Acceso a los datos ajenos “en la nube” e interceptación de las comunicaciones virtuales ajenas: diferente protección iusfundamental

Cristina Zoco Zabala – Universidad Pública de Navarra (España), cristina.zoco@unavarra.es

Resumen: La computación en la nube plantea serias amenazas para los derechos fundamentales -intimidad *ex* art. 18.1 CE y/o protección de datos personales *ex* art. 18.4 CE-, derivadas de la interceptación ajena de tales archivos, sin consentimiento de su titular, o de su utilización para fines distintos para los que fueron almacenados. El acceso ajeno a los datos en la nube, no queda protegido por el secreto de las comunicaciones *ex* art. 18.3 CE, pues no se intervienen comunicaciones a través de medio técnico de uso (chats, correos electrónicos, videoconferencias), sino datos de carácter personal, o no. La ponencia trata de determinar la diferente protección iusfundamental del acceso virtual a los datos ajenos en la nube, respecto del acceso virtual de terceros a las comunicaciones.

Palabras clave: Intervención virtual de las comunicaciones, intervención virtual de los datos, computación en la nube, intimidad, protección de datos personales, secreto de las comunicaciones.

1. Introducción

La computación en la nube o *cloud computing*, constituye un nuevo modelo de prestación de servicios de negocio y de tecnología cuya información se almacena de manera permanente en servidores, y permite a los usuarios guardar contenidos variados: vídeos, o documentos de contabilidad almacenados en el disco duro del ordenador de mesa o en el portátil; comporta grandes ventajas, pues una vez que estos archivos se depositan en la «nube» se puede acceder a ellos desde cualquier ordenador sito en cualquier parte del mundo, lo que sirve para que se pueda trabajar en cualquier lugar sin necesidad de transportar los ordenadores. Sin embargo, plantea serias amenazas para los derechos fundamentales -intimidad *ex* art. 18.1 CE y/o protección de datos personales *ex* art. 18.4 CE-, derivadas de la interceptación ajena de tales archivos, sin consentimiento de su titular, o de su utilización para fines distintos para los que fueron almacenados. No así para el secreto de las comunicaciones, pues el art. 18.3 CE protege frente a la intervención ajena de las comunicaciones a través de medio técnico de uso, sin autorización judicial, pero no frente a la intervención virtual de datos privados o públicos, y éstos sean o no de tráfico. El acceso ajeno a los datos en la nube, no queda protegido por el secreto de las comunicaciones *ex* art. 18.3 CE, pues no se intervienen comunicaciones a través de medio técnico de uso (chats, correos electrónicos, videoconferencias), sino datos.

El objeto de este trabajo consiste en verificar la diferente protección iusfundamental del acceso virtual a los datos ajenos en la nube (arts. 18.1 y 18.4 CE), respecto de la intervención ajena de las comunicaciones (art. 18.3 CE). Así pues, la interceptación de los datos personales en la nube sin consentimiento de su titular, su revelación a terceros, o su utilización para fines diferentes para los que tales datos fueron almacenados, vulnera el derecho fundamental a la intimidad *ex* art. 18.1 CE, pero no el secreto de las comunicaciones, pues no se interceptan comunicaciones a través de medio técnico de uso, sino datos personales. Así mismo, la interceptación ajena de datos no privados en la nube (archivos de empresas o de administraciones), su

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

revelación a terceros, o su utilización para otro fin diferente para el que fueron almacenados, también vulnera el art. 18.1 CE, salvo que tales archivos contengan datos de tráfico, automatizados o no, pues tales datos quedarían protegidos por el art. 18.4 CE.

2. Contenido del art. 18.3 CE

El art. 18.3 CE garantiza la libre comunicación con otras personas a través de medios técnicos, excluyendo a todos los demás, pues trata de preservar al individuo su esfera de actuación libre de intervención de los poderes públicos y de los particulares[1]. En tal sentido garantiza la libertad de las comunicaciones, entendida como proceso de transmisión de pensamientos, ideas, opiniones, o datos adjuntos a las comunicaciones, a través de un medio técnico, libre de la intromisión de terceros[2].

