LE QUID THE J. DUTILH BUSINESS LAW FIRM

C/ Capitán Haya 1, planta 15
28020 Madrid

T + 34 91 418 43 52
F + 34 91 418 43 54

www.lequid.eu

INFORME LEGAL PARA LA SOCIEDAD MERCANTIL E.TELECOM SOBRE LOS ASPECTOS LEGALES A TOMAR EN CUENTA EN SU SOLUCIÓN DE HOTSPOT

I. HECHOS

La sociedad mercantil e.Telecom plantea una consulta sobre los aspectos legales y obligaciones a cumplir en el uso de Hotspot de acceso a internet para redes wifi, a los fines de identificar las ventajas de la solución que han creado y que desean vender y posicionar en el mercado.

II. CONCLUSIONES Y RECOMENDACIONES

1.- La información del folleto promocional es imprecisa a nivel legal por lo cual se aconseja su modificación por los siguientes motivos:

1.1 En el folleto promocional se señala textualmente que: "*en caso de cometerse un delito informático en una empresa, el responsable penal es el gerente de la misma, lo que puede suponer penas económicas e incluso de prisión*". Afirmación que resulta incorrecta, ya que la reforma del Código Penal del año 2.010 señala literalmente en el nuevo art. 31 bis, y siempre bajo el prisma del principio de culpabilidad, que la persona jurídica responderá penalmente en dos supuestos:

1. *Por los delitos cometidos en nombre o por cuenta de la persona jurídica, y en su provecho, por sus **legales representantes y administradores de hecho o de derecho**.*

2. *Por los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de la persona jurídica, por quienes, **estando sometidos a la autoridad de sus legales representantes o administradores de hecho o de derecho**, han podido realizar los hechos por **no haberse ejercido sobre ellos el debido control** atendidas las concretas circunstancias del caso.*

En consecuencia, para que pueda responder penalmente la empresa, es necesario que el delito sea cometido por **el *administrador, por los trabajadores, empleados o contratados, sin que se pueda demostrar que se ha ejercido sobre los mismos el debido control***. Por lo cual las empresas (en este caso los hoteles) no responden, ni son responsables por delitos cometidos por terceros, como lo pueden ser los clientes o usuarios de sus servicios (huéspedes del hotel).

Salvo, que el delito sea cometido por sus administradores, trabajadores o personal contratado, utilizando la conexión wifi como medio para cometer el delito. Caso en el cual, la empresa deberá demostrar para no responder penalmente, que ha ejercido un debido control a través de los siguientes instrumentos:

- Instrumentos de prevención: códigos de conducta, programas de cumplimiento de la legalidad, etc., donde la empresa analiza los riesgos penales en que puede incurrir en función de su actividad, define las normas y

principios éticos por los que debe regirse el comportamiento de todos los agentes de la empresa, y prohíbe expresamente aquellas conductas que puedan ser consideradas constitutivas de delito.

- *Instrumentos de control*: internos y/o externos, que supervisen de manera continuada el cumplimiento de la normativa interna establecida para evitar la comisión de delitos y evalúen la existencia de nuevos riesgos.

- *Instrumentos disciplinarios*: para asegurar el debido control del cumplimiento de las normas de conducta establecidas por la empresa, donde puede implantarse un catálogo de sanciones internas que afecten a empleados y directivos de los que aquéllos dependen, de manera que éstos se involucrarán, a su vez, en el control sobre aquéllos.

2.- DELITOS QUE SE PUEDEN PRODUCIR A TRAVÉS DE REDES WIFI O INTERNET (DELITOS INFORMÁTICOS). CONSECUENCIAS PARA LAS EMPRESAS

La unidad de delitos telemáticos de la guardia Civil clasifica como **delito informático**, *todos aquellos delitos cometidos a través del medio telemático y cuya vía probatoria se sustenta en la prueba informática*. Así, entre los delitos que se pueden producir en el ámbito online y tipificados en el Código Penal (CP) podemos mencionar los siguientes:

