comunicaciones electrónicas, por lo que las reglas aplicables deben analizarse, además a la luz de (además de la Constitución) la LECrim, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en menor medida la LSSI y la Ley de Conservación de datos.

1. En el ámbito de la aplicación forzosa de la ley, de conformidad con la LECrim la interceptación de las **comunicaciones en tránsito** requiere, por lo general, de un mandamiento judicial que podrá ser concedido a las autoridades competentes cuando hubiere indicios "de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante

[275] SSTC 104/2006 de 3 de abril.

de la causa"[276] los cuales deben basarse en pruebas suficientes de que la comunicación interceptada sería material a un investigación criminal; se debe acreditar un fin legítimo y proporcionalidad, sin llegar a exigir indicios racionales.[277] La LECrim exige que concurran indicios de criminalidad. No se exige la aportación de un cuadro probatorio acabado, pero sí que se pongan a disposición del juez aquellos elementos de juicio en virtud de los cuales la policía ha podido llegar, de forma no arbitraria, a la conclusión de la necesidad de implantar la medida. Los indicios que se exigen son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento.[278]

No obstante, en ciertos casos, las autoridades competentes (Fuerzas y Cuerpos de Seguridad) pueden realizar actividades vigilancia electrónica sin obtener previamente un mandamiento judicial, por ejemplo, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas o rebeldes, la medida prevista de intervención podrá ser ordenada por el Ministro del Interior o, en

[276] Art. 579 LECrim.

[277] Fiscalía General del Estado. Circular 1/2013, sobre Pautas en Relación con la Diligencia de Intervención de las Comunicaciones Telefónicas, p.56.

[278] STS nº 926/2007, de 13 de noviembre.

su defecto, el Director de Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación. El Juez podrá acordar la medida, en resolución motivada, por un plazo de hasta tres meses prorrogables.[279]

La interceptación de las comunicaciones podrá ser concedida además de para investigar los delitos estipulados en el artículo 579.1 para otros delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.[280]

2. En relación con las c**omunicaciones electrónicas almacenadas**, se considera que las mismas no constituyen actos de comunicación, y por tanto, no están sometidos a la protección constitucional al secreto de las comunicaciones que requiere de un mandamiento judicial para el acceso por parte de las

[279] Art. 579 LECrim.

[280] Art, 588 ter a).Esta medida fue introducida por Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, aprobada el 15 de Septiembre de 2015, con el objeto de consagrar ciertas medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a los datos personales garantizados por la Constitución. El texto se encuentra disponible en: http://www.senado.es/legis10/publicaciones/pdf/senado/bocg/BOCG_D_10_597_4138.PDF

autoridades. Tal y como señala ORTÍZ PRADILLO[281], es posible que el objeto de la investigación no sea el contenido de ninguna comunicación sino la información almacenada en un servidor (p. ej. datos económicos o contables acreditativos de una contabilidad B al margen de la declarada y que demuestren la comisión de un delito contra la hacienda pública; datos empresariales que revelen la estructura y funciones de una organización criminal, o la infracción de los derechos de propiedad industrial o intelectual de terceros, etc.). Se considera más bien el cuerpo de los delitos informáticos. Los documentos no integrados en un proceso de comunicación y almacenados en archivos informáticos bien en teléfonos móviles, ordenadores o asimilados, tendrían la consideración de simples documentos y, por tanto, sólo resultan, en su caso protegidos por el derecho a la intimidad.[282]

Con relación al correo electrónico, en España su protección jurídica varía en función de si dicho mensaje ha sido ya leído. Esta distinción se ha acuñado por el Tribunal Constitucional, quien ha establecido que un correo ya leído quedan fuera del ámbito del Art. 18.3 CE, toda vez que se entiende concluido el proceso de comunicación, quedando sólo protegidos por el derecho a la intimidad.[283] La Fiscalía General del Estado apunta "razones de prudencia

[281] ORTIZ PRADILLO, J.: "Problemas Procesales de la Ciberdelincuencia", Colex. Madrid, 2013, p.216.

[282] STS 782/2007, de 3 de octubre.

[283]STC nº 70/2002, de 3 de abril.

deben llevar a solicitar la autorización judicial para acceder a cualquier mensaje enviado por correo electrónico"[284] sin embargo, esta directriz no parece de obligatorio cumplimiento a la luz de la doctrina jurisprudencial. Por el contrario, el acceso a un correo electrónico que no ha sido leído está protegido por el derecho al secreto de las comunicaciones, y por tanto su intervención requiere necesariamente de un mandamiento judicial.[285]

3. La de Conservación de Datos, tiene por objeto la regulación de la obligación de los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones de conservar **los datos de tráfico** (excluyendo en contenido) generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación por el plazo de un año, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de una autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. El contenido de las comunicaciones electrónicas se excluye del ámbito de aplicación de esta

[284] Fiscalía General del Estado. Circular 1/2013, sobre Pautas en Relación con la Diligencia de Intervención de las Comunicaciones Telefónicas, p.30.

[285] STC nº 70/2002, de 3 de abril.

norma.[286] A la luz de la definición de servicios de "operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones"[287], parece que los operadores de Cloud Computing no podrían considerarse sujetos obligados.

4. La LSSI es la transposición española de la Directiva 2000/58/CE. Esta Directiva destaca la relevancia el desarrollo tecnológico para el tratamiento de los datos personales tanto por las nuevas posibilidades que abre como por el incremento de la capacidad de almacenamiento de la información.[288] Tal y como señala RUBÍ, La novedad más relevante de esta Directiva "estriba en definir un sistema de protección que garantice la neutralidad tecnológica"[289] de modo que los servicios de Cloud Computing se entienden comprendidos dentro de la definición de servicios de la sociedad de la información.

[286] Esta norma constituye la transposición al ordenamiento jurídico español de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 marzo 2006. Esta Directiva fue declarada inválida por el Tribunal de Justicia de la Unión Europea en abril de 2014 (Sentencia en los asuntos acumulados C-293/12 y C-594/12 Digital Rights Ireland y Seitinger y otros). El Tribunal de Justicia considera que, al imponer la conservación de ciertos datos relativos a las comunicaciones electrónicas y permitir el acceso a las autoridades nacionales competentes, la Directiva se inmiscuye de manera especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal. Esta Decisión no tiene efectos directos en la Ley española, no obstante motivó la revisión de la misma#, estableciendo que la cesión de datos deberá limitarse a la información que resulte imprescindible para la consecución de los fines señalados en su artículo 1.

[287] Artículo 2 de la Ley 25/2007.

[288] Vid. Directiva 2000/58/C, considerandos.

[289] RUBÍ, Jesús: "La protección de datos en el sector de las telecomunicaciones" publicado en el Boletín del Ilustre Colegio de Abogados de Madrid, Mayo 2007, 3.ª época N.36 p. 175.

A la luz de las recientes modificaciones introducidas en la LECrim, "todos los prestadores de servicios de **telecomunicaciones**, de **acceso a una red de telecomunicaciones** o de **servicios de la sociedad de la información**, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar a las autoridades competentes al juez, al Ministerio Fiscal y a los agentes de Policía Judicial designados para la práctica de la medida, la asistencia y colaboración precisa para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones"[290] por lo que si bien el régimen de las obligaciones del la Ley 25/2007 y de la LSSI difieren, ambas categorías de proveedores tienen una obligación amplia de colaboración con la justicia criminal.

7.2.2. Mecanismos jurídicos para la obtención de datos en la nube

En el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial podrán requerir los **datos identificativos de titulares** de las cuentas directamente a los prestadores de servicios antes mencionados. No se requerirá de una orden judicial.[291] Las autoridades gubernamentales pueden acceder a las comunicaciones en tránsito y

[290] LECrim Art. 588 ter e).

[291] LECrim Art. 588 ter m).

a los datos de tráfico en el marco de la investigación de delitos graves, por regla general mediante un mandamiento judicial. No obstante, en determinas circunstancias se podrá autorizar la práctica de la intervención mediante orden administrativa, existiendo la obligación de realizar una notificación judicial con carácter *ex post*. Estas reglas aplican también a los correos electrónicos no leídos. Cuando se trata de correo electrónicos que ya han sido leídos o de otros contenidos almacenados, los mismos se pueden por virtud de una orden administrativa.

Más allá de la mera revelación de información, el juez podrá autorizar la "utilización así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos: a) delitos cometidos en el seno de organizaciones criminales b) delitos de terrorismo c) delitos cometidos contra menores o personas con capacidad modificada judicialmente d) delitos contra la Constitución, de traición y relativos a la defensa nacional e) delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación".[292] Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el

[292] LECrim Art. 588 septies a).

funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia.[293]

El alcance territorial de esta disposición es incierto, pero dada la naturaleza de Internet y de que gran parte la infraestructura en la que se apoyan los servicios de la sociedad de la información no está ubicada dentro del territorio español, el efecto extraterritorial propuesto por el legislador parece ser importante.

Con relación a los poderes de investigación en el ámbito de la seguridad nacional, el Art. 4 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, faculta al CNI a "obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España, pudiendo actuar dentro o fuera del territorio nacional" para el cumplimiento de sus objetivos. De conformidad con la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, un Magistrado del Tribunal Supremo se encargará específicamente del control judicial de las actividades del Centro Nacional de Inteligencia, incluida eventual autorización de actividades que puedan afectar a la inviolabilidad del domicilio y al secreto de las comunicaciones. El plazo para

[293] LECrim Art. 588 septies b).

acordarlas será ordinariamente de setenta y dos horas, pudiendo reducirse, de forma extraordinaria y por motivos de urgencia debidamente justificados, a veinticuatro horas.

7.2.3. Secreto de las actuaciones

Para que la diligencia de intervención telefónica (y por analogía, del correo electrónico) sea eficaz ha de estar acompañada necesariamente del secreto de las actuaciones.[294] De conformidad con la LECrim, los sujetos obligados a colaborar (dentro de los que se incluirían los prestadores de servicios de Cloud Computing como prestadores de servicios de la sociedad de la información) tienen la obligación de guardar secreto acerca de las actividades requeridas por las autoridades, so pena de delito de desobediencia .

7.2.4. Registros transfronterizos

En España, no existe un base jurídica procesal concreta para el registro transfronterizo, sin perjuicio de la aplicación de las disposiciones de la Convención de Budapest ratificadas por España. No obstante, tal y como ilustra ORTIZ PRADILLO,[295] en España, se ha defendido la legitimidad del acceso transfronterizo a datos

[294] STS 182/2004, de 23 de abril.

[295] ORTIZ PRADILLO, Juan Carlos y otros: “Problemas Procesales de la Ciberdelincuencia”, Colex 2013, p.212.

contenidos en sistemas equiparables al Cloud Computing tales como discos virtuales y el correo web a partir de diversos argumentos con independencia de la ubicación de dichos datos dentro del territorio español.

1. Para BÉRMUDEZ,[296] en virtud de que la aplicación analógica de la normativa sobre el registro de "papeles y otros efectos" y de la entrada en lugar cerrado, permitiría entender que, por tratarse de un registro digital de un soporte de almacenamiento que no se encuentra a disposición del Instructor o, en general, concurren razones de urgencia que hicieran que el soporte pudiera ser borrado o manipulado antes de que se pudiera llevar a cabo la intervención del mismo, el aseguramiento de la prueba se produciría mediante la captura a través de Internet de los datos contenidos en el mismo bajo la fe del Secretario Judicial, con la debida intervención y control judicial dial en la adopción y ejecución de la medida.

2. Por su parte, VELASCO ha afirmado que la deslocalización y la transnacionalidad no son variables que afecten a los derechos fundamentales, y por lo tanto a la licitud de la prueba a que se refiere el artículo 11.1 de la Ley Orgánica del Poder Judicial, en consecuencia, cuando las autoridades españolas tienen el poder de disposición sobre el terminal informático a través del cual resultan accesibles esos datos ubicados en una jurisdicción

[296] BERMÚDEZ J.A., Y OTROS: "Aspectos Procesales de la Investigación de la Criminalidad Informática. Capítulo 2". Escuela Judicial Española, Madrid, 2009.

> extranjera, pues entiende. "La tutela de los derechos fundamentales no puede quedar a la decisión del gestor de un servicio informático (por ejemplo de Google) sobre el lugar que elija para ubicar los medios técnicos desde los que lo presta, máxime cuando la infracción penal produce efectos dañinos en el país que trata de perseguir el delito, cuando los dispositivos/terminales se hayan ocupado y el delito haya producido efectos, por ejemplo, en España"[297] apunta.

