SEGURIDAD ELECTRÓNICA (ALGUNAS REFLEXIONES EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS PERSONALES Y DE LOS ENLACES ELECTRÓNICOS)

ELECTRONIC SECURITY (SOME REFLECTIONS ON THE SCOPE OF THE PROTECTION OF PERSONAL DATA AND ELECTRONIC LINKS)

PATRICIA MÁRQUEZ LOBILLO[1]

Sumario: I. INTRODUCCIÓN. II. SEGURIDAD ELECTRÓNICA Y PROTECCIÓN DE DATOS EN LA PROPUESTA DE REGLAMENTO DE 2012. III. SEGURIDAD ELECTRÓNICA Y ENLACES ELECTRÓNICOS.

Summary: I. INTRODUCTION. II. ELECTRONIC SECURITY AND DATA PROTECTION IN THE PROPOSED REGULATION, 2012. III. ELECTRONIC SECURITY AND LINKS.

I. INTRODUCCIÓN

Hace ya años que vieron la luz la Directiva sobre el comercio electrónico[2]; la Directiva sobre firma electrónica[3]; o aquellas Directivas y Reglamentos que tuvieron como objetivo garantizar un elevado nivel de protección de las personas en el tratamiento de datos personales[4], por mencionar algunas normas relevantes para nuestro trabajo y sin ánimo exhaustivo. En líneas generales, el objetivo propuesto por el legislador comunitario no era otro que garantizar a los usuarios o destinatarios de servicios *on line*, en general, y a los consumidores en particular, un nivel adecuado de protección y de seguridad, jurídica, de la información, de los datos personales, etc. que garantizase el correcto funcionamiento del Mercado interior de prestación de servicios de la sociedad de la información y contribuyese a incentivar la competitividad empresarial, sin poner en peligro los derechos y libertades de los ciudadanos europeos.

[1] Profesora Contratada Doctora de Derecho Mercantil de la Universidad de Málaga.

[2] Directiva 2000/31/CE, del Parlamento Europeo y del Consejo de 8 de junio de 2000, relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior («Directiva sobre el comercio electrónico»)

[3] Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica.

[4] Así, la propia Directiva sobre protección de datos del año 1995, o el Reglamento (CE) 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Sin olvidar, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Han sido, desde entonces, muchas las voces que hemos demandado el establecimiento de un marco jurídico adecuado para garantizar la ansiada seguridad electrónica[5], proviniese el mismo de los órganos legitimados para dictar normas o de la combinación de las disposiciones legales con las normas derivadas de los mecanismos de autorregulación[6].

El paso del tiempo no ha permitido hablar de seguridad electrónica, o al menos, no ha posibilitado hacerlo con total seguridad jurídica.

Es más, la evolución de las tecnologías de la información y la comunicación, en los últimos dos años, con la aparición de las Redes sociales, la *web 2.0.*, la ya *web 3.0.*, el empleo de RPA[7] con funciones privadas y la consiguiente obtención de imágenes y datos que permitan la localización e identificación de personas, o el *cloud computing*, por mencionar algunos ejemplos de una larga lista que sería prácticamente imposible reproducir, han reavivado los debates sobre la necesidad de proporcionar un elevado nivel de seguridad electrónica, de seguridad de la información y, en nuestro entendimiento de la misma, de seguridad jurídica, en las actividades y transacciones que se llevan a cabo en Internet.

De hecho, garantizar un elevado nivel de seguridad de las Redes y de la información (SRI) sigue siendo el caballo de batalla del legislador comunitario, como puede deducirse de la presentación, el 7 de febrero de 2013 de una Propuesta de Directiva cuyo objetivo principal es precisamente ese[8].