- ✓ Delito de descubrimiento y revelación de secretos (art. 197 CP).
- ✓ Delitos de estafa (arts. 248 a 251 CP) y blanqueo de capitales (art. 302 CP).
- ✓ Delito de daños informáticos (art. 264 CP): la intrusión en equipos ajenos («hacking»), la revelación de contenidos albergados en programas y archivos informáticos, los fraudes («phising» y «pharming»), la falsificación informática, y los daños a los elementos lógicos del sistema («cracking») y los delitos clásicos que encuentran en la red su medio comisivo, así, las amenazas, las vejaciones, el ciberterrorismo, los delitos contra la libertad sexual, los que afecten a la propiedad industrial, derecho de autor, acercamiento tecnológico a menores de trece años con fines sexuales o también conocido como “child grooming”, etc.

2.1 Penas aplicables a las personas jurídicas

a) Multas:

Multa por cuotas: Extensión máxima de cinco años, con una cuota diaria mínima de 30 € y máxima de 5.000 €.

Proporcional: al beneficio obtenido o facilitado, al perjuicio causado, al valor del objeto, o a la cantidad defraudada o indebidamente obtenida.

b) Disolución de la persona jurídica:

La disolución producirá la pérdida definitiva de su personalidad jurídica, su capacidad de actuar en el tráfico jurídico de cualquier modo.

c) **Suspensión de sus actividades**. (Máximo: 5 años)

d) **Clausura de sus locales y establecimientos**. (Máximo: 5 años)

e) **Prohibición de realizar en el futuro las actividades** en cuyo ejercicio se haya cometido, favorecido o encubierto el delito (esta prohibición podrá ser temporal máximo 5 años, o definitiva).

f) **Inhabilitación para obtener subvenciones y ayudas públicas**, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social. (Máximo: 5 años)

g) **Intervención judicial** para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario. (Máximo: 5 años)

Responsabilidad civil de la persona jurídica.

Según lo dispuesto en el art. 116.3 Código Penal, la responsabilidad penal de la persona jurídica llevará consigo su responsabilidad civil de forma solidaria con las personas físicas que fueren condenadas por los mismos hechos, remitiéndose a la regulación genérica del art. 110 CP en cuanto al contenido de la responsabilidad civil derivada de delito, que conllevaría la restitución, la reparación del daño, la indemnización de perjuicios materiales y morales.

3. El ciberataque y la obligación de las empresas (hoteles) de implementar medidas de ciberseguridad

El **Ciberataque** se define como la acción producida en el ciberespacio que compromete la *disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.*

En la práctica, el ciberataque es contrarrestado con medidas que garanticen la **Ciberseguridad**, cuyo objetivo es proteger la información ante accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones no permitidas, incluyendo la gestión de riesgos del ciberespacio, a través de la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados, basándose en los estándares internacionalmente aceptados.[1]

3.1 Regulación del cibercrimen y la ciberseguridad

Europa desde el 2011 cuenta con una legislación pionera sobre delitos en el ciberespacio, con el llamado **Convenio de Viena**, o **convenio internacional sobre el cibercrimen**, firmado en Budapest el **23 de noviembre de 2001,** y al que España se adherió en su día, y **ratificó en junio de 2010.**

Posteriormente, el 28 de enero de 2003, se promulgó la firma de un protocolo adicional al convenio para criminalizar los actos de racismo y xenofobia cometidos a través de sistemas informáticos.

Y recientemente el 4 de julio de 2013, El Parlamento Europeo (PE) respaldó una nueva **Directiva sobre ciberseguridad**, que contempla penas más estrictas para los autores de delitos cibernéticos y el espionaje industrial entre empresas.

Esta nueva directiva, será adoptada en los próximos meses por el Consejo, mientras que posteriormente los Estados miembros de la Unión Europea (UE) tendrán que trasponer la norma a su legislación nacional en un plazo de dos años. Dicha directiva tiene como ***objetivo facilitar la prevención e impulsar la cooperación policial y judicial en este ámbito, motivo por el cual los estados acordaron un plazo máximo de 8 horas para responder a la información solicitada, en caso de que producirse un ciberataque.***