Ahora bien, ambos argumentos defienden que existe un acceso transfronterizo legítimo en la utilización por parte de las autoridades de las credenciales de autenticación del imputado (usuario y contraseña) pero no la entrega directa por parte del proveedor de servicios de Cloud. Apunta VELASCO, "... Si por el contrario no se ocupa el dispositivo que realizó la comunicación, pero se conoce, y este opera desde fuera de España (refiriéndose al proveedor) no cabe otra manera de obtenerlo con licitud, que recabando directamente del proveedor. Si el proveedor se encuentra en España, cabe la aplicación de las figuras preparatorias a las injerencias telecomunicativas-principalmente la conservación de datos que luego se pedirán formalmente- e incluso investigativas, que se arbitran a través de su acuerdo razonado por auto judicial y se ejecutan a través del oportuno mandamiento a las empresas servidoras del correo electrónico afectado. Si el proveedor tiene su sede

[297] VELASCO NUÑEZ, Eloy: "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, gps, balizas, etc.: la prueba tecnológica" Diario La Ley, N.º 8183. Madrid, 2013.

en el extranjero y los datos no se encuentran en territorio español procede la utilización de los mecanismos de cooperación policial y judicial tales como la comisión rogatoria internacional o los tratados de asistencia mutua, respectivamente".[298]

En cuanto a los datos disponibles al público, según explica la Fiscalía General del Estado, "el principio básico es el de que no se precisa autorización judicial para conseguir lo que es público (...) Los rastreos policiales para localizar direcciones IP pueden por tanto realizarse sin necesidad de autorización judicial, ya que no se trata de datos confidenciales preservados del conocimiento público".[299] No se menciona si este criterio debe aplicarse solo dentro de los límites del ciberespacio nacional, lo cual es razonable, dado que el mismo no se puede determinar fácilmente. Por tanto, parece razonable asumir que las autoridades españolas realizan operaciones de rastreo en Internet fuera de las fronteras nacionales. Este criterio se alinea con el artículo 32 de la Convención de Budapest. Con relación a la obtención transfronteriza de evidencias, la Audiencia Nacional ha subrayado que, el hecho de que la globalización de las comunicaciones haga posible la obtención transfronteriza de

[298] VELASCO NUÑEZ, Eloy: "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, gps, balizas, etc.: la prueba tecnológica" Diario La Ley, N.º 8183. Madrid, 2013.

[299] Fiscalía General del Estado. Circular 1/2013, sobre Pautas en Relación con la Diligencia de Intervención de las Comunicaciones Telefónicas, p.47.

evidencias no deroga el régimen general al que han de ajustarse estas para su validez.[300]

7.2.5. Evidencias obtenidas en el extranjero

Sobre las comunicaciones obtenidas en el extranjero, por autoridades extranjeras la Fiscalía General ha ha señalado los Tribunales españoles no deben supervisar su legalidad a la luz de la normativa española, cuando se trate de países en los que se mantengan de modo efectivo los mismos valores y principios que en España se consagran en la Constitución. No es procedente imponer a servicios policiales extranjeros las mismas normas internas que la doctrina jurisprudencial interna ha establecido para los servicios policiales españoles. No obstante, queda abierta la posibilidad de valorar si las intervenciones fueron practicadas conforme a las normas procesales del país de obtención. En este caso, corresponde a quien lo alega la prueba de la inobservancia de la norma procesal extranjera y por tanto de la ilegalidad y nulidad de esta prueba.[301]

7.2.6. Recurso judicial

[300] SAN Sala Penal, 31/2009, de 30 de abril de 2009.

[301] Fiscalía General del Estado. Circular 1/2013, sobre Pautas en Relación con la Diligencia de Intervención de las Comunicaciones Telefónicas, p.142.

La Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen desarrolla la protección civil de estos derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen frente a todo género de injerencia o intromisiones ilegítimas, sin perjuicio de la protección penal que concurre en algunos casos.[302] Las intrusiones ilegítimas en estos derechos en el contexto del acceso gubernamental, pueden ser reparadas civilmente al amparo de esta norma.

7.3. Reino Unido

7.3.1. Marco Legal

A diferencia de la mayoría de los Estados modernos, el Reino Unido no cuenta con una constitución codificada. Su Constitución está formada por las leyes del Parlamento, sentencias y resoluciones judiciales.[303]

[302] Introducción de la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

[303]BLACKBURN, Robert: “Britain's unwritten constitution”. Disponible en: http://www.bl.uk/magna-carta/articles/britains-unwritten-constitution

En el Reino Unido, las potestades que las autoridades gubernamentales pueden utilizar para obligar a los proveedores de servicios de Cloud Computing a revelar información sobre sus usuarios, así como los límites a dichas potestades se encuentra principalmente en la Regulation of Investigatory Powers Act de 2000[304] (RIPA) y en Data Retention and Investigatory Powers Act de 2014 (DRIPA).

RIPA regula las competencias de los organismos públicos para llevar a cabo la vigilancia y la investigación, incluida la interceptación de las comunicaciones. La norma tipifica como delito la interceptación intencional y sin autorización legal de cualquier comunicación en el curso de su transmisión por medio de un sistema de telecomunicaciones pública y en ciertas circunstancias, de un sistema de telecomunicaciones privado[305] en el territorio del Reino Unido.[306]

La frase "en el proceso de transmisión" podría resultar confusa, no obstante se ha interpretado que cubre tanto las comunicaciones en tránsito como cualquier comunicación que se encuentra en estado de almacenamiento y que aún no ha sido leída (por ejemplo, un correo electrónico no leído).[307]

[304] Disponible en: http://www.legislation.gov.uk/ukpga/2000/23/contents

[305] La interceptación los sistemas de telecomunicaciones privados no sería punibles cuando quien las realiza es (a) una persona con derecho a controlar el funcionamiento o el uso del sistema (b) que tiene el consentimiento expreso o implícito de tal persona para hacer la intercepción. Art .1 (6) RIPA.

[306] Chapter I, Section 1.

[307] MCNICHOLAS, Nicholas J.F: "The UK Electronic Communications Act". Publicado en A Decade of Research @the crossroads of law and ICT. Bruselas, 2001, p.168.

7.3.2. Mecanismos jurídicos para la obtención de datos en la nube

RIPA contempla dos mecanismos para la obtención de comunicaciones electrónicas, a saber, la orden administrativa y la orden judicial:

Orden administrativa:

Las Autoridades gubernamentales británicas pueden, mediante una orden administrativa, obtener comunicaciones en tiempo real, comunicaciones almacenadas[308] y datos de tráfico en interés de la seguridad nacional; para prevenir o detectar delitos graves, incluido para dar efecto a las disposiciones de cualquier acuerdo de asistencia mutua internacional; salvaguardar el bienestar económico del Reino Unido. Estas órdenes deben ser proporcionales a los fines para los que se recaban.[309]

[308] RIPA Sección 2(7)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf

[309] Art. 5.3.

En relación con las comunicaciones en tiempo real, el Secretario de Estado puede autorizar la intervención mediante una orden de registro administrativa en interés de la seguridad nacional; para prevenir o detectar delitos graves, incluido para dar efecto a las disposiciones de cualquier acuerdo de asistencia mutua internacional; salvaguardar el bienestar económico del Reino Unido. Estas órdenes deben ser proporcionales a los fines para los que se recaban.[310]

Un número limitado de personas que pueden hacer las solicitudes de órdenes de interceptación, principalmente:

- El Director General del Servicio de Seguridad.
- El Jefe del Servicio Secreto de Inteligencia.
- El Director del GCHQ.
- El Director General de la Inteligencia Nacional Penal.
- El Comisionado de la Policía Metropolitana.
- El jefe de policía del Servicio de Policía.
- Los Comisionados de Aduanas e Impuestos Especiales.
- El Jefe de Inteligencia de Defensa.

[310] Art. 5.3.

- Una persona que, a los efectos de cualquier mutua internacional acuerdo de asistencia, es la autoridad competente de un país o territorio fuera del Reino Unido.

Una vez que la orden de interceptación se ha servido, la "persona que preste un servicio público de telecomunicaciones" o que tenga la totalidad o parte de un sistema de telecomunicaciones con sede en todo o en parte, en el Reino Unido" deberá tomar todas las medidas para dar cumplimiento a la orden de que se notifiquen (Sección 11.4) so pena de delito de desobediencia.[311] Nótese que la disposición habla concretamente de "servicio público de telecomunicaciones". El sector de las telecomunicaciones se encuentra fuertemente regulado (barreras de entrada, régimen de autorizaciones administrativas, servicio universal, etc.) y su régimen incorpora definiciones muy precisas sobre lo que considera un servicio público de telecomunicaciones. Aunque se ha sostenido que los sistemas de Cloud Computing basados en el Reino Unido nube basan estaban dentro del ámbito de RIPA,[312] desde la perspectiva penal no puede haber una interpretación extensiva del tipo de desobediencia, so pena de vulnerar el principio fundamental del derecho

[311] (a) en sentencia condenatoria, a una pena de prisión no superior a dos años o una multa, o ambas; (b) en sentencia sumaria, a una pena de prisión no superior a seis meses o una multa que no exceda el máximo legal, o de ambos ambos (RIPA Sección 11.4).

[312] GRINGAS, Clive: "UK Cloud Computing Interception - nothing new". Olswang, 2014. Diesponible en: http://www.olswang.com/pdfs/CloudComputingInterception_CQG.pdf

penal en las sociedades democráticas como el principio *nullum crimen nulla poena sine lege*.

En 2014 se introdujo Data Retention and Investigatory Powers Act (DRIPA). La norma continúa restringiendo el ámbito de aplicación a operadores públicos de telecomunicaciones,[313] no obstante, amplía la definición de servicios de telecomunicaciones a aquellos "servicios que consisten en provisión de acceso, y los medios para hacer uso de un sistema de telecomunicaciones que incluye en cualquier caso la creación, gestión o almacenamiento de las comunicaciones transmitidas, o que puedan ser transmitidas mediante el sistema". Bajo esta nueva perspectiva, lo más probable es que un proveedor de servicios de la nube se considere un "servicio de telecomunicaciones" si proporciona servicios de comunicaciones basados en la nube (servicios por ejemplo, mensajería instantánea, conferencia web o correo electrónico). La norma introduce introduce la figura del Comisionado de Interceptación de la comunicaciones cuyo cometido es proporcionar una supervisión independiente del uso de las facultades contenidas en el régimen de intercepción de conformidad con el Capítulo I de RIPA.

[313] Véase Parte 5 de la norma. Dispoible en:
http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf

7.3.3. Acceso transfronterizo

El aspecto más novedoso de DIRPA es que introduce la extraterritorialidad de los poderes de investigación del Gobierno del Reino Unido de la siguiente manera:

- La orden de interceptación puede recaer sobre proveedores no basados en el Reino Unido.
- La orden puede relacionarse con hechos que no han ocurrido en el Reino Unido, pero se refiere a ciudadanos del Reino Unido.
- Se tendrá en cuenta si el operador puede razonablemente practicar lo ordenado teniendo en cuenta las restricciones que impone la ley en el país donde se ejecutará la orden, y la orden será válida en la medida que no viole dichos requerimientos o restricciones.[314]

Orden Judicial

El gobierno puede solicitar que un tribunal autorice el acceso a datos en conexión con un abanico más amplio de delitos, que el tribunal podrá conceder lo solicitado si el gobierno puede demostrar que existen motivos razonables para creer que un delito (que no sea un delito menor) se ha cometido y los datos son probable que sea de valor sustancial a una investigación penal en curso.

[314] http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf

La Ley de Evidencia Penal de 1984 legitima a los agentes de policía a obtener cualquier información almacenada de forma electrónica y que sea accesible *desde* el domicilio, sin embargo, algunos han rechazado que se pueda obtener fuera del territorio nacional, debido a que la normativa aplicable a la policía limita la jurisdicción de los agentes de policía en el ejercicio de sus funciones al territorio del Reino Unido.[315] No obstante, a la luz de DRIPA, la actuación de las autoridades dentro del territorio del Reino Unido con efectos extraterritoriales introduce un importante cambio en el enfoque tradicional de jurisdicción. Asimismo, cabe recordar que el Reino Unido es parte de la Convención de Budapest (al igual que España y los EE.UU) por lo que las disposiciones del Art. 32 de dicha Convención resultaría aplicables en este contexto.

7.3.4. Recurso judicial

RIPA establece un tribunal independiente compuesto por altos cargos del Poder Judicial y de práctica legal. El tribunal tiene plena poderes para investigar y decidir cualquier caso dentro de su jurisdicción.[316] A diferencia de los Estados Unidos y España, en el Reino Unido no se contempla un derecho de daños específico para la

[315] WALDEN, Ian: "Cybercrime and Jurisdiction in the United Kingdom" en Cybercrime and Jurisdiction: A Global Survey. TMC Asser. La Haya, 2006, p.302.

[316] Su sitio web, procedimiento de quejas e informes anuales se pueden consultar en http://www.ipt-uk.com/

privacidad. Los perjuicios relacionados con intrusiones legítimas en la privacidad deben ampararse en las llamadas acciones de pérdida de confianza o *breach of confidence* (*Caso Earl Spencer vs Reino Unido*).[317]

Notas distintivas

A la luz de los extremos analizados, puede afirmarse que los tres ordenamientos jurídicos consagran valores de protección y garantías equivalentes con respecto al secreto de las comunicaciones y el contenido almacenado en servicios de Cloud Computing, a la par que facilitan el acceso por parte de las autoridades competentes tanto con fines de investigación y persecución criminal, como de inteligencia y seguridad nacional. No obstante, estos ordenamientos difieren en el enfoque reglas de procedimiento y requisitos a observar para el acceso a las mismas:

- **Documentos y comunicaciones almacenadas:** En España no se requiere de una orden judicial para el acceso a comunicaciones almacenadas (e-mails leídos) y documentos, las autoridades gubernamentales puedes solicitar el acceso a los mismos mediante una orden administrativa. En los EE.UU, por regla general se requiere la autorización judicial (orden judicial ECPA u orden

[317] GILIKER, Paula: "A Right to Personal Privacy the English Law of of Torts?". The Europeanisation of English Tort Law. Oxford, 2014 p. 173.

de registro, según el caso) almacenadas durante menos de 180 días. En el Reino Unido, se puede solicitar este acceso cuando se investiga una serie de delitos preestablecidos, en los demás caso se requerirá de una orden judicial.