Se propone, entre otras cosas, instar a los Estados a la cooperación entre ellos en materia de seguridad; y, exigir a los operadores de infraestructuras críticas (la banca, la bolsa, el transporte y la distribución de energía, los transportes aéreo, ferroviario y

[5] Ya nos pronunciamos sobre la materia en P. MÁRQUEZ LOBILLO, *Empresarios y profesionales en la sociedad de la información*, Edersa, 1ª ed., Madrid, 2004, y hemos reiterado nuestras demandas en "El consumidor en la contratación electrónica de servicios turísticos", *Revista de Derecho Mercantil*, núm. 282, págs. 209 y ss. *Vid.* A. MADRID PARRA, "Contratación electrónica y protección de datos personales", *Revista de la Contratación Electrónica*, nº 94, junio, 2008; J.I. PEINADO GRACIA, "La edad del Derecho, la edad de Internet. La seguridad jurídica e Internet", en VV.AA., *e-Abogacía*, Madrid, 2007; T. VÁZQUEZ RUANO, *La protección de los destinatarios de las comunicaciones comerciales electrónicas*, Marcial Pons, 1ª ed., Madrid, 2008.

[6] De forma detallada, *vid*., P. BENAVIDES VELASCO, "Los sellos y marcas de calidad (*trustmarks*) en el mercado digital y el Distintivo Público de Confianza en línea", en VV.AA., *Marca y publicidad comercial. Un enfoque interdisciplinar*, dir. Martínez Gutiérrez, A., Madrid, 2009.

[7] Los RPA son vehículos aéreos no tripulados. Empleados en un principio en funciones esencialmente militares, su uso cada vez más generalizado en el ámbito civil ha acrecentado el debate en torno al posible establecimiento o no de límites a la protección a la privacidad de las personas, tanto en lo relativo a la protección de sus datos personales, como de la propiedad privada y la propia imagen. Nuestras conclusiones sobre esta materia serán presentadas junto a las Dras. Guerrero Lebrón y Cuerno Rejano, en la conferencia *"Aeronaves no tripuladas (UAS). Estado de la legislación para realizar su integración en el espacio aéreo no segregado"*, que se pronunciará el 17 de octubre de 2013, en Bilbao, en el Seminario "Nuevos retos del Derecho del transporte: competencia, documentación, responsabilidad y seguridad".

[8] Propuesta de Directiva del Parlamento Europeo y del Consejo, de 7 de febrero de 2013, relativa a las medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión, COM (2013) 48 final.

marítimo, la sanidad, los servicios de Internet y las administraciones públicas) y a los proveedores clave de servicios de la sociedad de la información (plataformas de comercio electrónico, redes sociales, etc.), así como a las administraciones públicas, que adopten las medidas oportunas para gestionar los riesgos de seguridad y notificar los incidentes graves a las autoridades nacionales competentes.

Se considera que en el ámbito de la Unión Europea es necesario abordar la SRI de forma radicalmente distinta. Lo primero, es establecer un marco jurídico uniforme que colme las actuales lagunas jurídicas. La futura norma, en este sentido, pretende, por un lado, obligar a los Estados miembros a velar porque exista un nivel mínimo de capacidades nacionales mediante la designación de autoridades competentes en materia de SRI, la creación de equipos de respuesta a emergencias informáticas (CERT) y la adopción de estrategias y planes de cooperación nacionales en el ámbito de la SRI. En segundo lugar, las autoridades nacionales competentes deberán cooperar dentro de una red que garantice una coordinación segura y eficaz y, en particular, un intercambio coordinado de información y unas labores de detección y respuesta a escala de la Unión Europea.

A través de esta red, los Estados miembros deberán intercambiar información y cooperar para hacer frente a las amenazas e incidentes que puedan poner en peligro la SRI, sobre la base del plan de cooperación europeo en la materia.