El art. 18.3 CE tiene un doble significado positivo y negativo. Desde una dimensión positiva, protege el derecho de toda persona a utilizar los medios que la tecnología o el procedimiento ofrece para transmitir las comunicaciones a través de dichos medios. También tiene un significado negativo, pues permite la intervención de las comunicaciones realizadas a través de medio técnico de uso mediante una resolución judicial que sea constitucionalmente conforme. En tal sentido, prohíbe la inmisión de un tercero en el proceso comunicativo, si no es con el consentimiento del titular de dicho proceso, de modo expreso o presunto, o mediante resolución judicial suficientemente fundada. El art. 18.3 CE delimita el contenido del secreto de las comunicaciones al permitir interceptarlas cuando exista una resolución judicial suficientemente motivada que, en sí misma, no constituya una actuación probatoria, pero pueda conducir

[1] (DÍEZ-PICAZO, 2005: 313)
[2] (RODRÍGUEZ LÁINZ, 2011: 206). Se protege la comunicación realizada a través de canales o medios cerrados, entendiendo por tales, no aquellos medios inexpugnables al conocimiento ajeno, sino como contraposición a la comunicación abierta, esto es, no secreta (STC 170/2013). Esta cuestión ha sido tratada por la doctrina (RODRÍGUEZ LÁINZ, 2014: 4).

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

como diligencia instructora a la obtención de prueba; bien mediante la aprehensión de cartas o telegramas, bien mediante la grabación de una conversión telefónica.

El art. 18.3 CE constituye un derecho autónomo que consagra la libertad de las comunicaciones de modo implícito y, de modo expreso, su secreto. Posee eficacia *erga omnes* directa, *ex constitutione*[3], por lo que prohíbe la intervención de las comunicaciones ajenas (poderes públicos y particulares), realizadas a través de un medio técnico, o mediante la aprehensión física del soporte de un mensaje[4], al tiempo que permite su interceptación siempre que vaya precedida de una resolución judicial que sea constitucionalmente conforme (PULIDO QUECEDO , 2007: 9 a 11); es decir, fundada en sospechas objetivas de la presunta comisión de un delito grave del intervenido, que puede ser el sospechoso o un tercero relacionado con él[5]. En tal sentido, la entrega

[3] Esta tesis (BILBAO UBILLOS, 1997: 809 y 810), no es sostenida por otro sector de la doctrina, que defiende que el secreto de las comunicaciones constituye sólo un derecho público subjetivo por lo que del artículo 18.3 CE no se origina para los particulares, de modo directo, deber alguno que sea jurídicamente coercible; deber que puede existir a partir de la existencia de disposiciones infraconstitucionales, penales o civiles (JIMÉNEZ CAMPO, 1987: 56 a 58). Sin embargo, el carácter normativo de la Constitución determina que los derechos fundamentales son de aplicación directa frente a los poderes públicos y los particulares (artículo 9.1 CE), cuando no hay una ley que adapte el contenido de un derecho fundamental en defensa de la autonomía privada. Así, por ejemplo, la intervención de las comunicaciones en el centro de trabajo por parte del empresario, determina la necesidad de cohonestar las debidas garantías de la intervención de las comunicaciones (artículo 18.3 CE) con la libertad de empresa exigida por el artículo 38 CE. Sin embargo, la inexistencia de un procedimiento especial para la intervención de las comunicaciones cuando la necesidad de ello se origina en el ámbito privado, no permite al empresario intervenir las comunicaciones sin cumplir el procedimiento general habilitado para ello pues, por encima de todo, debe ser respetado el derecho fundamental, y, con él, las garantías generales establecidas por la ley para su efectivo cumplimiento.

[4] En suma, se proscribe toda intervención en sentido estricto que suponga una aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o la captación de otra forma del proceso de comunicación, como el simple conocimiento antijurídico de lo comunicado (por ejemplo, la apertura de la correspondencia ajena guardada por su destinatario (STC 230/2007).