- **Comunicaciones en tránsito:** En España en principio se requiere la obtención de una orden judicial previa para el acceso legítimo por parte del gobierno al contenido de la comunicaciones en proceso de transmisión así como los correos no abiertos, así como para los datos de tráfico, no obstante en algunos se permita la práctica mediante una orden administrativa, pudiendo producirse el control judicial de forma *ex post*. En los EE.UU se aplican por regla general se requiere de una autorización judicial, no obstante, en determinados caso la autorización se puede realizar por via administrativa, En el Reino Unido las autoridades pueden acceder a comunicaciones en tránsito y almacenadas mediante una orden judicial, sin embargo ciertos delitos especialmente grave permiten el acceso administrativo, siempre que la orden se ajuste a los requisitos del proporcionalidad y finalidad establecidos. En los EE.UU. la libertad de expresión tiene un valor constitucional máximo, las peticiones en las que intersectan este derecho difícilmente son autorizadas por los tribunales.

- **Seguridad nacional:** Si bien el régimen de EE.UU y el Reino Unido resultan comparables, resulta difícil una comparación con el régimen español, pues este no regula con detalle los poderes y limitaciones del CNI, restringiéndose a encomendarle la "obtención de señales" y estableciendo un régimen de supervisión judicial.

7.4. Asistencia judicial entre la UE y los EE.UU.

Los atentados terroristas del 11 de septiembre de 2001 contra las Torres Gemelas de Nueva York, produjeron conmoción profunda en la comunidad internacional y reforzaron la idea de facilitar que las diversas resoluciones dictadas en un proceso penal tuviesen efectos más allá de las fronteras de un Estado, así como de flexibilizar las barreras jurisdiccionales existentes entre los distintos Estados. Este clima impulsó las negociaciones entre los EE.UU y la Unión Europea en este sentido, que concluyeron en acuerdos internacionales con el objeto de perfeccionar o complementar las relaciones bilaterales de cooperación existentes entre los distintos Estados Miembros y los EE.UU. en asuntos penales.

En junio de 2003 la Unión Europea decidió firmar dos acuerdos en materia de asistencia judicial y extradición, respectivamente.[318] Más adelante, en octubre de 2009, el Consejo de Europa emitió la Decisión 2009/820/PESC sobre la celebración, en nombre de la Unión Europea, del Acuerdo de Extradición entre la Unión Europea y los Estados Unidos de América y del Acuerdo de Asistencia Judicial en materia penal entre la Unión Europea y los Estados Unidos de América.[319] La particularidad de estos acuerdos reside en que los mismos no introducen cuerpos normativos autónomos *per se*, sino que garantizan una regulación homogénea y reforzada a través de la subsiguiente reforma de los tratados existentes entre cada uno de los EE.UU. y los Estados Miembros de la UE.[320]En consecuencia encontramos que los acuerdos actuales de los EE.UU. con España y el Reino Unido, respectivamente, son sustantivamente parecidos, aunque con ciertos matices importantes heredados de las primeras versiones respectivas de acuerdos individuales de preexistentes.

El artículo 4 del Tratado de Asistencia Judicial introduce una novedad importante en relación con la cesión de información bancaria, estableciendo que la misma no podrá denegarse por motivos de secreto bancario, sin embargo, sí que podrá aplicarse el

[318]Decisión del Consejo 2003/516/CE: , de 6 de junio de 2003, relativa a la firma de los Acuerdos entre la Unión Europea y los Estados Unidos de América sobre Extradición y Asistencia Judicial en Materia Penal http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003D0516

[319] Acuerdo de Asistencia Judicial en materia penal de la Unión Europea con Estados Unidos. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:jl0052

[320] JIMÉNEZ LÓPEZ, Raquel: "Convenios Bilaterales y de la Unión Europea con Terceros". Cooperación Judicial Penal en Europa. Madrid 2013. p. 912.

criterio general de la doble tipificación, es decir, exigir que la conducta esté tipificada en ambos ordenamientos para que la cesión de información sea legítima.

Asimismo, estableció los países podrán limitar la prestación de su asistencia a los delitos que:

- sean punibles con arreglo a la legislación de ambos países (requirente y requerido);
- sean punibles con la privación de libertad o una medida de seguridad por un periodo máximo (de al menos cuatro años en el país solicitante y dos años en el país requerido);
- se especifiquen como graves y punibles con arreglo a la legislación de ambos países.

Aunque un país limite su prestación de asistencia a los dos últimos tipos de delitos, deberá facilitar la identificación de las cuentas bancarias relacionadas con la actividad terrorista y el blanqueo de productos generados por actividades delictivas graves que sean punibles con arreglo a la legislación de ambos países.[321]

7.4.1. EE.UU. y el Reino Unido

[321] Art.4.4(a) del Tratado
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2003.181.01.0034.01.SPA

La cooperación judicial entre EE.UU. y el Reino Unido se rige por el Tratado de Asistencia Judicial en materia penal de 1994,[322] modificado, modificado por el Acuerdo de Asistencia Judicial UE-EE.UU. [323]

De conformidad con su artículo 1, los Estados contratantes se prestarán asistencia mutua, de conformidad con el Tratado, en cuanto se refiere a las investigaciones y procedimientos en materia penal seguidos en cualquiera de ellos. La asistencia comprenderá la provisión de documentos, antecedentes y elementos de prueba; la ejecución de órdenes de registro y embargo, la iniciación de procedimientos penales en el Estado requerido, entre otros, también autoriza cualquier otra forma de asistencia acordada por las partes.

Existe una obligación positiva de asistencia por parte de ambos Estados, salvo en circunstancias excepcionales previstas en el Art. 3 del Tratado. Así, la Autoridad Central del Estado requerido podrá denegar la asistencia, por ejemplo, si la Parte Requerida considera que la solicitud podría menoscabar su soberanía, seguridad u otros intereses esenciales, resulta contraria al orden público, o se refiere a un delito

[322] Treaty Between the UNITED STATES OF AMERICA and the UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, 1994. Disponible en: http://fas.org/irp/world/uk/us-uk-mla.pdf

[323] Instrument as contemplated by Article 3 (2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters signed 6 January 1994. Disponible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/238612/7613.pdf

que es considerado por la Parte Requerida como: (i) un delito de carácter político (ii) un delito en el orden militar que no sea también un delito a la luz del derecho penal ordinario de la Parte Requerida. También podrá denegar una solicitud cuando esta implique el ejercicio de poderes de búsqueda y captura que no se podrían ejercer en el territorio de la Parte Requerida en circunstancias similares.

Se deberá seguir el método de ejecución especificado en la solicitud en la medida en que sea compatible con las leyes y prácticas de la Parte Requerida. Cuando así se solicite, la Parte requerida deberá mantener la confidencialidad de la solicitud, no obstante, en caso de que la solicitud no pueda ser ejecutada sin violar la confidencialidad de la misma, la Parte requerida informará de ello a la Parte Requirente, quien determinará si, y en qué medida, desea que la solicitud sea ejecutada.

A menos de que se indique lo contrario por la Parte Requerida cuando se ejecuta la solicitud, la información o pruebas o el contenido de que se han descrito en la medida judicial o administrativa con la solicitud puede ser utilizado para cualquier propósito por la Parte requirente.

7.4.2. EE.UU. y España

La cooperación judicial entre España y EE.UU. se rige por el Tratado de Asistencia Jurídica Mutua de 1990, modificado, modificado por el Acuerdo de Asistencia Judicial UE-EE.UU.[324]

De conformidad con el artículo 1, los Estados contratantes se prestarán asistencia mutua, de conformidad con el Tratado, en cuanto se refiere a las investigaciones y procedimientos en materia penal seguidos en cualquiera de ellos. La asistencia comprenderá la provisión de documentos, antecedentes y elementos de prueba; la ejecución de órdenes de registro y embargo, la iniciación de procedimientos penales en el Estado requerido.

También autoriza cualquier otra forma de asistencia no prohibida en la legislación del Estado requerido. Nótese que, a diferencia del acuerdo con el Reino Unido, el Tratado español somete los acuerdos entre las partes a la legislación del Estado requerido, no sólo aquellas diligencias que impliquen el ejercicio de poderes de búsqueda y captura. La asistencia se prestará con independencia de que el hecho que motiva la solicitud de asistencia sea o no delito en el Estado requerido. Existe

[324] Instrumento contemplado por el art 3(2) del Acuerdo de asistencia judicial entre los Estados Unidos de América y la Unión Europea firmado el 25 de junio de 2003, sobre la aplicación del Tratado de asistencia jurídica mutua en materia penal entre USA y el Reino de España firmado el 20 de noviembre de 1990, hecho ad referendum en Madrid el 17 de diciembre de 2004. Disponible en: http://www.boe.es/boe/dias/2010/01/26/pdfs/BOE-A-2010-1172.pdf

una obligación positiva de asistencia por parte de ambos Estados, salvo en circunstancias excepcionales previstas en el artículo 3 del Tratado. La Autoridad Central del Estado requerido podrá denegar la asistencia si la solicitud se refiere a un delito tipificado en la legislación militar y no en la legislación penal ordinaria, o la ejecución de la solicitud pudiera atentar contra la seguridad u otros intereses esenciales del Estado requerido.

En cuanto a las condiciones de confidencialidad de las pruebas aportadas, podrá pedir que la información o las pruebas aportadas tengan carácter confidencial, en los términos y condiciones que se especifiquen (Art. 5.5). No obstante, no podrá imponer restricciones genéricas respecto a las normas legales del Estado requirente sobre el procesamiento de datos personales como una condición adicional para que proporcione pruebas o información (Art. 7.3.b).

El Estado requerido podrá exigir que el Estado requirente limite el uso de la información o las pruebas que se le faciliten para sus investigaciones o procedimientos penales, para prevenir una amenaza inmediata y grave a su seguridad pública, para sus procedimientos (judiciales o administrativos) que no sean penales pero estén directamente relacionados con las investigaciones o procedimientos cubiertos por el Tratado, salvo que la información o las pruebas se

hubieran hecho públicas o que el Estado requerido otorgue previamente su consentimiento (Art. 7.2).

En relación con órdenes de registro y embargo, El Estado requerido cumplimentará toda solicitud de registro, embargo y entrega de cualquier objeto, entre ellos, sin que esta enumeración tenga carácter exhaustivo, cualesquiera documentos, antecedentes o elementos de prueba, siempre que en la solicitud se incluya información que justifique dicha acción según la legislación del Estado requerido (Art. 14).

7.5. Dos casos emblemáticos en materia de acceso gubernamental

7.5.1. Caso Bélgica vs Yahoo!

El caso Bélgica vs Yahoo! se inició con la solicitud dirigida por parte del fiscal de la localidad belga de Dendermonde a Yahoo! con el objeto de que la compañía revelase las direcciones IP de determinadas usuarios investigados por fraude informático en Bélgica. En el caso se abordaron dos cuestiones:

a) **Naturaleza de los servicios de correo electrónico:** ¿servicios de comunicaciones electrónicas o servicios de la sociedad de la información? En el caso se plantea la cuestión de si los servicios de correo electrónico web (SaaS) se consideran servicios de comunicaciones electrónicas a la luz del artículo 46 bis del Código de Procedimiento Penal belga, el cual obliga a sus proveedores respectivos a revelar datos identificativos sus usuarios a la justicia criminal cuando así se solicite por las autoridades competentes [325] y por tanto, si existe un deber de cooperación con la justicia por parte del de Yahoo! como proveedor de servicios de correo electrónico que se encuentran accesibles desde Bélgica.

Sobre este particular, el fiscal de Dendermonde sostuvo que Yahoo! es un proveedor de servicios de comunicaciones electrónicas y en consecuencia, estaba obligado a cumplir con la solicitud de información a la luz del citado artículo 46 bis del Código de Procedimiento Penal belga. Por su parte, Yahoo! argumentó no podía considerársele un proveedor de servicios de comunicaciones electrónicas. Para la compañía, la expresión "proveedor de servicios comunicaciones electrónicas" contenida en el artículo 46 bis del Código de Procedimiento Penal tiene el mismo significado que el término "proveedor de servicios comunicaciones electrónicas" definido el artículo 2 de

[325] Code d'Instruction Criminelle.

la Ley de Comunicaciones Electrónicas belga,[326] que define los servicios de comunicaciones electrónicas como aquellos "servicios normalmente ofrecidos a cambio de pago, que en su totalidad o principalmente, consiste en la transferencia, incluyendo los procesos de conmutación y enrutamiento de señales a través de redes de comunicaciones electrónicas".[327] Los proveedores de servicios de la sociedad de la información, tales como los proveedores de direcciones de correo electrónico gratuito, no se consideran un proveedor de servicios de comunicaciones electrónicas, Yahoo! Con apoyo es este argumento, Yahoo! considera que no está obligada a revelar los datos solicitados la fiscalía.[328]

Según la definición, los servicios de comunicaciones electrónicas son servicios que consisten en el transporte de señales (datos) sobre una red de comunicaciones electrónicas (por ejemplo, acceso de banda ancha a Internet, líneas telefónicas, conexiones móviles). Parece que el alcance se restringe a los llamados proveedores de servicios de Internet o Internet Service Providers (ISPs), es decir, proveedores que otorgan acceso a Internet y se ocupan del

[326] Loi relative aux communications électroniques, de 13 de junio de 2005. Disponible en: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2005061332

[327] Art. 2.5.

[328] ROLAND, Nicolas:"Court of Appeal of Antwerp confirms Yahoo!'s obligation to cooperate with law enforcement agencies", Bruselas, 2014. Disponible en: http://www.stibbe.com/en/news/2014/july/benelux-ict-law-newsletter-49-court-of-appeal-of-antwerp-confirms-yahoo-obligation

transporte de las señales electrónicas través de la red. Los servicios de acceso a Internet no suelen ser gratuitos sino que requieren de una suscripción y de un pago, tal y como apunta la definición.