En tercer lugar, siguiendo el modelo de la Directiva Marco sobre las comunicaciones electrónicas, se pretende la implantación de una cultura de gestión de riesgos, que ha de combinarse con la garantía del intercambio de información entre los sectores público y privado. Las empresas de los sectores críticos concretos antes citados y las administraciones públicas deberán evaluar los riesgos a que se enfrentan y adoptar medidas adecuadas y proporcionadas para garantizar la SRI. Estas empresas deberán notificar a las autoridades competentes todos los incidentes que supongan un peligro grave para el funcionamiento de sus redes y sistemas de información y comprometan de forma significativa la continuidad de los servicios críticos y el suministro de mercancías.

II. SEGURIDAD ELECTRÓNICA Y PROTECCIÓN DE DATOS EN LA PROPUESTA DE REGLAMENTO DE 2012

El establecimiento de mecanismos adecuados para garantizar la protección de los datos personales en Internet, compatible con la libre circulación de los mismos entre los Estados miembros, ha sido una constante en la política legislativa comunitaria.

Consciente del hecho de que la evolución tecnológica supone un reto en la materia, debido a la magnitud que ha alcanzado el intercambio y la recogida de datos personales, y la facilidad que, en orden a la utilización de los mismos permiten las tecnologías, sin olvidar que las personas difunden a través de las redes sociales un volumen de información personal incalculable, el legislador comunitario, en la

Propuesta de Reglamento sobre protección de datos del año 2012[9], pone de relieve la importancia que posee la seguridad y la confianza en el entorno *on line* como baluarte del desarrollo económico europeo, destacando el papel fundamental que, en este sentido ostenta, la garantía de un elevado nivel de protección de datos[10] (Considerando quinto).

Se parte del hecho de que si bien los objetivos y principios del marco normativo actual siguen siendo adecuados, no han evitado, la fragmentación en la aplicación por parte de los Estados miembros de las normas sobre protección de datos, como tampoco han paliado los problemas de inseguridad jurídica, ni han contribuido a evitar la percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad *on line*.

…Ha llegado por ello el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas...

Ese parece ser el objetivo de la Propuesta del que, sin ánimo exhaustivo, queremos resaltar aquellos aspectos que, en nuestra opinión, contribuyen considerablemente a incrementar el nivel de protección-seguridad en materia de datos personales recogidos y tratados en el marco de actividades en línea, propiciando, en definitiva, un elevado nivel de seguridad electrónica que contribuya al crecimiento económico de Europa.

En este sentido, destaca la consagración legislativa del principio de neutralidad tecnológica en materia de protección de datos personales, a fin de conseguir que los mecanismos protectores se apliquen siempre y en todo caso, con independencia del medio o tecnología empleada para la obtención y tratamiento de los datos, pretendiéndose con ello evitar riesgos de elusión del régimen jurídico propuesto (Considerando décimo tercero).

De especial relieve, por el carácter transnacional de las actividades electrónicas, son las previsiones sobre la aplicación de las normas contenidas en el Reglamento a

[9] Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), de 25 de enero de 2012, COM (2012) 11 final. *Vid.* el exhaustivo comentario de la misma de F.J. SEMPERE SAMANIEGO, *Comentarios prácticos a la Propuesta de Reglamento de Protección de Datos de la Unión Europea*, 2013, http://www.privacidadlogica.es/wp-content/uploads/2013/09/comentarios-reglamento-pdatos_Javier-Sempere-Samaniego.pdf.

[10] Así se reconoce en la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Una Agenda Digital para Europa*, de 28 de agosto de 2010, COM (2010) 245 final, afirmando de forma gráfica que *"Los europeos no adoptarán una tecnología en la que no confíen; la era digital no es ni el «Gran hermano» ni el «salvaje oeste cibernético»"*; así como, en la Comunicación de la Comisión, *Europa 2020. Una estrategia para el crecimiento inteligente, sostenible e integrador*, de 3 de marzo de 2010, COM (2010) 2020 final.

interesados que residen en la Unión Europea, cuando el tratamiento se lleve a cabo por parte de responsables no establecidos en la Unión, atendiéndose para ello al criterio de "control de la conducta". Para constatar la existencia de dicho control habrá de evaluarse si las personas físicas son objeto de un seguimiento en internet con técnicas de tratamiento de datos que consistan en la aplicación de un «perfil» a un individuo con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes (Considerandos vigésimo y vigésimo primero).