[5] La intervención de las comunicaciones no se puede decidir con fines meramente prospectivos, es decir, 'para ver qué pasa y no porque en realidad se pueda decir que ha pasado o esté a punto de pasar algo relevante' (ANDRÉS IBÁÑEZ, 2005: 20). Sin embargo, ello no significa que el intervenido tenga que estar imputado, ni haberse procedido a la apertura de procedimiento contra dicho interceptado o contra tercero relacionado con él, pues no se requiere la existencia de indicios razonables de su presunta culpabilidad. Precisamente, la intervención de las comunicaciones persigue la obtención de pruebas para abrir el proceso de instrucción contra el intervenido, o tercero relacionado con él.

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

de listados de teléfonos de llamadas recibidas de números de teléfono de receptores sospechosos por las compañías telefónicas a la policía sin previa intervención de las comunicaciones a través de medio técnico de uno y previa autorización judicial motivada no queda protegida por el art. 18.3 CE, pues no se trata de datos obtenidos como consecuencia de la intervención de las comunicaciones, constitucionalmente conforme. Dicha actuación debería quedar protegida *ex* art. 18.4 CE, por tratarse de datos de tráfico; sin embargo tal norma de derecho fundamental no alude, en su contenido, a la posibilidad de intervenir dichos datos previa resolución judicial y a la necesidad de que la ley determine los supuestos de intervención que con las debidas garantías jurisdiccionales, quedarían protegidos por el art. 18.1 CE. Por el contrario, el Tribunal Constitucional reconoce haber otorgado monopolio jurisdiccional para garantizar la intervención de supuestos que afectan a la intimidad, en aras de la seguridad pública. Lo que, a futuro, puede vaciar de contenido algunos derechos fundamentales, como el derecho a la intimidad[6].

[6] En una misma sentencia -la 123/2002- el Tribunal Constitucional ha expresado, de un lado, que la vulneración del secreto de las comunicaciones telefónicas requiere la interferencia directa en el proceso de comunicación mediante el empleo de cualquier artificio técnico de captación, sintonización o desvío y recepción de la señal telefónica como forma de acceso a los datos confidenciales de la comunicación: existencia, contenido, y circunstancias externas. Se entendería, así, que la entrega de los listados de los teléfonos de llamadas telefónicas de los receptores, quedaría protegida si lo es como consecuencia de la interceptación de las comunicaciones constitucionalmente conforme. Mientras que la captación de estos datos sin previa intervención judicial motivada no quedaría protegida por el art. 18.3 CE, sino por el art. 18.4 CE que, sin embargo, no alude a autorización judicial alguna para demandar la entrega de listados de teléfonos a las compañías. Paradójicamente, el Tribunal Constitucional ha entendido que la entrega de los listados por las compañías telefónicas a la policía sin previa autorización judicial de intervención de las comunicaciones telefónicas realizada a través de medio técnico de uso, vulnera el art. 18.3 CE, por aducir que los listados telefónicos incorporan datos relativos al teléfono de destino, el momento en el que se efectúa la comunicación y su duración, por lo que afectan al proceso de comunicación. De tal manera, que para su conocimiento y registro resulta necesario acceder de forma directa al proceso de comunicación con independencia de que estos datos se tomen en consideración una vez finalizado aquél proceso a efectos, bien de la lícita facturación del servicio prestado, o bien de su ilícita difusión. Aunque señala que el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones de menor intensidad que las escuchas telefónicas. Véase, en el mismo sentido, las SSTC 56/2003 y 70/2002.

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

3. Intervención virtual de las comunicaciones e intervención del ordenador

La versatilidad de este terminal informático lo convierte, hoy en día, en máquina electrónica imprescindible, en el ámbito laboral y familiar. En su origen fue un almacén de datos (años 70), pasando a asumir, de modo progresivo, otras funciones: soporte de libros y documentos, depósito de vídeos y fotografías, así como instrumento de comunicación mediante correo electrónico o a través de Internet (chats, videochats, etc).