Yahoo! ofrece una aplicación gratuita de correo electrónico que permite a los sus usuarios enviar y recibir mensajes de correo electrónico. Yahoo! no está involucrado en el transporte de señales o información sobre la red (desde y hacia sus servidores) como tal, estos se cubren por el ISP al que está suscrito el usuario Yahoo!. Para hacer uso de los servicios de Yahoo el usuario tendrá que contar con un servicio de acceso internet (e.g. banda ancha, internet móvil, etc.).

Para algunos, Yahoo! no podía ser calificado como proveedor de servicios de comunicaciones electrónicas y por lo tanto no podía ser sujeto a la Sección 46 bis CPP, independientemente de si tiene alguna presencia en Bélgica. Y lo mismo se aplica a los proveedores de servicios de correo web o comunicaciones similares, como Hotmail, Gmail, Facebook, Twitter o Skype.[329]

[329]DE SCHRIJVER, S. and DAENENS T: "The Yahoo! Case: The End of International Legal Assistance In Criminal Matters". 2013. Disponible en: http://whoswholegal.com/news/features/article/30840/yahoo-case-end-international-legal-assistance-criminal-matters

b) Jurisdicción extraterritorial: En segundo lugar, el caso plantea una cuestión jurisdiccional, en particular de ejercicio de la jurisdicción Belga fuera del territorio. Se discute si Bélgica a través de su fiscal puede enviar válidamente una solicitud de cooperación a un proveedor de servicios que no tiene presencia (oficinas o sucursales) ni tampoco tiene infraestructura (centros de datos) si no en el territorio de otro Estado, en concreto en los EE.UU, sin hacer uso de los mecanismos de cooperación judicial internacional existentes.

El caso se desenvolvió de la siguiente manera:[330]

- En marzo de 2009, la Corte de Dendermonde falló en contra de Yahoo! determinando que la empresa tenía un deber de colaboración con la justicia criminal belga, e imponiéndole una multa sustancial[331] por su negativa a proporcionar las direcciones IP de los presuntos delincuentes en violación del Derecho Procesal Penal belga. Según la Corte, aunque Yahoo! se encuentra establecida fuera del territorio de Bélgica, tiene presencia comercial en el país puesto que sus servicios son accesibles desde Bélgica. El deber de cooperación

[330] Un resumen cronológico del caso puede encontrarse en VAN LINTHOUT, P & LERKHOFS,J: "Tour de table – major cases and important events". Cybercrime Convention Committee (T-CY), Strasbourg, 2-3 December 2013. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/Octopus2013_TCY_10th_plen.pdf

[331] En concreto, una pena pecuniaria de 55.000 euros, y una penalidad de 10.000 euros por cada día de retraso en la cesión de los datos.

en Bélgica se extiende a cualquier proveedor cuyos servicios sean accesibles desde Bélgica.

- En junio de 2010, la Corte de Apelaciones de Gent[332] absolvió a Yahoo! afirmando que la compañía no podría ser calificada un "proveedor de servicios de comunicaciones electrónicas" ni tampoco un "operador de redes de comunicaciones electrónicas" únicamente sobre la base de la provisión de sus servicios de correo electrónico, pues dichos servicios no constituyen *per se* servicios de comunicaciones electrónicas. El proveedor del acceso a Internet sí que se considera un proveedor de servicios de comunicaciones electrónicas. En consecuencia, Yahoo! no podría ser obligado a cooperar con las autoridades belgas en virtud de una disposición específica del Código de Procedimiento Penal belga.

- En enero de 2011, la Corte Suprema revocó en casación el fallo de la Corte de Apelaciones de Gent, señalando que las definiciones de "operador de redes de comunicaciones electrónicas" y "proveedor de servicios de comunicaciones electrónicas" contenidas en la Ley de Comunicaciones Electrónicas no debían aplicarse en los procedimientos penales, y que en cambio, a estos conceptos debía dárseles una interpretación más amplia en el contexto penal, pudiendo dicha interpretación cubrir a los servicios de correo electrónico ofrecidos por

[332] http://oerlemansblog.weblog.leidenuniv.nl/files/2011/02/Gent_-_OM-Yahoo.pdf

Yahoo!. Para la Corte, en el Derecho Penal la terminología debe interpretarse con independencia de la terminología acuñada en el Derecho Civil, y en caso analizado, aunque la Ley de Comunicaciones Electrónicas y el Código de Procedimiento Penal usan idéntica terminología, su ámbito de aplicación en la práctica es diferente, pudiendo cubrir a diferentes entidades. Según esta Sentencia, a la luz Código de Procedimiento Penal belga, Yahoo! se considera "proveedor de servicios de comunicaciones electrónicas", con independencia de que se encuentre establecido fuera del territorio de Bélgica.

- En octubre de 2011, la Corte de Apelaciones de Bruselas absolvió a Yahoo! tras examinar en primer lugar la cuestión jurisdiccional y concluir que existía un vicio de grave procedimiento en la notificación que se había realizado a Yahoo!. El ministerio público de Bélgica no tiene jurisdicción fuera de Bélgica, asimismo, la Corte argumentó que el mero hecho de que resultara técnicamente posible para el fiscal contactar con Yahoo! desde desde Bélgica a través de medios electrónicos o de otro tipo de comunicación, no era suficiente para considerar que se había producido una notificación válida, por tanto no existía evidencia de que había ocurrido requerimiento alguno en el territorio de Bélgica.

- En septiembre de 2012, la Corte Suprema de Bélgica consideró en casación, ante la apelación por parte del Ministerio Público, que "El hecho de que el Fiscal del Ministerio Público envíe, desde Bélgica, la solicitud por escrito al que se refiere el Art. 46 bis Código de Procedimiento Penal (Belga) requiriendo la cooperación del operador de redes de comunicaciones electrónicas o de servicios de comunicaciones electrónicas establecidos fuera del territorio belga a una dirección extranjera, no invalida la solicitud".[333]

- En noviembre de 2013, la Corte de Apelaciones confirmó la aplicabilidad del artículo 46 bis del Código de Procedimiento Penal a los servicios de correo electrónico ofrecidos por Yahoo! ratificando los argumentos de la Corte de Dendermonde en primera instancia. Asimismo, consideró que el ejercicio de jurisdicción por parte del Ministerio Fiscal fuera de Bélgica sin utilizar mecanismo de cooperación judicial fueron válidos. En definitiva, opinó que Yahoo! debía "traer" la información; y que en caso de no desear cooperar con la justicia belga, debería proceder a excluir el rango de direcciones IP belgas de sus servicios, procediendo a imponer una pena pecuniaria a la compañía.

[333] VAN LINTHOUT, P & LERKHOFS, J: "Tour de table – major cases and important events". Cybercrime Convention Committee (T-CY), Strasbourg, 2-3 December 2013. D.9.

Para algunos, este fallo parece ignorar la complejidad de los problemas de la jurisdicción en Internet.[334] No obstante, a la luz del último criterio jurisprudencial mencionado, en Bélgica la justicia criminal puede obtener datos directamente de un proveedor de servicios de comunicaciones electrónicas establecido en el extranjero en lugar de utilizar los Procedimientos de asistencia mutua. Para otros es el reflejo y una posible solución a los problemas jurisdiccionales de Internet.

7.5.2. Caso Microsoft vs Estados Unidos

El caso Microsoft vs Estados Unidos,[335] aún pendiente de resolución definitiva, ejemplifica algunos de los retos que plantea la nube. En el marco de la investigación de un delito relacionado con el tráfico de estupefacientes, un juez de Nueva York, emitió una orden de registro ECPA, ordenando a Microsoft Inc., proveedor estadounidense de servicios de Cloud Computing con operaciones globales, a entregar información sobre una cuenta de servicios msn/hotmail en el ámbito B2C, incluidos datos almacenados. En este caso, la información solicitada se encontraba alojada "exclusivamente" en Irlanda, en centros de datos de propiedad, operados, y controlados por Microsoft,[336] cuya sede principal se encuentra en los EE.UU.

---

334 http://whoswholegal.com/news/features/article/30840/yahoo-case-end-international-legal-assistance-criminal-matters

335 La documentación más relevante del caso puede consultarse en http://digitalconstitution.com/about-the-case/

336 http://digitalconstitution.com/wp-content/uploads/2014/11/government-warrant.pdf

Microsoft reveló los datos de tráfico que se encontraban en territorio de los EE.UU, no obstante, se negó a revelar datos de contenido argumentando que las autoridades de los EE.UU. no podían exigirle la entrega de datos almacenados en Irlanda sin hacer uso del Tratado de Asistencia Legal Mutua (MLAT) existente entre Irlanda y los EE.UU. Se trataba de una orden extraterritorial, pues el registro en cuestión se produciría en Irlanda.

Microsoft ha argumentado que el uso unilateral de las autoridades de los EE.UU. de una orden de registro para obtener un correo electrónico que se encuentra en otro país pone en riesgo la privacidad y las relaciones internacionales cordiales en riesgo. Microsoft ha perdido en primera y segunda instancia, ahora corresponde a la Corte Suprema establecer el justo equilibrio.

En el caso se debaten principalmente dos cuestiones 1) si existe un registro extraterritorial o no 2) si en ECPA permite la realización de registros extraterritoriales.

Para Microsoft, existiría un registro extraterritorial por parte de los EE.UU. en territorio irlandés. Tal registro no podría ampararse en ECPA, ya que existe una presunción de que la norma no se aplica extraterritorialmente. En contraste, la

sentencia condenatoria contra Microsoft por parte de la Corte de Nueva York apunta lo siguiente:[337]

- **La búsqueda se produce en el territorio de los EE.UU:** El magistrado argumenta, citando a ORIN, que En el contexto de la información digital, tal y como señala ORIN *"una búsqueda ocurre cuando la información o los datos son expuestos a posibles observaciones humanas, tal y como cuando aparece en una pantalla en vez de cuando es copiada por el disco duro o procesada por un el ordenador"* En el presente caso, en la opinión de la Corte, la exposición no tiene lugar hasta que la información es revisada en los EE.UU. En consecuencia, no existe una búsqueda extraterritorial.

- **ECPA no excluye los efectos extraterritoriales:** La exposición de motivos de la Stored Communications Act (SCA)[338] establece que no se aplican al mundo digital las clásicas protecciones que aplican a las órdenes de búsqueda y captura en un domicilio. En tal virtud, se establece un modelo de orden de registro que se ejecuta como una citación, es decir, que se entrega al proveedor de servicios de Internet directamente, y no implica que las fuerzas y cuerpos de seguridad del Estado tengan que acudir físicamente a hacer la

[337] MEMORAMDUM AND ORDER (D. NY.2015). Disponible en: http://digitalconstitution.com/wp-content/uploads/2014/09/Magistrate-Judge.pdf

[338] Título con el que se codificó ECPA en el U.S Code.

> búsqueda y captura por ellos mismos a un data center. Ha sido la ley desde hace mucho tiempo que este tipo de órdenes requieren al destinatario producir la información en posesión, custodia o control, con independencia de la ubicación de la información. Nada en el texto de ECPA establece una excepción para los registros almacenados en el extranjero.[339]

El magistrado trae a colación un número de problemas con el argumento esgrimido por Microsoft[340]:

- El proveedor no verifica la información de residencia del usuario.

- El sujeto intentado cometer una actividad criminal podría, fácilmente falsear su residencia para que se le asigne un servidor fuera de los Estados Unidos con el objeto de evadir órdenes de registro SCA.

- Si una orden de registro SCA fuera ejecutada como una orden de registro tradicional, la única vía para su ejecución en el extranjero sería la asistencia judicial (MLATs).

[339] MEMORAMDUM AND ORDER (D. NY.2015). Disponible en: http://digitalconstitution.com/wp-content/uploads/2014/09/Magistrate-Judge.pdf p.14.

[340] MEMORAMDUM AND ORDER (D. NY.2015). Disponible en: http://digitalconstitution.com/wp-content/uploads/2014/09/Magistrate-Judge.pdf p.14.

De esta forma, la Corte estableció que incluso cuando ECPA se aplica a datos almacenados fuera del territorio de los EE.U, la orden de registro que recae sobre esos datos no viola la presunción de que la ley de los EE.UU no aplica extraterritorialmente.[341]

[341] MEMORAMDUM AND ORDER (D. NY.2015). Disponible en: http://digitalconstitution.com/wp-content/uploads/2014/09/Magistrate-Judge.pdf, p.26.

8. CAPÍTULO VII: GESTIÓN DE LOS RIESGOS DE SEGURIDAD

A diferencia de las disparidades existentes en el ámbito de la privacidad, en el ámbito de la seguridad de la información sí que existe un acuerdo pacífico, apoyado en estándares internacionales sobre cuáles son sus objetivos:[342] confidencialidad, integridad y disponibilidad. Curiosamente, también existe en la industria consenso sobre una premisa fundamental: La seguridad al cien por cien no existe, ningún sistema u organización (pública o privada), resulta completamente inmune ante ataques, fallos, desastres y otras amenazas físicas y cibernéticas. La clave de la gestión de riesgos en este ámbito reside en aplicar las medidas y controles adecuados para proteger los activos de información, a la luz del estado de la ciencia y de la técnica.