Creemos que resulta fundamental, igualmente, el reconocimiento, de forma expresa, de la vigencia y aplicación de las normas sobre responsabilidad de los prestadores de servicios de la sociedad de la información contenidas en la Directiva sobre el comercio electrónico (Considerando décimo séptimo)[11].

Se establece de forma clara la consideración de datos personales de los identificadores en línea facilitados por las personas físicas a través de sus dispositivos, aplicaciones, herramientas y protocolos, así como mediante las direcciones de los protocolos de internet o los identificadores de sesión almacenados en *cookies*. Si bien, se reconoce, que no siempre y en todo caso, dichos datos tendrán la consideración de personales, como sucede en cualquier otro supuesto (Considerando vigésimo cuarto y art. 4).

La exigencia de consentimiento expreso al tratamiento de datos personales no planteará, de aprobarse la Propuesta (art. 4), duda alguna, considerando el legislador manifestado el mismo *…mediante la selección de una casilla de un sitio web en internet o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales…* De tal forma que, *…si el consentimiento del interesado se ha de dar a raíz de una solicitud electrónica, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta...* (Considerando vigésimo quinto).

Partiendo de la necesaria licitud en la recogida y el tratamiento de datos personales, asentada en los antecedentes legislativos de la Propuesta y en el propio articulado de la misma[12], se entiende que el interés legítimo de un responsable puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, al que, en cualquier caso, asiste el derecho a oponerse al tratamiento alegando motivos que tengan que ver con su situación particular (Considerando trigésimo octavo).

[11] De las mismas nos hemos ocupado, con detenimiento, en P. MÁRQUEZ LOBILLO, "Responsabilidad derivada de la prestación de servicios de la sociedad de la información", en VV.AA. (Coords. A. Parra y Mª J. Guerrero Lebrón), *Derecho patrimonial y tecnología: revisión de la contratación electrónica con motivo del Convenio de las Naciones Unidas sobre Contratación electrónica de 23 de noviembre de 2005 y de las últimas novedades legislativas*, Madrid, 2007 y en "Prestadores de servicios de intermediación: algunas especialidades de su estatuto jurídico", *Revista de la Contratación Electrónica*, nº 88, 2007.

[12] *Vid.* arts. 6 y ss.

La seguridad electrónica adquiere, en este punto, un papel fundamental, por entender el legislador comunitario que concurre el exigido interés legítimo al tratamiento, en la medida estrictamente necesaria a efectos de garantizar la seguridad de red e información, a saber, la capacidad de un sistema de red o de información de resistir, en un nivel determinado de confianza, acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, y la seguridad de los servicios afines ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de las autoridades públicas, los equipos de respuesta a emergencias informáticas (CERT), los equipos de respuesta a incidentes de seguridad informática (CSIRT), los proveedores de redes y servicios de comunicaciones electrónicas y los proveedores de tecnologías y servicios de seguridad. Se trataría, por ejemplo, de impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, así como detener ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas (Considerando trigésimo noveno).

En orden al cumplimiento de las exigencias de información sobre el responsable del tratamiento y el objetivo que subyace en la recogida de datos debe destacarse la exigencia contenida en el Considerando cuadragésimo sexto de la Propuesta. El principio de transparencia, dice el legislador comunitario, exige que toda información dirigida al público o al interesado sea fácilmente accesible y fácil de entender, lo que resulta especialmente pertinente …*cuando, en determinadas situaciones, como la publicidad en línea, la proliferación de agentes y la complejidad tecnológica de la práctica, resulte difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, los datos personales que le conciernen*…

En cuanto al régimen del derecho de acceso a los datos personales, se prevé que el responsable del tratamiento deberá utilizar todas las medidas razonables para verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea, sin que pueda conservar datos personales con el único propósito de poder responder a posibles solicitudes (Considerando quincuagésimo segundo).