En suma, el computador constituye terminal que alberga datos personales contenidos en archivos informáticos variados, al tiempo que es instrumento para el almacenamiento y transmisión de correos electrónicos u otras comunicaciones telemáticas como chats, videoconferencias. Sin embargo, procede distinguir entre los datos personales de tráfico consecuencia de la navegación por internet, para buscar información o para leer el correo electrónico, protegidos *ex* art. 18.4 CE, de los datos personales consecuencia del conjunto de archivos personales que el titular del mismo acumula en el disco duro del terminal, protegidos *ex* art. 18.1 CE[7]. Se advierte, así, que los

[7] La jurisprudencia del Tribunal Constitucional, a la que sigue el Tribunal Supremo no diferencian entre datos personales y datos de tráfico en la determinación de los derechos fundamentales que pueden ser vulnerados como consecuencia de la intervención del ordenador. Así pues, establece que no hay duda "de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros, datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

dispositivos tecnológicos-electrónicos constituyen una importante fuente de prueba en el proceso penal[8].

El acceso de un tercero al ordenador para la observancia de datos personales contenidos en los archivos personales precisa de consentimiento del titular (art. 2.2 LO 1/1982 de 5 de mayo, de protección del Derecho al Honor, a la Intimidad Personal y Familiar, y a la Imagen). Los documentos, fotografías o vídeos almacenados en el disco duro del terminal se cualifican como datos personales y no como comunicaciones al no existir un proceso comunicativo a través de medio técnico de uso. De todo ello resulta que la incautación y posterior apertura de los archivos sin consentimiento del titular, o sin autorización judicial, no cercena el art. 18.3 CE sino el derecho fundamental a la intimidad. La necesaria autorización judicial para intervenir los datos personales del ordenador, por sospechas de la presunta comisión de un delito grave tampoco resulta del art. 18.1 CE ni de la LO 1/1982 que lo configura. Sin embargo, la incautación, en todo caso policial, del ordenador para la intervención de los correos electrónicos o las comunicaciones instantáneas a través de internet (chats, videoconferencias, comunicaciones con vídeo y voz) previa resolución judicial motivada en las sospechas de la presunta comisión de un delito grave queda protegido por el art. 18.3 CE.

personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información" (STC 173/2011). Procede diferenciar la intervención de los correos personales leídos y almacenados en un terminal informático de los correos leídos como consecuencia de la interceptación de las comunicaciones a través de medio técnico de uso (STC 170/2013). Véase en el mismo sentido, STS 342/2013, de 17 de abril (Sala de lo Penal, Sección 1ª);

[8] "Los dispositivos tecnológicos/electrónicos (datos: ordenadores, voz e imagen: grabadores, localizadores: GPS, telecomunicativos: teléfonos móviles y sus múltiples variantes), fuente de prueba en el proceso penal, forman ya tal parte de nuestra vida particular, familiar y laboral cotidiana que difícilmente es planteable no ya su desaparición de nuestra existencia sino una vida alternativa sin ellos. Nos acompañan a diario, dormimos a su lado (gracias a su carácter móvil y a las comunicaciones sin cable que permiten), nos enlazan con tales fuentes de información (Internet principalmente) y nos relacionan de tal forma con los demás (redes sociales) que han devenido en pocos años simplemente irrenunciables" (VELASCO NÚÑEZ. 2013: 3 Y 4).

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

La observancia ajena de los archivos personales a través del terminal informático es decisión única del titular del mismo, pues el derecho fundamental a la intimidad no contiene una delimitación restrictiva similar a la establecida para la interceptación de los procesos comunicativos que tienen lugar a través de medios telefónicos, postales, telegráficos o telemáticos[9]. Sin embargo, el Tribunal Constitucional y el Tribunal Supremo han equiparado la delimitación restrictiva del derecho al secreto de las comunicaciones (la intervención precedida de autorización judicial) con la incautación del ordenador para la observancia no telemática de los contenidos incluidos en su disco duro. Intervención que, a diferencia del art. 18.3 CE, no prevé el art. 18.1 CE por tratarse de datos personales y no comunicaciones, pero que la jurisprudencia entiende posible y necesaria, por existir un interés constitucionalmente relevante superior al derecho que se pretende proteger, cual es la sospecha de la presunta comisión de un delito grave. En tal sentido, determina que la medida restrictiva de la intimidad tiene que estar prevista en la ley y ser susceptible de autorización judicial. También señala la necesidad de garantizar los criterios de proporcionalidad[10]. En suma, se impone la necesidad