Los ciberataques y los incidentes relacionados la seguridad han experimentado un crecimiento frenético en los últimos años. La motivación de los atacantes ha pasado de ser la notoriedad y el reconocimiento público, a la obtención de grandes sumas de dinero a través del apoderamiento de registros, de propiedad intelectual y de la I+ D de las organizaciones. Por otro lado, el acceso gubernamental ilegal (con fines de

[342] En este sentido, véase: KATSIKAS, Sokratis K, BACKES, Michael: "Information security: 9th international conference, ISC 2006, Samos Island, Greece, August 30-September 2, 2006: proceedings". Berlín, 2006, p. 531.

inteligencia,[343] seguridad nacional y cualesquiera otros fines) también forma parte del de ecosistema de ciberamenazas en un mundo hiperconectado. Desde la perspectiva económica, los costes de un incidente de seguridad pueden ser altos; según un estudio de *Ponemon Institute*, el coste por cada registro de cliente oscila entre 58 y 250 euros,[344]dependiendo del sector afectado. Por su parte, Sony atribuyó unos costes de 132 millones de euros a los ataques a su red de PlayStation en 2011, los cuales pusieron en peligro los datos personales de alrededor 100 millones de clientes.[345] En términos globales, un país como el Reino Unido estima que la delincuencia le cuesta unos 33 mil millones de euros al año.[346] Esta cifra es más importante que la del PIB de países como Honduras[347] o Paraguay.[348]

La seguridad de la información constituye una de las piezas centrales de la contratación de servicios de Cloud Computing.

En la fase precontractual, se deben determinar una serie de requisitos de seguridad basado en una análisis de riesgos,[349] para luego hacer un examen de cómo

[343] Vid. Capítulo IV

[344] http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html

[345] http://www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/

[346] UNITED KINGDOM, Cyber Security Strategy: "Protecting and promoting the UK in a digital world", Londres, 2011.

[347] http://www.datosmacro.com/pib/honduras

[348] http://www.datosmacro.com/pib/paraguay

[349] En este sentido, véase la "Metodología para análisis de Riesgos en el Cloud Computing de la Agencia Europea de Seguridad y Redes de ENISA, 2009. Disponible en:

determinado proveedor de servicios si el proveedor o proveedores de servicios los cumple, o no. En particular, el proceso de toma de decisión en materia de seguridad debe implicar al menos tres preguntas (i) ¿Qué nivel seguridad requieren los activos de información que serán tratados en servicios de Cloud, en función de su valor para el negocio, y de los requerimiento legales aplicables (ii) ¿Qué nivel de seguridad (controles, tecnologías, estándares) se proporciona a esos activos antes de ser llevados a la nube? (iii) ¿Qué nivel de seguridad se garantiza y se demuestra por parte del proveedor?. Sólo si la ecuación resultante indica que los datos tendrán un nivel igual o mayor de seguridad la nube será un buen lugar para los datos corporativos.

Por un lado, la utilización de servicios de Cloud Computing implica que un tercero procesa en su infraestructura información muy valiosa para la organización y sobre la que recaen numerosas obligaciones cuyo cumplimiento atañe al cliente de Cloud; por otro lado, los proveedores de Cloud Computing tienen la capacidad de generar economías de escala muy significativas, que permiten desplegar recursos, desarrollar tecnologías competencias y capacidades en materia de seguridad que resultan inalcanzables para la mayoría de las organizaciones. Compañías como Amazon, Microsoft o Google tienen entre sus filas varios de los mejor ingenieros de seguridad del mundo.[350]Asimismo, la concentración de sistemas de computación en la nube

https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/view

[350] http://bits.blogs.nytimes.com/2014/12/02/computing-goes-to-the-cloud-so-does-crime/

implica que los servidores son susceptibles teóricamente de estar gobernados por una mayor uniformidad, facilitando una mejor gestión, las alertas de seguridad pueden ser resueltas más rápido, y los dispositivos que acceden a los datos pueden ser inspeccionados de un modo más uniforme[351].

8.1. La responsabilidad ante incidentes de seguridad de la información

Resulta imprescindible delimitar contractualmente los criterios para determinar la responsabilidad del proveedor que custodia los datos, ante incidentes que vulneren la seguridad de los datos. En caso de contratos sometidos a legislación de sistema anglosajón, son habituales las limitaciones de responsabilidad de los prestadores de servicio y, en particular, la determinación de una cantidad económica máxima. No obstante, dichas previsiones son contrarias a las legislaciones del sistema continental, como la nuestra, en la que la responsabilidad será determinada por parámetros como la culpa o negligencia del proveedor,[352] en el marco del incidente. Determinar la existencia de negligencia es una cuestión compleja. No existe jurisprudencia que sirva como referente en la industria para configurarla en el marco

[351] MICROSOFT: "The Economics of the Cloud", 2010. Disponible en: http://www.microsoft.com/en-us/download/details.aspx?id=5166
[352] CSA-ES ISMS Forum: "Cloud Compliance Report", 2011 p. 93.

de un incidente de seguridad. Ahora bien, el concepto viene ligado a lo que se considera **objetivamente razonable**. En este sentido, parece razonable que lo que se exija sea la perfecta aplicación de las medidas, controles y estándares pactados en el contrato, y que constituyan estos el marco de actuación que eventualmente pueda utilizarse para determinar la culpa o negligencia del proveedor. Evidentemente, el usuario deberá poder valorar *ex ante* si este marco le parece **objetivamente razonable**. Esta aproximación implica que se compartan los riesgos y las responsabilidades en el tratamiento de los datos. Otra aproximación implicaría que el proveedor asumiera una responsabilidad ilimitada, si esto ocurriera en el marco de la relación a sus cientos o miles de cliente, probablemente su beneficio tendería a desaparecer.

8.2. El cumplimiento en materia de seguridad de la información

En lo relativo a los datos de carácter personal, la Directiva 95/46/CE prevé la plena responsabilidad del responsables del tratamiento[353] en la elección de encargados del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnicas y organizativas de los tratamientos que deban efectuarse por el encargado, así como para asegurarse de dichas medidas son llevadas a la práctica.

[353] El artículo 17, apartado 2.

En España, el RLOPD establece un listado de medidas de seguridad mínimas a aplicar a en función de los datos que se traten. No obstante, estás medidas pueden resultar insuficientes para la protección efectiva de los datos contra las amenazas en el ciberespacio, por ejemplo, no se contempla el cifrado de los datos cuando se encuentran en estado de almacenamiento, no se contemplan los mecanismos de autenticación fuerte.

El nivel de seguridad y los controles a aplicar en los servicios de Cloud Computing, dependerá de la información que se vea involucrada en los mismos. Por ejemplo, si un servicio IaaS se utiliza para alojar una página web cuyo contenido está destinado a ser públicamente accesible, el requisito de la disponibilidad prevalecerá sobre el de confidencialidad, por tanto, se prestará especial a las garantías de continuidad que aseguren que el servicio siempre estará disponible y que tendrá capacidad para absorber picos de demanda. Si un servicio SaaS se utiliza para tratar datos relativos a recursos humanos, la confidencialidad será el aspecto principal a tener en cuenta por los que habrá que valorar las medidas contra ataques maliciosos tales como el control de acceso y el cifrado, entre otras.

A continuación se describen los estándares de referencia en seguridad y privacidad en la actualidad, a cuyo cumplimiento se recomienda someter los servicios de Cloud Computing contratados.

8.3. Los estándares de referencia en seguridad de la información

8.3.1. ISO 27001:2013

El estándar ISO/IEC 27001:2013 [354] es el estándar por excelencia a nivel mundial en materia de seguridad de la información. La norma especifica los requisitos que debe tener un Sistema de Gestión de la Seguridad de la Información (SGSI) en cuanto a su establecimiento, implantación, mantenimiento y mejora continua, con arreglo al "Ciclo de Deming" o compuesto por cuatro fases: Plan, Do, Check, Act (PDCA).

A la luz de ISO 27001, resulta imprescindible que exista un gobierno y coordinación de la seguridad de la información en la organización y un compromiso por parte de la Alta Dirección para con esta. Asimismo, se debe garantizar que los riesgos se identifican, se analizan y se gestionan, con arreglo al ciclo PDCA para conseguir el objetivo de mejora continua.

Su implementación debe ir necesariamente acompañada de la implementación de los controles específicos contenidos estándar ISO/IEC 27002, los cuales se incorporan además como "ANEXO A" a la propia norma ISO/IEC 27001.

[354] Aprobado y publicado en octubre de 2005 y actualizado en 2013 por la ISO (International Organization for Standardization y por la comisión International Electrotechnical Commission).

8.3.2. ISO/IEC 27002:2013

ISO/IEC 27002 proporciona recomendaciones sobre las mejores prácticas en la gestión de la seguridad de la información, que se definen en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)"[355]. La norma contempla 35 "Objetivos de control" sobre la seguridad y 114 "Controles" específicos para alcanzar estos objetivos. Dichos objetivos se agrupan bajo los siguientes dominios o áreas:

- Políticas de seguridad.
- Aspectos organizativos de la seguridad de la información.
- Seguridad ligada a los recursos humanos
- Gestión de activos
- Control de accesos.
- Cifrado.
- Seguridad física y ambiental.

[355] ISO/IEC 27002:2013.

- Seguridad en la operativa. Seguridad en las telecomunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relaciones con proveedores.
- Gestión de incidentes en la seguridad de la información.
- Gestión de la continuidad del negocio.
- Cumplimiento normativo.

La norma ISO/IEC 27002 es una guía de buenas prácticas y no es certificable *per se*, no obstante, sus controles se pueden incorporar dentro del Sistema de Gestión de la Seguridad de la Información gobernado por ISO/IEC ISO 27001, que sí es certificable.

8.3.3. ISO/IEC 27018:2014

ISO/IEC 27018:2014 es el primer estándar internacional en materia de privacidad en Cloud Computing. Establece un marco comúnmente aceptado de objetivos de control, controles y directrices para la protección de información personal en el ámbito de la nube pública. En particular, la norma se basa en el estándar ISO/IEC 27002, teniendo en cuenta los requisitos normativos en materia de privacidad que podrían ser aplicable en el entorno de la nube pública.[356] Si bien las leyes y

[356] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498

reglamentos de privacidad varían en torno a diferentes jurisdicciones, los principios establecidos en ISO/IEC 27018 son prácticamente universales.

8.4. Objetivos de seguridad y controles a incluir

El modo de entrega de los servicios en la nube creará numerosos perímetros virtuales, así como un modelo de seguridad con responsabilidades compartidas entre el cliente y el proveedor de servicios en la nube.[357] Los objetivos de seguridad a cubrirse en el marco contractual deberían ser, al menos, los siguientes:

- Separación lógica de la información o isolación
- Cifrado.
- Identificación y autenticación.
- Borrado de la información y garantía de irrecuperabilidad.
- Estándares a implementar.
- Seguridad física y de los equipos.
- Disponibilidad del servicio.
- Planes de continuidad de negocio.
- Respuesta ante incidentes.
- Seguridad de las redes.

[357] MATHER Tim, KUMARASWAMY Subra, SHAHED Latif: "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance". California, 2009, p.7, 109.

- Copias de seguridad y pruebas recuperación.
- Seguridad en el desarrollo de aplicaciones.
- Notificación de las posibles brechas de seguridad.
- Auditoría de seguridad.
- Análisis de riesgos periódicos.

La implementación de estos objetivos de seguridad en la nube tiene ciertas particularidades. 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 se traten con fines ilegítimos, el aislamiento también depende de medidas técnicas tales como el *hardening* de los hipervisores y la correcta gestión de los recursos comunes si se utilizan máquinas virtuales para compartir recursos físicos entre diferentes clientes. Sobre las particularidades de la nube en materia de seguridad, ISO se encuentra desarrollando un estándar específico, la norma ISO/IEC 27017.

En relación con las protecciones a través de mecanismos criptográficos, el cifrado robusto, en reposo y en tránsito, puede contribuir de forma significativa a prevenir los accesos no autorizados datos personales. Los factores que afectan a la seguridad de los datos cifrados incluyen la fortaleza del algoritmo, así como la longitud de la

llave utilizada, generalmente las llaves más largas son las más seguras.[358] Otros factores que afectan la seguridad en el cifrado es la gestión de las claves, cómo se almacenan y el control de las llaves de cifrado o quién tiene acceso dichas llaves para descifrar la información. Si bien el cifrado en los servicios de cloud es posible tanto en tránsito como el reposo, el control sobre las llaves del mismo con frecuencia depende del tipo de servicio del que se trate. En IaaS el cliente recibe un servicio de mero de los almacenamiento en una infraestructura que un tercero opera y protege, en SaaS, en cambio, el cliente recibe un servicio que requieren un procesamiento activo esos datos (p. ej. una aplicación de RRHH) para lo cual un algoritmo o sistema debe entender los datos para filtrar el spam, separar correos prioritarios, etc. Si las llaves se controlan exclusivamente por el cliente de forma que los sistemas del proveedor no tiene acceso inteligible a los datos, estas funcionalidades normalmente no son posibles.

Según Verizon, en 2014 hubo más de 7 millones de vulnerabilidades explotadas y a autenticación sigue siendo el eslabón más débil en la cadena de seguridad. Por ejemplo, en el incidente de seguridad que afectó a JP Morgan en 2014, los hacker penetraron en 90 servidores, ganado privilegios de administrador de alto nivel, afectando 76 millones de hogares y 7 millones de pequeñas empresas.[359] El ataque se

[358] En este sentido puede consultarse HON W. Kuan, MILLARD Christopher: "Control, Security, and Risk in the Cloud" Cloud Computing Law. Oxford, 2013. p.19.

[359] http://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm

podría haber prevenido con la implementación de dos factores en uno de los servidores de red de, dejándolo vulnerable a ataques.[360]Por tanto, es importante que se garantice la utilización de mecanismos de doble factor de autenticación en las distintas capas del servicio.[361]

[360] http://www.esecurityplanet.com/network-security/entry-point-identified-for-jpmorgan-chase-breach.html

[361] http://www.slideshare.net/VerizonEnterpriseSolutions/data-breachinvestigationsreport2015

8.5. Protecciones equivalentes

En el marco de los servicios cloud es recomendable el establecimiento de un marco contractual uniforme, en virtud del cual se garantice la protección efectiva de los datos, tanto desde la perspectiva técnica como jurídica, con independencia de su ubicación.