Destaca, en este sentido, y en orden al ejercicio de los derechos de oposición, rectificación y cancelación, la regulación del denominado "derecho al olvido"[13] o derecho de la persona física a que se rectifiquen los datos que le conciernen cuando los mismos no se ajusten a las previsiones establecidas en el Reglamento.

Se considera que a los interesados ha de asistirles el derecho a que se supriman y no se traten sus datos personales, en caso de que ya no sean necesarios para los fines para los que fueron recogidos o tratados de otro modo, de que los interesados hayan retirado su consentimiento para el tratamiento, de que se opongan al tratamiento de

[13] M.A. DAVARA RODRÍGUEZ, "El derecho al olvido en Internet", *Diario La Ley*, núm. 8137, 30 de julio de 2013. *Vid*. art. 17 de la Propuesta de Reglamento.

datos personales que les conciernan o de que el tratamiento de sus datos personales no se ajuste de otro modo a lo dispuesto en el presente Reglamento. Salvo, que, como indica el legislador, la posterior conservación de los datos debe autorizarse cuando sea necesario para fines de investigación histórica, estadística y científica, por razones de interés público en el ámbito de la salud pública, para el ejercicio del derecho a la libertad de expresión, cuando la legislación lo exija, o en caso de que existan motivos para restringir el tratamiento de los datos en vez de proceder a su supresión (Considerando quincuagésimo tercero).

Con el fin de reforzar este «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que los responsables del tratamiento que hayan hecho públicos los datos personales estén obligados a informar a los terceros que estén tratando tales datos, de que un interesado les solicita que supriman todo enlace a sus datos personales, o las copias o réplicas de los mismos. A fin de garantizar el cumplimiento de este deber, se impone al responsable del tratamiento el deber de tomar todas las medidas razonables, incluidas las de carácter técnico, en relación con los datos cuya publicación sea de su competencia. Se afirma, además, en relación con la publicación de datos personales por un tercero, que el responsable del tratamiento debe ser considerado responsable de la publicación, cuando haya autorizado para ello a dicho tercero.

El control sobre los propios datos y el derecho de acceso de los interesados se refuerza, en los supuestos de tratamiento por medios electrónicos, en un formato estructurado y de uso habitual, concediéndoles el derecho a obtener una copia de los datos que les conciernan, también en formato electrónico de uso habitual. Asimismo se debe autorizar a los interesados a transmitir de una aplicación automatizada, como una red social, a otra aquellos datos que hayan facilitado. Tal debe ser el caso cuando el interesado haya facilitado los datos al sistema automatizado de tratamiento, dando su consentimiento o en cumplimiento de un contrato (Considerando quincuagésimo quinto y art. 18).

III. SEGURIDAD ELECTRÓNICA Y ENLACES ELECTRÓNICOS

La mención expresa de la problemática en materia de seguridad electrónica, seguridad jurídica y enlaces electrónicos en este trabajo, nos ha surgido a raíz de la lectura de la magnífica monografía publicada por Vázquez Ruano[14].

La cantidad de información presente en un entorno como Internet, y la complejidad en la que la misma puede llegar a presentarse, justifica el empleo de *links* o enlaces[15] que, insertos en la página de un determinado prestador, permiten a los

[14] T. VÁZQUEZ RUANO, *La inserción de enlaces en una web: Cuestiones de propiedad industrial y competencia desleal*, Marcial Pons, 1ª ed., Madrid, 2013.