[9] El Tribunal Constitucional ha señalado que el consentimiento eficaz del sujeto particular permite la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno, aunque este consentimiento puede ser revocado en cualquier momento (SSTC 173/2011; 159/2009; 196/2006; 83/2002). También determina que se socava el derecho fundamental a la intimidad cuando existiendo consentimiento del titular se subvierte el alcance para el que dicho consentimiento se otorgó, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida (SSTC 173/2011; 70/2009; 206/2007; 196/2004). El Tribunal Supremo ha expresado que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. También señala que la incautación del ordenador para el conocimiento de datos íntimos precisa de la entrada en domicilio. "De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales delimitaren el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías", STS 342/2013, de 17 de abril (Sala de lo Penal, Sección 1ª).

[10] STC 173/2011. En relación con esta cuestión, el Tribunal Supremo señala lo siguiente: "el acceso a los contenidos de cualquier ordenador por los agentes de policía, ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

de que la norma de derecho fundamental delimite el contenido del art. 18.1 CE, habilitando al legislador para que determine en qué casos, y bajo qué procedimiento, se limita el contenido de este derecho fundamental por exigencias de seguridad. La posibilidad de delimitar mediante ley, el contenido de un derecho, y las garantías de dicha limitación, tiene que ser recogido en la norma de derecho fundamental[11].

---

espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal.

La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital.

Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías", STS 342/2013, de 17 de abril (Sala de lo penal, Sección 1ª).

[11] La LECrim determina que el volcado de información contenida en ordenadores, memorias digitales o soportes de tal clase, habrá que tener en cuenta el art. 577 LECrim en orden a la presencia del perito en el lugar del registro y de la ocupación simultánea de los objetos relacionados con la investigación. La doctrina establece que dada la complejidad técnica de la aprehensión de los "muy volátiles e intrusivos elementos de convicción y prueba de los delitos informáticos" hace necesaria la presencia del perito en las diligencias de entrada, registro y confiscación, que pueda hacer real el mandato de no importunar más de lo necesario que pretende el art. 552 LECrim. Si el registro se realiza en el despacho de abogados el art. 32.2 del Estatuto General de la Abogacía Española establece que si "el decano de un colegio, o quien estatutariamente le sustituya, fuere requerido en virtud de norma legal o avisado por la autoridad judicial, o en su caso gubernativa, competente para la práctica de un registro en el despacho profesional de un abogado, deberá personarse en dicho despacho y asistir a las

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

Cuestión diferente es la observación ajena de los correos electrónicos o de las comunicaciones a través de medio técnico de uso como consecuencia del consentimiento de la entrada en el ordenador por parte del titular. La incautación del ordenador para su observancia necesita autorización judicial, si lo que se pretende es acceder al correo electrónico para observar la llegada de correos electrónicos[12]. Sin embargo, no se vulnera el art. 18.3 CE si el titular del terminal permite su intromisión, dando a conocer las claves de acceso al correo (que puede ser el mismo que para el acceso al ordenador), o haciendo partícipes a los demás de los correos electrónicos, o del chat que mantiene con otro interlocutor, a través de su apertura mediante el uso de sus claves. En el ámbito empresarial, el Tribunal Constitucional ha negado la libertad del empresario para registrar los ordenadores que son propiedad de la empresa[13].

4. Intervención virtual de las comunicaciones e interceptación de los datos en la nube

Algo diferente de la interceptación del ordenador supone la intervención virtual del mismo a través del servicio de internet que se conoce como "computación

diligencias que en el mismo se practiquen, velando por la salvaguarda del secreto profesional». La doctrina también establece que si ello resulta posible, "en el mismo auto concediendo la autorización judicial para la entrada y registro se proceda a la incautación o intervención de los dispositivos de memoria -cds, dvds, discos duros, usbs, etc.- y se concrete la pericia a realizar, identificándose todos ellos por el secretario judicial en el acto del registro y con constancia detallada en el acta levantada por él" (SUÁREZ ROBLEDANO, 2011: 91).