Las Cláusulas Contractuales Tipo y Privacy Level Agreement de la Cloud Security Alliance son importantes modelos contractuales de referencia en este sentido, obstante, a efectos del cumplimiento de la normativa europea de protección de datos, sólo las Cláusulas Contractuales Tipo cuentan actualmente con el respaldo formal de la Comisión de la Unión Europea.

En relación con las protecciones jurídicas, los responsable del tratamiento europeos deben garantizar que tratan los datos se tratan de conformidad con los requerimientos de las leyes y principios europeos, y que dichos requerimientos deben ser de obligado cumplimiento para los proveedores por vía contractual con independencia de su ubicación.

Se ha propuesto la elaboración de códigos de conducta para proveedores de servicios de cloud preparado por la comisión en colaboración con varios actores de la

industria en la forma de Cloud Select Industry Group (C-SIG), el proyecto de código se ha sometido a la aprobación por parte del Grupo de Trabajo del Art. 29.[362]

[362] https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

9. CONCLUSIONES

De lo expuesto anteriormente, se pueden extraer las siguientes conclusiones:

1. El Cloud Computing forma parte de la realidad tecnológica en la que vivimos y será el protagonista del contexto informático corporativo, educativo y gubernamental en los próximos años. Los movimientos internacionales de datos forman, sin duda, parte de esta realidad tecnológica.

2. En la actualidad, el mundo carece de un marco global de privacidad vinculante e interoperable que aborde los movimientos internacionales de datos respondiendo al estado tecnológico actual y dando la certeza jurídica necesaria a los distintos actores del Cloud Computing en el ámbito B2B. Es necesaria la creación de un marco normativo neutral que, partiendo de la premisa de que los flujos internacionales son la regla y no la excepción, fije los principios básicos para la protección adecuada y uniforme de los datos y de los derechos de sus titulares con independencia de la ubicación de aquellos. Esto permitiría conciliar la innovación y la competitividad con la privacidad y la protección de los datos de los ciudadanos.

3. Las restricciones a los movimientos internacionales de datos son el principal reto jurídico al que se enfrenta el Cloud Computing en Europa. El modelo proyectado tanto por el Convenio 108, como por la Directiva 95/46/CE no resulta compatible con Internet y con un mundo digitalizado e hiperconectado. Reguladores y *policy makers* europeos han hecho un esfuerzo plausible que se ha materializado en la elaboración de herramientas encaminadas a minimizar el impacto de la obsolescencia normativa en la economía digital, así, instrumentos como Safe Harbor, las Cláusulas Contractuales Tipo y las guías del Grupo de Trabajo del Art. 29 han permitido cierto despegue del Cloud en Europa, no obstante, existe un fragmentación en la interpretación y aplicación de estas herramientas por parte de las distintas autoridades de control de los Estados Miembros, a la par que complejidades y carga burocráticas cuyo beneficio para la privacidad es incierto que impiden que los servicios en la nube alcancen todo su potencial en Europa. El Nuevo Reglamento Europeo de Protección de Datos en vías de aprobación podría corregir esta situación estableciendo un régimen uniforme en la región, adaptado a la realidad tecnológica actual y que garantice la protección efectiva de los derechos de los residentes europeos con relación a sus datos con independencia de la ubicación de los mismos. Este enfoque es sin duda el acertado, y estaría en armonía con el concepto de protección de datos, que como bien señala HUSTINX: no fue diseñado para limitar el uso de las

tecnologías de la información *per se*, sino para proporcionar garantías cuando las tecnologías de información se utilizan para el procesamiento de la información concerniente a los individuos,[363] opinión que suscribimos totalmentente.

4. Las preocupaciones relacionadas con los movimientos internacionales de datos se basan con frecuencia en percepciones sobre este fenómeno en contraposición a la localización de datos, más que en hechos demostrables desde la perspectivas jurídica y de seguridad. En tal virtud debemos puntualizar lo siguiente:

    a. La localización geográfica forzada de datos *per se* no equivale, ni garantiza, el cumplimiento normativo de las obligaciones que recaen sobre los mismos.

    b. La ubicación geográfica no representa una protección contra el acceso ilegal por parte de actores maliciosos en el ciberespacio, incluidos gobiernos. En un mundo digitalizado e hiperconectado, la protección contra las amenazas cibernéticas se procura a través de la aplicación de

[363] HUSTINX, Peter, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2014. Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf

medidas técnicas y organizativas adecuadas. Los ataques cibernéticos pueden iniciarse en cualquier lugar del mundo donde exista una conexión a Internet, y pueden dirigirse a cualquier infraestructura o componente conectado a la Red, con independencia de su ubicación.

c. La localización geográfica tampoco constituye una defensa frente a los poderes de investigación de las autoridades gubernamentales con relación a los datos en el ámbito criminal. Aunque los ordenamientos jurídicos de los Estados democráticos avanzados pueden diferir en su enfoque, estos contemplan poderes similares de acceso a la información tratada en servicios como el Cloud Computing en el ámbito de la justicia criminal y de la seguridad nacional, incluido el acceso transfronterizo. La existencia de tratados de asistencia judicial en materia penal hacen que la ubicación física de los datos sea una barrera mucho menos significativa para el acceso de las autoridades a la información en el marco de la investigación de actividades delictivas. Asimismo, existe un número de tratados internacionales específicos (p.ej. contra la delincuencia organizada, el blanqueo de capitales, la lucha contra el terrorismo y el tráfico de estupefacientes, entre otros) ratificados por buena parte de las democracias alrededor del mundo,

que fomentan el intercambio de información entre los Estados en este ámbito.

5. La inexistencia de una regulación homogénea en materia de privacidad, seguridad y movimientos internacionales de datos hace que resulte fundamental (i) la identificación y valoración de los riesgos de privacidad y seguridad en la fase pre- contractual (ii) el aseguramiento por vía contractual de las protecciones adecuadas aplicables a los datos, en particular:

    a. Con independencia de la ley aplicable y la jurisdicción competente a las que las partes tengan a bien adoptar y acogerse, respectivamente, a efectos de la relación mercantil, en lo relativo al tratamiento de datos de carácter personal, en principio es recomendable pactar la aplicación de la ley que corresponde a la ubicación del cliente de Cloud o responsable del tratamiento, de cara a facilitar el cumplimiento normativo, así como la eventual defensa de los derechos parte de los interesados o titulares de los datos y la supervisión por parte de sus autoridades competentes. Esta recomendación debe ser valorada cuidadosamente, pues aunque resulta razonable y práctica en regiones o países con un régimen de protección garantista p.ej. dentro del Espacio Económico Europeo, si el cliente de Cloud Computing se

encuentra establecido en países donde donde no funciona el Estado de Derecho, y no se garantizan los valores democráticos y el derecho a la privacidad, respectivamente, probablemente se deba valorar el sometimiento a una ley extranjera, en la medida de lo posible.

b. Dado que en materia penal la jurisdicción no puede ser en modo alguno determinada por las partes con carácter *ex ante*, el cliente contratante de de servicios de Cloud Computing deberá determinar qué protecciones en cuanto al debido proceso aplicarían a una investigación sobre datos tratados mediante Servicios de Cloud Computing en función del lugar de su propio establecimiento establecimiento y el de su proveedor (p.ej. el requerimiento de una orden judicial, la protección del secreto de las comunicaciones y la confidencialidad de los datos almacenados, entre otras). Si el lugar del establecimiento de las partes es distinto, el cliente deberá compararlas las protecciones jurídicas que ofrecen su propio ordenamiento frente al del proveedores, incluidos los posible acuerdos bilaterales o multilaterales existentes, con el objeto de hacer una valoración jurídica de los riesgos.

c. La protecciones contractuales deben cubrir, como mínimo, los requerimientos normativos aplicables al cliente de Cloud Computing en función de su lugar de establecimiento, de su actividad de negocio, o de los tratamientos concretos que pretenda realizar mediante servicios de Cloud Computing. No obstante, el cumplimiento normativo no implica necesariamente la protección efectiva de la información contra las amenazas en el ciberespacio. La protección de la información requieres de medidas adecuadas a la luz del estado de la ciencia y de la técnica en cada momento, más allá de los requerimientos mínimos impuestos por el legislador. En la actualidad, el cifrado robusto, la autenticación de doble factor, así como la realización de ciberejercicios para probar la robustez y resiliencia de los servicios de Cloud Computing, entre otras que se han señalado en la presente Tesis Doctoral, resultan imprescindibles.

6. En relación con el acceso gubernamental a la información, no cabe duda de que los Estados tienen la obligación positiva de proteger a sus ciudadanos frente al crimen y que la posibilidad de acceso a los datos gestionados en servicios de Cloud Computing con arreglo a la ley es necesario. La aparición nuevas formas de criminalidad y amenazas terroristas que usan el ciberespacio y potencialmente servicios de Cloud Computing para operar nos

recuerdan los restos a los que las autoridades se enfrentan. No obstante, debe existir un equilibrio que permita reconciliar la necesidad del Estado de protegerse y de proteger a sus ciudadanos frente al crimen, con la privacidad y los valores democráticos. España, Reino Unido y los EE.UU establecen una serie de poderes de investigación por parte de las autoridades y de protecciones y garantías equivalentes en el ámbito de la aplicación forzosa de la ley. No obstante, en materia de seguridad nacional si bien el régimen de EE.UU y el Reino Unido resultan comparables, resulta difícil hacer una comparación con el régimen español, pues éste último no regula con detalle los poderes y limitaciones del Centro Nacional de Inteligencia, restringiéndose a encomendarle la "obtención de señales" y estableciendo un régimen de supervisión judicial, una mayor transparencia en relación con los poderes de investigación que se le otorgan y las limitaciones a los mismos contribuiría a la ponderación de estas actividades.

7. Las revelaciones por parte de Snowden en el año 2013 hicieron patente la necesidad de garantizar por parte de los Estados la sujeción de sus autoridades de seguridad e inteligencia al imperio de la ley, cuya interpretación debe estar preestablecida, así como y de la transparencia de estas normas y de la sujeción a mecanismos de supervisión independiente que sean efectivos. La exigencia de asegurar el sometimiento de las actividades de

inteligencia alrededor del mundo no es una cuestión nueva. Los servicios de inteligencia, en cierta medida, han operado siempre al margen de la ley. No obstante el poder de Internet y el aumento de las capacidades de cómputo, hacen que los riesgos injerencias en privacidad y los derechos fundamentales derechos los individuos sean mayores.

8. Existe un foco legítimo de preocupación sobre cómo se establece este equilibrio por parte de los Estados Unidos, en un mercado digital global donde proveedores estadounidenses, sometidos a las normas estadounidense dominan. La aprobación de "Freedom Act" ha constituido un importante paso por su parte en este sentido, al prohibir expresamente la recolección masiva de datos por parte de las autoridades gubernamentales. Por otro lado, la eventual aprobación del proyecto de "Judicial Redress Act", que establecería el derecho de los países europeos (en calidad de aliados designados) a obtener tutela judicial y resarcimiento frente el mal uso de sus datos por parte de las agencias gubernamentales sería un paso clave en la dirección correcta. No obstante, es imprescindible que se garantice la correcta aplicación del ordenamiento jurídico y de los mecanismos de supervisión, solo esto restablecerá la confianza en los intercambios de datos trasatlánticos, y de la confianza de sus aliados, incluida Europa. Los compromisos por parte de los

gobiernos europeos, y de otros alrededor del mundo en esta dirección también es necesario.

9. Algo que se percibe como la pérdida de soberanía por los Estados que ven limitada su hacer cumplir la ley penal sobre sus propios ciudadanos dentro de su propio territorio son razones pueden motivar la fragmentación de Internet y destruir las economías de escala (p. ej. requiriendo la localización forzada) por ello, a nuestro juicio deben revisarse los mecanismos de cooperación internacional existentes, y darles celeridad de forma que las diligencias se ejecuten en menor tiempo y que no entorpezcan la investigación. En concreto, para la consecución de este objetivo se recomienda utilización de medios electrónicos, la digitalización de los procedimientos, la incorporación de plantillas únicas para llevar a cabo las solicitudes, y la reducción de las partes involucradas en la recepción y ejecución de las diligencias. También se recomienda la incorporación de elementos de extraterritorialidad en las leyes nacionales bajo fórmulas como las que han utilizado Brasil y el Reino Unido, amparadas en el principio de la nacionalidad y otros criterios de interés legítimo, bajo los que el territorio donde se encuentra almacenada la evidencia es irrelevante; así como su correcto encaje en los principios de Derecho Internacional que rigen la jurisdicción en Internet.

10. Las reglas aplicables al ejercicio de la jurisdicción en el ámbito del Cloud Computing deben fijarse en el marco de un consenso político y jurídico internacional. Ese consenso debe responder a los los valores democráticos y del debido proceso y reconocer la realidad tecnológica en que vivimos, en la que el territorio es cada vez menos relevante. Con relación al ejercicio de la jurisdicción con efectos extraterritoriales, deben garantizarse el debido proceso y tutela efectiva para los investigados (con independencia de su nacionalidad), asimismo debe modularse valor de la evidencia obtenida directamente por los Estados sin hacer uso de un MLAT, cuando el MLAT es requerido.

10. GLOSARIO DE TÉRMINOS

Protección de datos[364]

1. **Afectado o interesado o titular de los datos:** persona física titular de los datos que sean objeto del tratamiento.

2. **Autenticación:** procedimiento de comprobación de la identidad de un usuario.