En concreto, el texto aprobado contempla una pena máxima de 2 años de cárcel contra el acceso ilegal a sistemas de información y bases de datos, así como por interceptar comunicaciones o producir y vender los instrumentos para cometer estos delitos, y 3 años de cárcel a aquellos que usen 'botnets' (controladores remotos de ordenadores) para cometer actividades ilícitas. Mientras, que los ataques contra instalaciones energéticas, redes de transporte o páginas web gubernamentales irán acompañados de una pena mayor, que podría alcanzar hasta 5 años de cárcel. Asimismo, se establecen sanciones penales para las empresas que contraten los servicios de un pirata informático para acceder a la base de datos de la competencia, contemplando incluso el cierre de sus establecimientos o el fin de las subvenciones públicas.

[1] Instituto Español de Ciberseguridad (SCSI, Spanish Cyber Security Institute). Informe La Ciberseguridad Nacional, un compromiso de todos. La necesidad de evolucionar de una cultura reactiva a una de prevención y resiliencia. Publicado en junio de 2012

Por otra parte, es importante resaltar la aprobación de la ***"Estrategia de Ciberseguridad de la UE",*** y en el ámbito específico de España, la **Estrategia de Seguridad Nacional 2013,** aprobada el pasado mes de junio, y que forman una articulación fundamental de la Seguridad Nacional como Política de Estado, al contener las directrices con el fin de reasignar todos los recursos disponibles del Estado de manera eficiente para la preservación de la Seguridad Nacional. Siendo **la ciberseguridad** uno de los principales ámbitos de actuación de dicha Estrategia**.**

Por último, es importante mencionar las normas jurídicas referentes en la materia como lo son:

- La **Directiva 2009/136/CE/** del Parlamento Europeo y del Consejo, de 25 de noviembre, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.

- La **Directiva 2009/140/CE** del Parlamento Europeo y del Consejo, de 25 de noviembre, por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

4.- Conclusiones y Recomendaciones: Ventajas legales de la solución e.Hotspot de e.Telecom

De la revisión de la normativa vigente, y la información expuesta en los puntos 1,2 y 3 del presente informe, podemos concluir y recomendar lo siguiente:

(i) Si los *gerentes, administradores, trabajadores o personal contratado* de los hoteles utiliza la conexión wifi en el ejercicio de sus funciones, la solución e.Hotspot de acceso a internet de e.Telecom puede ser una herramienta muy útil que permita *controlar* dichas actividades para evitar **responsabilidad penal** de la empresa, cuyas sanciones contempladas en el ***Código Penal***, pueden consistir en multas con una cuota diaria mínima de 30 € y máxima de 5.000 €, e incluso, disolución de la empresa (persona jurídica), suspensión de sus actividades o clausura del establecimiento.

(ii) La solución e.Hotspot de acceso a internet de e.Telecom ***permite la identificación*** *de los usuarios* en caso de detectar *un problema de seguridad en la red, localizar un contenido ilícito o haber identificado u observado una conducta que pudiera ser delictiva*. Asimismo, facilita al cliente (hoteles) ***información completa*** de los responsables de dichos actos, así como ***informes y reportes completos*** del servicio de conectividad de la red wifi, que podrá poner a disposición de los cuerpos de seguridad ante las eventuales solicitudes y requerimientos, en aras de reforzar la colaboración público-privada, necesaria para cumplir y garantizar la *"Estrategia de Ciberseguridad de la UE", y los objetivos previstos en la "*Estrategia de Seguridad Nacional de España 2013".

(iii) Facilita la colaboración con el incremento de la ***capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas*** y siempre podrás contar con el ***apoyo y asistencia de tu proveedor de servicios*** (e.Telecom), a los fines de cumplir con disposiciones de la ***nueva Directiva sobre ciberseguridad***, cuyo objetivo es facilitar la prevención e impulsar la cooperación policial y judicial en este ámbito, estableciendo un plazo máximo de 8 horas para responder a la información solicitada, en caso de que producirse un ciberataque.