[12] El Tribunal Supremo (STS 342/2013, de17 de abril, Sala de lo Penal, Sección 1ª) diferencia entre los correos electrónicos observados como consecuencia de la entrada en el servicio de los ya observados por su destinatario, y que quedan almacenados en el terminal informático, a los efectos de su protección por los artículos 18.3 CE y 18.1 CE, respectivamente: " (…) el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información".

[13] STC 186/2000.

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

en la nube" o *cloud computing*. La razón estriba en que este modelo de prestación de servicios de negocio y de tecnología almacena documentos con contenidos variados (vídeos, documentos de contabilidad, de tratamiento de textos) almacena datos a través del servicio de internet. De tal manera, que una vez que estos archivos se depositan en la "nube" se puede acceder a ellos desde cualquier ordenador sito en cualquier parte del mundo, lo que sirve para que se pueda trabajar en cualquier lugar sin necesidad de transportar los ordenadores[14]. Así mismo, los archivos se mantienen de forma segura, de tal manera que si el disco duro del ordenador queda estropeado, existe una copia de seguridad en la "nube", es decir, en otro disco duro[15].

[14] (SALAS ZÁRATE, COLOMBO-MENDOZA, 2012: 55). Entre otros beneficios, la computación en la nube supone minimizar el gasto de capital y reducir el costo de propiedad. Además tiene la ventaja de no necesitar espacio físico para almacenar servidores y bases de datos, ya que están en la nube. Supone también la independencia de localización y dispositivo; es independiente de los sistemas operativos y, virtualmente, tiene capacidad de almacenamiento ilimitada (AREITIO, 2010: 44). El Dictamen del Comité Económico y Social Europeo sobre el tema de la computación en nube en Europa, de 28 de enero de 2012, indica que, en la práctica, la computación en nube se apoya en un modelo económico prometedor, en el que se presentan facilidades y utilidades de gran importancia sobre la base de un número de usuarios potenciales importante, entre los que destacan las empresas y los servicios públicos, con la compartición de los medios y recursos informáticos que permite la optimización de su uso, la movilidad que permite la computación en nube, especialmente para los usuarios móviles, que pueden acceder a sus datos de forma permanente, la integración fácil, ajustable y transparente de los distintos componentes técnicos y la distribución de los costes a lo largo de todo el ciclo de vida de los sistemas informáticos, sin una inversión inicial elevada". Así mismo, la comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (COM, 2012, 529 final, de 27 de septiembre de 2012), bajo el epígrafe "Liberar el potencial de la computación en la nube en Europa", pretende permitir y facilitar una adopción más rápida de este tipo de computación en todos los sectores de la empresa. En tal sentido, la comisión entiende que mientras la red global permite la disponibilidad de información en todas partes y para cualquier persona, la computación en la nueve ofrece la posibilidad de tener capacidad informática en cualquier lugar y para toda persona (DAVARA RODRÍGUEZ, 2013: 1).

[15] Existen diferentes modelos de *cloud computing*. Se clasifican en nubes públicas, privadas, comunitarias e híbridas. En la nube pública la infraestructura de nube se hace disponible al público en general o a un gran grupo industrial y es propiedad de una organización que vende los servicios de *cloud computing*. Los servicios se ofrecen al público en general o a grupos de personas de varias organizaciones. Su propietario es el proveedor de servicios. Las aplicaciones e información se almacenan en servicios externos y el servicio se ofrece a través de internet. En la nube privada la infraestructura de *cloud* sólo opera para una organización. Puede gestionarla la propia organización o una tercera parte y puede existir en el local o fuera. Tiene como destinatarios, generalmente a las empresas. Este concepto hace referencia a redes o centros de procesamiento de datos propietarios que utilizan las características del *cloud computing*, tales como la virtualización. En suma, se parte de los principios del *cloud computing* tradicional y ofrecen los mismos servicios pero dentro de la estructura de la propia compañía. La ventaja respecto de la nube pública es que los datos se localizan dentro de la