3. **Cesión o comunicación de datos:** tratamiento de datos que supone su revelación a una persona distinta del interesado.

4. **Copia de respaldo:** copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

5. **Datos de carácter personal:** cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

6. **Destinatario o cesionario:** la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos .En el caso de entes sin

[364] De conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD).

personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará destinatario a la persona o personas integrantes de los mismos.

7. **Encargado del tratamiento:** la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará encargado del tratamiento a la persona o personas integrantes de los mismos.

8. **Exportador de datos personales:** la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español y responsable del tratamiento de los datos de carácter personal que son objeto de transferencia internacional a un país tercero.

9. **Importador de datos personales:** la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

10. **Tratamiento de datos:** cualquier operación o procedimiento técnico, sea o no automatizado, que implique la recogida, grabación, conservación, elaboración,

modificación, consulta, utilización, bloqueo, modificación, o cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

11. **Responsable del fichero o del tratamiento:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará responsable del tratamiento a la persona o personas integrantes de los mismos.

12. **Usuario:** sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

13. **Tercero:** persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará tercero a la persona o personas integrantes de los mismos.

14. **Transferencia internacional de datos a países terceros:** tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo , bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

Cloud Computing

15. **Clúster:** Conjunto de servidores que trabajan como una única máquina mejorando el desempeño de las transacciones y operaciones implementadas en este sistema.

16. **Centro de datos:** Centros de Procesamiento de Datos, ubicación física donde se concentran todos los equipos electrónicos necesarios para el procesamiento de la información de una organización.

17. **On-premise:** Modelo referido al esquema tradicional de licenciamiento, es decir la empresa adquiere las licencias que le otorgan derecho de uso de los sistemas del proveedor, los integra en sus propias instalaciones y mantiene sus datos dentro de su propia infraestructura de tecnología.

18. **SLA:** “Service Level Agreement” o “Acuerdo de Nivel de Servicio”. Es un protocolo plasmado normalmente en un documento de carácter legal por el

que una compañía que presta un servicio a otra se compromete a hacerlo bajo determinadas condiciones y con unas prestaciones mínimas.

19. **TI o IT:** Tecnologías de la Información.

20. **TIC o ICT:** Tecnologías de la Información y la Comunicación.

21. **Virtualización:** Es el concepto que describe cómo en un solo computador físico se coordina el uso de los recursos para que varios sistemas operativos puedan funcionar al mismo tiempo de forma independiente y sin que ellos (los SO) sepan que están compartiendo recursos con otros sistemas operativos.

11. BIBLIOGRAFÍA[365]

- AARONSON, Susan: "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security". APSA 2014 Annual Meeting Paper. Disponible en SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2453025

- AGUILAR, Mariano: "Comisiones rogatorias y obtención de pruebas en el extranjero". Boletín del Ministerio de Justicia, ISSN-e 0211-4267, Año 55, Nº 1905. Madrid, 2001.

- ARENAS RAMIRO, Mónica: "El Derecho Fundamental a la Protección de Datos en Europa". Tirant Lo Blanche. Valencia, 2006.

- ARTICLE 29 DATA PROTECTION WORKING PARTY: "Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules". Bruselas, 2012. Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

- ARTICLE 29 DATA PROTECTION WORKING PARTY: "Explanatory Document on the Processor Binding Corporate Rules". Bruselas, 2013 (rev. 2015). Disponible en:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf

- ASCENSIO, Hervé: "Extraterritoriality as an instrument". Contribution to the work of the UN Secretary-General's Special Representative on human rights and transnational corporations and other businesses. Paris, 2010. Disponible en: http://www.univ-paris1.fr/fileadmin/IREDIES/Contributions_en_ligne/H._ASCENSIO/Extraterritoriality__Human_Rights_and_Business_Entreprises.pdf

- BERMÚDEZ J.A.: "Aspectos Procesales de la Investigación de la Criminalidad Informática". Escuela Judicial Española, Madrid, 2009.

[365] Los enlaces referenciados en las siguientes páginas fueron accedidos por última vez por la autora en noviembre de 2015.

- BORTNICK, Jane: "International Data Flows Issues". Issue brief number IB81040. Washington, 1982 (rev.1983). Disponible en: http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=577604

- CHANDER, Anupam y LE, Uyen P.: "Breaking the Web: Data Localization vs. the Global Internet". Emory Law Journal, Forthcoming; UC Davis Legal Studies Research Paper No. 378. EE.UU., 2014. Disponible en SSRN: http://ssrn.com/abstract=2407858

- CLOUD SECURITY ALLIANCE: "Guía para la seguridad en áreas críticas de atención en Cloud Computing" traducida al castellano por ISMS Forum Spain. Madrid, 2009. Disponible en: https://cloudsecurityalliance.org/guidance/csaguide-es.v2.pdf

- COHN, Cindy. REITMAN, Rainey: "USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here" EFF, San Francisco, 2015. https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here

- COVINGTON & BURLING: "The USA PATRIOT Act and the Use of Cloud Services: Q&A. Disponible en: http://www.insideprivacy.com/PatriotActQA.pdf

- CYBERCRIME CONVENTION COMMITTEE (T-CY): "Transborder access to data and jurisdiction: Options for further action by the T-CY". Estrasburgo, 2013. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)28_Plen10AbrRep_V3.pdf

- CYBERCRIME CONVENTION COMMITTEE (T-CY): "Transborder access to data and jurisdiction: Options for further action by the T-CY". Estrasburgo, 2014. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pd

- DOYLE, Charles: "Privacy: An Overview of the Electronic Communications Privacy Act" Congressional Research Service. 2012. Disponible en: https://www.fas.org/sgp/crs/misc/R41733.pdf

- DLA Piper: "Data Protection Laws of the World". 2013. Disponible en: http://dlapiperdataprotection.com/

- DE SCHRIJVER, S. and DAENENS T: "The Yahoo! Case: The End of International Legal Assistance In Criminal Matters". Bruselas, 2013. Disponible en: http://whoswholegal.com/news/features/article/30840/yahoo-case-end-international-legal-assistance-criminal-matters

- EUROPEAN Commission: "Unleashing the Potential of Cloud Computing in Europe". Bruselas, 2012. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

- EUROPEAN Cloud Partnership Steering Board: "Establishing a Trusted Cloud Europe". Brussels 2014. Disponible en: https://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

- FISHMAN, William L.: "Introduction to transborder data flows". Reprinted from Stanford journal of international law. v. 16, Summer 1980. Citado por BORTNICK, Jane: "International Data Flows Issues". Issue brief number IB81040. Washington, 1982 (rev.1983). Disponible en: http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=577604

- FLORES PRADA, Ignacio "Criminalidad Informática aspectos sustantivos y procesales". Tirant Monografías 818, Valencia 2012.

- GARCIMARTIN ALFÉREZ, Francisco J.: "Sobre el fundamento de la cooperación jurídica internacional", Cooperación jurídica internacional, Colección Escuela Diplomática núm. 5, Madrid, 2001.

- GILIKER, Paula: "A Right to Personal Privacy the English Law of of Torts?". The Europeanisation of English Tort Law. Oxford, 2014.

- GHEMAWAT, S. GOBIOFF, H, and LEUNG, S.T: "The Google File System". 2003. Disponible en: http://static.googleusercontent.com/media/research.google.com/en//archive/gfs-sosp2003.pdf

- GOOGLE, Transparency Report https://www.google.com/transparencyreport/userdatarequests/legalprocess/

- GONZÁLEZ, R: "Diccionario de Computación y Electrónica". México D.F, 2004.

- GRINGAS, Clive: "UK Cloud Computing Interception - nothing new". Olswang, 2014. Disponible en: http://www.olswang.com/pdfs/CloudComputingInterception_CQG.pdf

- Harvard Research Draft Convention on Jurisdiction with respect to Crime, 1935.

- HON W. Kuan, MILLARD Christopher: "Control, Security, and Risk in the Cloud". Cloud Computing Law. Oxford, 2013.

- HON W. Kuan, MILLARD Christopher: "DATA EXPORT IN CLOUD COMPUTING – HOW CAN PERSONAL DATA BE TRANSFERRED OUTSIDE THE EEA? THE CLOUD OF UNKNOWING, PART 4", 2012. Disponible en: http://script-ed.org/wp-content/uploads/2012/04/hon.pdf

- HON, W. Kuan. MILLARD, Christopher. REED, Chris. SINGH, Jatinder. WALDEN, Ian. CROWCROFT, Jon: "Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Queen Mary School of Law Legal Studies Research Paper 191/2015. London, 2015. Disponible en SSRN: http://ssrn.com/abstract=2527951

- HUSTINX, Peter, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2014. Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf

- INTECO-CERT: "Riesgos y Amenazas en Cloud Computing". León, 2011.Disponible en: http://sie.fer.es/recursos/richImg/doc/14829/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

- ITU Yearbook of Statistics. Ginebra, 2014.

- JENNINGS, Robert. WATTS, Arthur, OPPENHEIM Lawrence: "Oppenheim's international law". Essex, 1992.

- JIMÉNEZ LÓPEZ, Raquel: "Convenios Bilaterales y de la Unión Europea con Terceros". Cooperación Judicial Penal en Europa. Madrid, 2013.

- KOHL, Uta: "Jurisdiction and the Internet: Regulatory Competence over Online Activity". Cambridge Univ. Press. Cambridge, 2007.

- KORFF, Douwe. V: "The rule of law on the Internet and in the wider digital world". Disponible en: http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/70114_Rule%20of%20Law%20on%20the%20Internet_web.pdf, Consejo de Europa, 2014.

- KUNER, Christopher: "Requiring local storage of Internet data will not protect privacy. Oxford University Press. Oxford, 2013.

- KUNER, Christopher "Transborder Data Flows and Data Privacy Law". United Kingdom, 2013.

- MARTINEZ, Ricard: "Derecho y Cloud Computing". Civitas, Madrid, 2012, p.34.

- MATHER Tim, KUMARASWAMY Subra, SHAHED Latif: "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance". California, 2009.

- MAXWELL, Winston. WOLF, Christopher: "A Global Reality: Governmental Access to Data in the Cloud". A Hogan Lovells White Paper. París, Washington, 2012. Disponible en: http://www.hoganlovells.com/files/Publication/80a807f2-e619-41dc-98e4-e6a7b5f6c5f8/Presentation/PublicationAttachment/9bab0ead-0b8b-4cdb-bb08-8ba1b95a9df9/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf

- MELL, Peter; GRANCE, Timothy: "THE NIST Definition of Cloud Computing". Gaithersburg, 2011. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

- MICROSOFT: "The Economics of the Cloud", 2010.

- MONTERO AROCA, J. : "La prueba en el proceso civil", Ed. Civitas, 5ª ed., Madrid 2007, p. 162. Citado por BELLIDO PENADÉS, R.: "La Prueba Ilícita y su control en el Proceso Civil". Revista Española de Derecho Constitucional ISSN: 0211-5743, núm. 89, mayo-agosto (2010).

- MICHAELS, Ralf: "Territorial Jurisdiction After Territoriality" en Globalisation and Jurisdiction" editado por SLOT, Pieter J. BULTERMAN, Mielle K. Kluwer Law International, Países Bajos 2004.

- McKinsey Global Institute: "Global flows in a digital age: How trade, finance, people, and data connect the world". 2014.

- NIST: "The NIST Definition of Cloud Computing". EE.UU, 2011.

- KATSIKAS, Sokratis K, BACKES, Michael: "Information security: 9th international conference, ISC 2006, Samos Island, Greece, August 30-September 2, 2006: proceedings". Berlín, 2006.

- ENISA: "Metodología para análisis de Riesgos en el Cloud Computing de la Agencia Europea de Seguridad y Redes. Heraklion, 2009. Disponible en: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/view

- MCNICHOLAS, Nicholas J.F: "The UK Electronic Communications Act". Publicado en A Decade of Research @the crossroads of law and ICT, Bruselas, 2001.

- MICHAELS, Ralf: "Territorial Jurisdiction After Territoriality" en Globalisation and Jurisdiction" editado por SLOT, Pieter J. BULTERMAN Mielle K. Kluwer Law International, Países Bajos, 2004.

- MORILLAS CUEVA, Lorenzo: "Curso de Derecho penal español. Parte general", Madrid, Marcial Pons, 1996, p. 120. Citado por SANZ HERMIDA, Ágata: "Extraterritorialidad de la Ley Penal y Jurisdicción, Madrid, 1999. https://www.uclm.es/area/procesal/Extraterritorialidad.htm#_ftn36

- ONG Article 19: "The Johannesburg Principles on National Security, Freedom of Expression and Access to Information" U.N. Doc. E/CN.4/1996/39, Londres, 1996. Principio 2. Disponible en: https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf

- ORTIZ PRADILLO, J.: "Problemas Procesales de la Ciberdelincuencia", Colex. Madrid, 2013.

- REY, Nathaly: "La Contratación de Servicios de Cloud Computing: Consideraciones sobre la Seguridad de la Información". Tesina de Doctorado, Universidad Complutense de Madrid, 2013.

- Restatement (Third) of Foreign Relations Law of the United States, 1987.

- ROLAND, Nicolas:"Court of Appeal of Antwerp confirms Yahoo!'s obligation to cooperate with law enforcement agencies", Bruselas, 2014. Disponible en: http://www.stibbe.com/en/news/2014/july/benelux-ict-law-newsletter-49-court-of-appeal-of-antwerp-confirms-yahoo-obligation

- RUBÍ, Jesús: "La protección de datos en el sector de las telecomunicaciones" publicado en el Boletín del Ilustre Colegio de Abogados de Madrid, Mayo 2007, 3.ª época N.36.