(iv) La solución e.Hotspot de e.Telecom garantiza el fortalecimiento de la seguridad de los sistemas de la información y las redes de comunicaciones que soportan, así como la seguridad de la conexión wifi, en cumplimiento de las disposiciones previstas en la **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)**, **Ley 25/2007, de 18 de octubre,** de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones y la ***nueva Directiva sobre ciberseguridad.***

(v) Permite cumplir con el "***Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas****"* regulado en la ***Directiva 2006/24/CE*** *del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones*, y la **Ley 25/2007, de 18 de octubre,** *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*, que establece como obligación, el *Conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación (como lo son las redes wifi), y la cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales* (art.1 Ley 25/2007).

Así, los datos objeto de conservación serán los siguientes:

i) La identificación de usuario asignada; ii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono. iii) Con respecto al acceso a Internet, la fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado. iv) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario. v) Datos necesarios para identificar el tipo de comunicación y servicio de Internet utilizado y los vi) Datos necesarios para identificar el equipo de comunicación de los usuarios. (Art. 3 Ley 25/2007)

La obligación de conservación de los referidos datos ***cesa a los doce meses computados desde la fecha en que se haya producido la comunicación*** (Art. 5) y solo podrán ser cedidos previa autorización judicial, y únicamente a los agentes facultados.

Siendo importante destacar que a estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación. Si no se establece otro plazo distinto**, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden.**

El incumplimiento de las obligaciones antes mencionadas, constituyen una **infracción grave regulada en la Ley General de Telecomunicaciones (Ley 32/2003, de 3 de noviembre) con *multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio, el límite máximo de la sanción será de 500.000 euros*.**

Dichas infracciones graves, en función de sus circunstancias, podrán llevar aparejada amonestación pública, con publicación en el «Boletín Oficial del Estado» y en dos periódicos de difusión nacional, una vez que la resolución sancionadora tenga carácter firme. Todo ello, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

Por otra parte, en caso de revelar contenido de las conversaciones, o datos no previstos en la *ley 25/2007*, de conservación de datos; aplicará las disposiciones de la *Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), y su reglamento de desarrollo*, cuyo incumplimiento puede ocasionar infracciones leves (sancionadas con multa de 900 a 40.000 euros), graves (sancionadas con multa de 40.001 a 300.000 euros) o muy graves sancionadas con multa de (300.001 a 600.000 euros).

(vi) En el ámbito de ***propiedad intelectual,*** la ***Ley 2/2011, de 4 de marzo, de Economía Sostenible*** en su Disposición final cuadragésima tercera, modifica ***Ley de Propiedad Intelectual*** e introduce un nuevo apartado segundo del artículo 8 de la **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)** que señala lo siguiente:

"*Los órganos competentes con el objeto de identificar al responsable que está realizando la conducta presuntamente vulneradora,* ***podrán requerir a los prestadores de servicios de la sociedad de la información la cesión de los datos que permitan tal identificación a fin de que pueda comparecer en el procedimiento****. Tal requerimiento exigirá la previa autorización judicial de acuerdo con lo previsto en el apartado primero del artículo 122 bis de la Ley reguladora de la Jurisdicción contencioso-administrativa. Una vez obtenida la autorización,* ***los prestadores estarán obligados a facilitar los datos necesarios para llevar a cabo la identificación".***

Por ello, la solución e.Hotspot de e.Telecom te permite disponer de los datos de identificación de los usuarios, para que puedas cumplir con la Ley, en aras de proteger y salvaguardar los derechos de propiedad intelectual de terceros frente a una vulneración.

(vii) Por último, destacar que la solución e.Hotspot de e.Telecom, permite cumplir con las *obligaciones de información sobre seguridad* reguladas en la ***Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)*** que en su Artículo 12 bis destaca que: Los proveedores de servicios de intermediación establecidos en España que realicen actividades consistentes en la prestación de servicios de acceso a Internet (como en éste caso lo es el ofrecer conectividad y acceso a internet a través de wifi), *estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados. Igualmente, … informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia; y facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.*

Siendo una infracción leve el incumplimiento de las referidas obligaciones de información sobre seguridad, sancionada con multa de hasta 30.000 euros, cuya obligación a través de la solución e.Hotspot de e.Telecom podrás cumplir.

En Madrid, a 17 de julio de 2013

Reciban un cordial saludo,

Sor Arteaga

LeQuid