[15] No podemos olvidar, en este sentido, que la propia norma española sobre comercio electrónico, la Ley 34/2002, de 12 de julio, permite el recurso a hipervínculos que contengan la información que exige a los prestadores de servicios de la sociedad de la información, así, por ejemplo, en materia de información sobre los códigos de conducta a los que esté adherido el prestador.

usuarios que cliquean en los mismos el acceso a otro sitio de Internet diferente, a otra página distinta de aquella en la que se encuentra. Otra forma de realizar dichos acceso es la que se lleva a cabo por los conocidos buscadores de información, quienes como sabemos utilizan robores de rastreo de espacios *on line* a fin de crear bases de datos con las referencias a sitios de terceros, relacionando dichos sitios con palabras claves.

El recurso a esta técnica electrónica plantea problemas de diversa naturaleza, relacionados con posibles lesiones, a las libertades de información y expresión; a los derechos a la propiedad intelectual y de autor; a la competencia leal que ha de presidir el funcionamiento del Mercado.

A simple vista, parece que no requiere mayor explicación el hecho de que cualquier prestador es libre de enlazar en su página de Internet todas las páginas que estime convenientes, siempre que, cuando lo haga respete las normas sobre comercio electrónico, propiedad intelectual y competencia[16]. Se trata, en definitiva, del principio *free link* o de libertad de enlace, vistos como una manifestación, entendemos clara, de los derechos constitucionales a la libertad de información y de expresión, insistimos, siempre que la misma se acomode al ordenamiento jurídico.

Se plantea, en este sentido, la necesidad de establecer una diferencia que la Dra. Vázquez aborda de forma sumamente acertada, y que está íntimamente relacionada con el carácter absoluto o no del principio *free link*. Así las cosas, puede suceder que el prestador a cuya página se dirige el enlace haya previsto técnicas que impidan o simplemente controlen el acceso al espacio que se inserta en la Red[17], de tal forma que sea necesaria la obtención de una autorización previa para que dicho enlace pueda realizarse. También puede suceder[18] que el prestador no emplee dichas técnicas, de tal forma que cualquiera pueda enlazar su página en otro *site*, generándose una suerte de consentimiento presunto al enlace que, de no presumirse podría suponer un grave riesgo para el propio funcionamiento de la Red.

Otro de los problemas que reseña la autora y que consideramos debe referenciarse es el que se genera cuando se ejecutan los enlaces, pues en tal caso se realizan copias temporales de los contenidos ajenos disponibles en la Red, a fin de que los usuarios puedan visualizarlos. De conformidad con lo establecido en el artículo 31 del Texto Refundido de la Ley de Propiedad Intelectual (TRLPI), no será necesario

[16] Ya tuvimos oportunidad de pronunciarnos sobre el particular, afirmando que el hecho de que todo esté disponible en la Red no justifica, en ningún caso, que pueda conculcarse el ordenamiento jurídico al que, de forma expresa, se remite el art. 1.2 de la Ley de Comercio electrónico española. *Vid.* P. MÁRQUEZ LOBILLO, "El almacenamiento en la memoria caché como limitación del artículo 31 TRLPI (A propósito de la Sentencia de la Audiencia Provincial de Barcelona de 17 de septiembre de 2008)", *Cuaderno Mercantil*, Sepin, nº 2, enero, 2009.

[17] Pensemos, por ejemplo, en el empleo de recursos electrónicos que impidan que los rastreadores *on line* empleados por los motores de búsqueda puedan localizar tu página, de tal forma que, si quieren incluir la misma en el buscador deban recabar tu consentimiento.

[18] Y en nuestra opinión es lo más habitual si tenemos en cuenta que la finalidad del que crea una página de Internet no es otra que obtener el mayor número de visitas de la misma, sobre todo si posee carácter comercial.