- SANZ HERMIDA, Ágata: "Extraterritorialidad de la Ley Penal y Jurisdicción". Madrid, 1999. Disponible en: https://www.uclm.es/area/procesal/Extraterritorialidad.htm#_ftn36

- SCHWARTZ M., Paul: "Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment". UC Berkeley School of Law. California, 2009. Disponible en: http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf

- SOLOVE, Daniel: "Surveillance Law in Dire Need of Reform: The Promise of the LEADS Act", blogpost. Disponible en: https://www.linkedin.com/pulse/surveillance-law-dire-need-reform-promise-leads-act-daniel-solove

- STIGLITZ, Joseph E., WALSH, Carl E.: Microeconomía, Barcelona, 2009.

- TAPIA F, Isabel: "Lecciones de Derecho Procesal". Volumen 1. Universitat Illes Balears, 2010.

- UNITED NATIONS: "Report of the International Law Commission", United Nations Publications, 2006.

- UNITED NATIONS General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 1990. Principio 9. Disponible en: http://www.refworld.org/docid/3ddcafaac.html

- UNITED NATIONS: "Report of the International Law Commission". New York, 2006. Anexo E. Disponible en: http://legal.un.org/ilc/documentation/english/reports/a_61_10.pd

- UNITED KINGDOM Cyber Security Strategy: "Protecting and promoting the UK in a digital world". Londres, 2011.

- VAN OUDENHOVE, Bart: "The formation of Contracts through the Internet, A decade of Research @ the Crossroads of Law and ICT". Bruselas, 2001.

- VELASCO, Cristos: "La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet. Tirant lo Blanch, Valencia Mayo 2012.

- VELASCO NUÑEZ, Eloy: "Delitos cometidos a través de internet. Cuestiones procesales". La Ley, 2010.

- VELASCO NUÑEZ, Eloy: "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, gps, balizas, etc.: la prueba tecnológica" Diario La Ley, N.º 8183. Madrid, 2013.

- WALDEN, Ian: "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent". Queen Mary School of Law Legal Studies Research Paper No. 74/2011. November 14, 2011, p.2. Disponible en SSRN: http://ssrn.com/abstract=1781067

- WALDEN, Ian: "Cybercrime and Jurisdiction in the United Kingdom" en Cybercrime and jurisdiction : a global survey. TMC Asser, La Haya, 2006.

- WANG Chenxi: How Secure Is Your Cloud? Forrester Research, Cambridge.

- WESTMORELAND, Kate: "Jurisdiction over user data - what is the ideal solution to a very real world problem". Julio, 2014. The Center for Internet and Society at Stanford Law School. Disponible en: http://cyberlaw.stanford.edu/blog/2014/07/jurisdiction-over-user-data-what-ideal-solution-very-real-world-problemhttps://www.leviathansecurity.com/blog/the-value-of-cloud-security/

12. SITIOS EN RED

- http://oerlemansblog.weblog.leidenuniv.nl/files/2011/02/Gent_-_OM-Yahoo.pdf
- http://digitalconstitution.com/wp-content/uploads/2014/11/government-warrant.pdf
- http://digitalconstitution.com/about-the-casehttp://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html
- http://www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/
- http://www.datosmacro.com/pib/honduras
- http://www.datosmacro.com/pib/paraguay
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498
- http://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm
- http://www.esecurityplanet.com/network-security/entry-point-identified-for-jpmorgan-chase-breach.html
- https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct
- http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf
- http://bits.blogs.nytimes.com/2014/12/02/computing-goes-to-the-cloud-so-does-crime/
- https://www.dropbox.com/business_agreement
- http://www.google.com/apps/intl/en-GB/terms/premier_terms_ie.html

- http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=7703
- http://www.hldataprotection.com/2015/08/articles/international-eu-privacy/russia-update-regulator-publishes-data-localization-clarifications/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ChronicleOfDataProtection+%28HL+Chronicle+of+Data+Protection%29
- http://politica.elpais.com/politica/2014/12/05/actualidad/1417793649_334772.html
- http://www.euractiv.com/infosociety/merkel-hollande-lay-foundation-p-news-533560
- http://uk.reuters.com/article/2013/06/16/us-germany-spying-idUKBRE95F0EU2013061
- http://www.rt.com/op-edge/256049-france-new-spying-rules-law/
- http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html
- http://www.telegraph.co.uk/technology/10421835/Germany-France-and-Spain-were-all-spying-on-citizens.html
- http://gizmodo.com/what-is-the-cloud-and-where-is-it-1682276210
- http://ec.europa.eu/justice/newsroom/data-protection/news/131127_en.htm
- http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf
- http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf
- https://ustr.gov/tpp
- http://servicescoalition.org/negotiations/trade-in-services-agreement
- https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here

- https://www.huntonprivacyblog.com/2014/12/02/poland-amends-personal-data-protection-act/
- https://www.law.cornell.edu/wex/fourth_amendment
- http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/3021_art15Conf_Conclusions_v1e.pdf
- http://www.euractiv.com/sections/infosociety/germany-set-bundescloud-316939
- http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf
- https://www.sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf
- http://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html
- http://www.irishtimes.com/business/technology/state-sanctions-phone-and-email-tapping-1.2027844
- http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
- https://en.wikipedia.org/wiki/Edward_Snowden
- http://www.gartner.com/newsroom/id/2616115
- http://press.ihs.com/press-release/design-supply-chain/cloud-related-spending-businesses-triple-2011-2017
- http://www.zdnet.com/article/cloud-computing-the-4th-it-industrial-revolution/

13. LEGISLACIÓN

INTERNACIONAL

- Convención de Budapest: Convenio número 185, del Consejo de Europa, sobre Ciberdelincuencia, de 23 de noviembre de 2001. Disponible en: http://conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm

- Carta Europea de Derechos Humanos. Decisión 2012/C 326/02 del Parlamento Europeo, el Consejo y la Comisión. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

EUROPA

- Tratado de la Unión Europea de 7 de febrero de 1992 firmado en Maastricht. (TUE). Versión consolidada publicada en el Diario Oficial de la Unión Europea el 30 de marzo del 2010. Disponible en: http://www.boe.es/doue/2010/083/Z00013-00046.pdf

- Convenio 108 del consejo de europa. Convenio nº 108 del consejo de europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Disponible en: https://www.agpd.es/portalwebAGPD/internacional/textosynormas/textos_consejo_europa/common/PDFs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf

- Directiva 2002/58/CE del parlamento europeo y del consejo del 12 de junio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF

- Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

- Proyecto de Reglamento General de Protección de Datos

  Propuesta de la Comisión
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF
  Propuesta del Parlamento
  http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/es/pdf
  Propuesta del Consejo
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

- Decisión 2009/820/PESC sobre la celebración, en nombre de la Unión Europea, del Acuerdo de Extradición entre la Unión Europea y los Estados Unidos de América y del Acuerdo de Asistencia Judicial en materia penal entre la Unión Europea y los Estados Unidos de América.

- Acuerdo de Asistencia Judicial en materia penal de la Unión Europea con Estados Unidos. Disponible en:
  http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:jl0052

- Decisión 2010/87/UE de la Comisión, de 05 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, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32010D0087

- Decisiones de Adecuación de la Comisión Europea en materia de protección de datos:

  - Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.
  - Decisión 2000/520/CE, de 26 de julio de 2000.
  - Decisión 2002/2/CE, de 20 de diciembre de 2001.
  - Decisión 2003/490/CE, de 30 de junio de 2003.
  - Decisión 2003/821/CE, de 21 de noviembre de 2003.
  - Decisión 2004/411/CE, de 28 de abril de 2004.
  - Decisión 2008/393/CE, de 8 de mayo 2008.
  - Decisión 2010/146/CE, de 5 de marzo de 2010.
  - Decisión 2010/625/CE, de 19 de octubre de 2010.
  - Decisión 2011/61/CE, de 31 de enero de 2011.
  - Decisión 2012/484/CE, de 21 de agosto de 2012.

- Decisión 2013/65/CE, de 19 de diciembre de 2012.
- Decisión 2010/87/CE, de 5 de febrero de 2012.

ESPAÑA

- Constitución Española, 1978.

- Código Civil: Real Decreto de 24 de julio de 1889, texto de la edición del Código Civil mandada publicar en cumplimento de la Ley de 26 de mayo último (Vigente hasta el 30 de Junio de 2017).

- Ley de Enjuiciamiento Criminal: Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal (cuya última modificación se encuentra en *vacatio legis* y entrará en vigor el 06 de diciembre de 20015).

- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

- Ley Orgánica 2/1986 de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Tratado de Asistencia Jurídica Mutua en Materia Penal entre los Estados Unidos de América y el Reino de España firmado el 20 de Noviembre de 1990.

- Instrumento contemplado por el art 3(2) del Acuerdo de asistencia judicial entre los Estados Unidos de América y la Unión Europea firmado el 25 de junio de 2003, sobre la aplicación del Tratado de asistencia jurídica mutua en

materia penal entre USA y el Reino de España firmado el 20 de noviembre de 1990, hecho ad referendum en Madrid el 17 de diciembre de 2004.

REINO UNIDO

- Police and Criminal Evidence Act 1984.
- Regulation of Investigatory Powers Act de 2000.
- Data Retention and Investigatory Powers Act de 2014.
- Mutual Legal Assistance Treaty between the United States of America and the United Kingdom of Great Britain and Northern Ireland de 1994.

BÉLGICA

- Code d'Instruction Criminelle.
- Loi relative aux communications électroniques de 13 de junio de 2005.

EE.UU.

- Electronic Communications Privacy Act (ECPA) de 1986.
- Communications Assistance for Law Enforcement Act (CALEA) de 1994.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) de 2001.
- Foreign Intelligence Surveillance Act (FISA) de 2008.
- Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act (USA Freedom Act) de 2015.
- Judicial Redress Act de 2015 (Proyecto).
- Sarbanes-Oxley Act (SOX) de 2002.
- Health Insurance Portability and Accountability Act de 1996.

- The Gramm–Leach–Bliley Act (GLB) de 1999.

14. NORMAS Y ESTÁNDARES

- ISO/IEC: 13335-1:2004.
- ISO/IEC: 27001:2013.
- ISO/IEC: 27002:2013.
- ISO/IEC:27018:2014.
- PCI/DSS.
- OECD Privacy Framework, 2013. Disponible en: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
- Marco de Privacidad APEC.Disponible en: https://www.sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf
- Estándares Internacionales sobre Protección de Datos Personales y Privacidad, Resolución de Madrid. Madrid, 2009. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

15. JURISPRUDENCIA, SENTENCIAS Y RESOLUCIONES[366]

EUROPA

- Caso Lotus (Francia vs. Turquía) Corte Permanente de Justicia Internacional, Ser. A, No. 10, 1927. Disponible en: http://www.dipublico.org/10984/s-s-lotus-1927-corte-permanente-de-justicia-internacional-ser-a-no-10/ /

- Caso Facebook (Maximillian Schrems vs Data Protection Commissioner) Tribunal de Justicia de la Comunidades Europeas. Asunto C−362/14. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d52cb5dc0589b84e368960866f8b1f9746.e34KaxiLc3eQc40LaxqMbN4ObNyNe0?text=&docid=169195&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=82286

ESPAÑA

- STS 246/1995, de 20 de febrero.
- STS 1377/1999, de 8 de febrero.
- STS 688/2009, de 18 de junio.
- STC 184/2003, de 23 de octubre.
- SSTC 104/2006 de 3 de abril.
- STS 182/2004, de 23 de abril.
- STC 173/2011, de 7 de noviembre.
- STS 782/2007, de 3 de octubre.
- SAN Sala Penal, 31/2009, de 30 de abril.
- AEPD. Resolución Nº Expediente: TI/00032/2014.
- AEPD. Informe Jurídico 2001-000.

[366] Los enlaces referenciados fueron accedidos por última vez por la autora en noviembre de 2015.

EE.UU.

- *United States vs. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001). Disponible en: http://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/

- *United States v. Microsoft*. MEMORAMDUM AND ORDER (D. NY.2015). Disponible en: http://digitalconstitution.com/wp-content/uploads/2014/09/Magistrate-Judge.pdf

- Caso ACLU v. Clapper. Corte de Apelaciones de los Estados Unidos para el Segundo Circuito. NY, Mayo, 2015. Disponible en: http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf

BÉLGICA

- Arrest dd. 30 juni 2010, uitgesproken door het Hof van Beroep te Gent.

16. CONFERENCIAS Y PRESENTACIONES

- JOBS, Steve. Apple WWDC conference, 1997 https://www.youtube.com/watch?v=Or7zaUaP-J8

- Gartner Symposium, 2013 http://www.gartner.com/newsroom/id/2613015

- VAN LINTHOUT, P & LERKHOFS,J: "Tour de table – major cases and important events".

- Cybercrime Convention Committee (T-CY), Strasbourg, 2-3 December 2013. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/Octopus2013_TCY_10th_plen.pdf

- KUTTERER, C: "Law enforcement internet jurisdiction". Intervención en CDPD 2015, min. 43. Disponible en: https://www.youtube.com/watch?v=NL4nNlzyqmQ

- SVANTESSON, Dan B: "Law enforcement internet jurisdiction". Intervención en CDPD 2015, min. 36. https://www.youtube.com/watch?v=NL4nNlzyqmQ

- VELASCOS, Cristos, CPDP 2015: Law enforcement internet jurisdiction https://www.youtube.com/watch?v=NL4nNlzyqmQ

- HORNLE, Julia-Queen Mary University of London CPDP 2015: Law enforcement Internet Jurisdiction. Disponible en: https://www.youtube.com/watch?v=NL4nNlzyqmQ