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

Este servicio virtual que necesita conexión a internet para su uso puede almacenar ficheros personales y compartidos con otros trabajadores de la empresa; supone un servicio de alojamiento en internet de archivos personales (documentos de Word, Excel, fotografías, vídeos, etc.) y compartidos (empresas) pero no es una página web. De tal manera que la intervención de estos ficheros no queda protegida por el art. 18.3 CE, pues no alberga comunicaciones a través de un medio técnico de uso[16]. Tampoco queda protegida por el art. 18.4 CE cuando se trata de archivos personales *ex* art. 2.2 a) LOPD. Se entiende, así, que la intervención de estos ficheros personales o domésticos precisa del consentimiento del titular *ex* art. 18.1 CE y *ex* art. 2.2 LO 1/1982; del mismo modo, se prohíbe revelarlos una vez que el titular ha consentido el acceso a los mismos a un tercero, *ex* art. 7.3 LO 1/1982. En la medida en que no son datos de tráfico, se impide todo tratamiento por parte de las operadoras: grabación, conservación, modificación, bloqueo de datos (art. 3 c. LOPD). Por el contrario, la intervención de los ficheros no personales (ficheros de la empresa, o de una administración) que albergan datos de tráfico quedan protegidos por las garantías del art. 18.4 CE, cuales son la obligación de los usuarios y de las operadoras de no revelar los datos a terceros, ni de darles una finalidad distinta de la que la empresa o la administración consintieron. Sin embargo, dichos datos pueden ser objeto de tratamiento por parte de las operadoras, con el consentimiento del titular[17].

propia empresa lo que redunda en una mayor seguridad de éstos. En la nube comunitaria, la infraestructura de nube se comparte por parte de varias organizaciones y soporta una comunidad específica que tiene intereses compartidos (por ejemplo misión, requisitos de seguridad, política y consideraciones de cumplimiento). La pueden gestionar las organizaciones o una tercera parte y puede existir en el local o fuera. La nube híbrida supone una composición de dos o más nubes (privada, pública o comunitaria) única para las entidades pero se limitan juntas por medio de tecnología propietaria o estandarizada que permite la portabilidad de datos y aplicaciones. Esta cuestión ha sido tratada por la doctrina (AREITIO, 2010: 43).

[16] La doctrina ha planteado problemas de protección de datos y de privacidad, derivada de la dispersión de datos en la nube que haría necesaria una puesta revisión de las normas y políticas comunitarias e internacionales tales como la Directiva Europea de Protección de Datos o el Programa norteamericano *Safe Harbor*, para la cesión de datos entre EEUU y la UE, por razones de seguridad (AREITIO, 2010: 47; LEENES, 2010: 1 Y 2).

[17] Servicios como *Dropbox* o *Box* y algunos más especializados como *Soundcloud, Flickr* o *YouTube***,** facilitan poner a disposición de tus amigos documentos, fotografías y vídeos sin usar soportes físicos, simplemente a partir de un enlace a una página web. Sin embargo, estos

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

Tampoco, en este caso es posible una autorización judicial para que la policía intervenga los datos de tráfico pues nada de ello se deduce del art. 18.4 CE y de la LOPD.

Sería preciso que la Constitución aludiera a la necesaria intervención judicial de los datos en la "nube", pues ello podría ser de interés, en un futuro, para la indagación de delitos por sospechas objetivas de su presunta comisión, y porque dicha intervención, de producirse, estaría garantizada a través de una autorización judicial, por analogía con los arts. 18.3 y 18.2 CE. Requisito que la jurisprudencia del Tribunal Constitucional ha exigido sólo en algunos escenarios de interceptación de la intimidad para la obtención de pruebas de la presunta comisión de un delito: la intervención del ordenador y sus datos personales[18]. La interceptación de los datos y documentos personales "en la nube" puede ser un buen medio para poder obtener información de la presunta comisión de un delito grave, teniendo en cuenta que muchas veces resulta difícil o imposible la incautación del ordenador del titular por los agentes, porque dicho computador ha desaparecido; también porque, una vez los agentes hayan incautado el ordenador, no contenga información al haber sido borrada por su titular o por un tercero, bajo sospecha de poder ser inspeccionado por los servicios de seguridad. Dicha intervención debería ser implementada previa autorización judicial, lo que llevaría consigo una necesaria reforma del art. 18.4 CE. Sin duda, que la Constitución tendría que delimitar, de

servicios en la nube suponen que se comparta los archivos no sólo con los contactos del titular de los mismos sino también con los autores de la aplicación o espacio online. En tal sentido, han surgido tecnologías en forma de software que permiten crear una propia nube personal, un espacio propio gestionado por uno mismo para compartir por *streaming* o mediante descarga el contenido personal sin intermediarios.

[18] La doctrina ha puesto de manifiesto la problemática de la computación en la nube, en la medida en que el proveedor puede realizar espionaje e incautar información; Así por ejemplo, entiende que la información de ciertas redes sociales (*Facebook*) se utiliza para pasarla a otros usuarios, y también se pueden utilizar aplicaciones de terceros para ser ejecutadas en tales plataformas. En tal sentido, entiende que es posible la creación de aplicaciones para ejecutarlas en la nube de una red social con el fin de robar datos sensibles. La dispersión de datos precisa de leyes de privacidad internacionales como la directiva de protección de datos (AREITIO, 2010: 47). También se ha puesto de manifiesto que la acumulación de datos en la nube plantea problemas de seguridad, transparencia, confidencialidad, ausencia de políticas de regulación (CERRILLO, 2010: 1).

.

modo restrictivo, este derecho fundamental, y el legislador regular, democráticamente, el procedimiento que garantice la persecución del bien jurídico de la seguridad, sin merma de objetivación de los criterios que pueden delimitar restrictivamente, o, en su caso, limitar el contenido de los arts. 18.4 y 18.1 CE.

5. Bibliografía

- BILBAO UBILLOS, J.M. (1997): *La eficacia de los derechos fundamentales frente a particulares*, Centro de Estudios Políticos y Constitucionales, Madrid, 1997.
- DÍEZ-PICAZO, L.M. (2005): *Sistema de derechos fundamentales*, Cizur Menor, Thomson-Civitas.
- E. VELASCO NÚÑEZ (2013): "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario la Ley*, 8183. Madrid, páginas. 3 a 4.
- J. AREITIO (2010): "Protección del cloud computing en seguridad y privacidad", *Revista Española Electrónica*, 666, Madrid, páginas. 42 a 48.
- J. JIMÉNEZ CAMPO (1987): "La garantía constitucional del secreto de las comunicaciones", en *REDC*, 20. Madrid, 1987, páginas 56 a 58.
- J.L. RODRÍGUEZ LÁINZ (2014): "Reflexiones sobre los nuevos contornos del secreto de las comunicaciones (Comentario a la STC 170/2013, de 7 de octubre)", en *Diario La Ley,* 8271. Madrid, páginas 0 a 1.
- J.M. SUÁREZ ROBLEDANO (2011): "Intervención de comunicaciones electrónicas", *Foro. Nueva Época*, 14. Madrid, páginas 73 a 99.
- M. PULIDO QUECEDO (2007): "La noción de 'secreto de las comunicaciones' *ex* artículo 18.3 CE", *Repertorio Aranzadi del Tribunal Constitucional*, 16. Cizur Menor, páginas 9 a11.
- M. SALAS ZÁRATE, M. L. COLOMBO-MENDOZA, L. (2012): "Cloud computing: una revisión de los servicios y proveedores paas, iaas, saas services and providers", *Lampsakos*, 7. Medellín, páginas 47 a 57.

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

- M.A. DAVARA RODRÍGUEZ (2013): "Europa y la computación en la nube", *El consultor de los ayuntamientos y de los juzgados*, 7. Madrid, páginas 755 a 760.

- P. ANDRÉS IBÁÑEZ (2005): "La función de las garantías en la actividad probatoria".En VV.AA., *La restricción de los derechos fundamentales de la persona en el proceso penal. Cuadernos de Derecho Judicial*, Madrid, CGPJ.

- RODRÍGUEZ LÁINZ, J.L. (2011): *Estudios sobre el secreto de las comunicaciones. Perspectiva doctrinal y jurisprudencial,* Madrid, La Ley.

- R. LEENES (2010): "Who controls the cloud?", *Revista de Internet, derecho y política (IDP*), 11. Barcelona, páginas 1 a 2.

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014

ISBN-13: 978-84-15698-74-6 / D.L.: TF-589-2014