recabar la autorización del autor de una obra en los supuestos de reproducción provisional, carente por sí misma de una significación económica independiente, que sean transitorios o accesorios y que formen parte integrante y esencial de un proceso tecnológico, con la única finalidad de facilitar la transmisión en red, entre terceras partes, por un intermediario. Las posibles lesiones a los derechos de propiedad intelectual en el empleo de enlaces o *links* no son pensables cuando hablamos de los denominados enlaces simples, planteándose mayores inconvenientes en los casos de enlaces complejos (enlaces de profundidad, *frames*, *P2P links*…)[19]. Así las cosas, cuando se produzca un mero enlace, sin alteración del contenido, estaremos ante una conducta amparada en la excepción del artículo mencionado. No así en aquellos casos en los que cuando se pulse el enlace la página no se perciba en la forma en la que la ha previsto su titular. No cabrá entender que existe consentimiento presunto alguno al cambio, debiendo el prestador que realiza el enlace solicitar en consentimiento expreso del titular del *site* que quiere enlazar, para introducir dichas modificaciones (licencias de uso o *web linking agrement*).

Hay otro aspecto que no ha quedado resuelto en los más de diez años de vigencia de la norma sobre comercio electrónico española, aspecto que, además, genera una importante inseguridad jurídica y electrónica, y potencia, en nuestra opinión, la desconfianza de los usuarios de Internet. Nos referimos al régimen de responsabilidad de los prestadores de servicios de intermediación, que tantos pronunciamientos judiciales ha motivado y que tantos quebraderos de cabeza nos ha ocasionado a aquellos que hemos tratado la materia[20]. Conforme a las normas sobre comercio electrónico, el prestador de servicios que se limite a enlazar páginas de terceros o que facilite instrumentos de búsqueda, mediante enlaces en definitiva, no va a ser considerado responsable del contenido enlazado, salvo que hubiera tenido conocimiento efectivo acerca de la ilicitud de la actividad o de la información enlazada; o cuando teniéndolo hubiera actuado diligentemente eliminando o inutilizando el vínculo; y ello, siempre que no actúe bajo la dirección, autoridad o control del prestador que facilita la localización. Y suerte que la problemática generada en la práctica ha llevado a nuestro Tribunal Supremo a entender que para que exista dicho conocimiento efectivo no es necesario un pronunciamiento judicial previo.

---

[19] Sumamente acertado nos parece el pronunciamiento, en este sentido, de la Audiencia Provincial de Madrid, en su Auto de 11 de septiembre de 2008, en el que el ponente afirma que …*el enlace simple o de superficie no supone infracción de los derechos de propiedad intelectual. Este tipo de links constituye únicamente una forma de facilitar al usuario de Internet el acceso a otra página web sin tener que «teclear» el nombre de esa página*… mientras que, en otros supuestos, como es el caso de los enlaces complejos (enlaces de profundidad, frames, P2P links…) y, en general, cuando …*existe reproducción de la página web ajena dentro de la propia*…, podríamos hablar de infracción de los derechos de propiedad intelectual puesto que no existe la provisionalidad y temporalidad exigida por la norma reguladora de dichos derechos, como mecanismo necesario para que el enlace cumpla la función que le es propia (Fundamento de Derecho sexto). En la misma línea se había pronunciado la Audiencia Provincial de Navarra, en sentencia de 20 de diciembre de 2007 y la Audiencia Provincial de Madrid, en Auto de 18 de junio de 2008.

[20] *Vid. supra*, nota 11 y más recientemente, P. MÁRQUEZ LOBILLO, "Telecinco *versus* Youtube: nada nuevo bajo el sol. Sobre la responsabilidad de los prestadores de servicios de intermediación", *Cuaderno Mercantil*, Sepin, septiembre, 2010.

Compartimos con la Dra. Vázquez, por último, la necesidad de diferenciar entre enlaces o *links* promocionales y aquellos que no lo son, sobre todo si tenemos en cuenta que los datos que permitan el acceso de manera directa al espacio de un tercero no tienen, *per se* la consideración de comunicación comercial, conforme a lo establecido en la norma sobre comercio electrónico. Y decimos que es necesaria la diferenciación porque, como es obvio, el tratamiento de los problemas que puedan derivarse de los *links* según sean o no promocionales, desde la óptica de la protección de los signos distintivos y del derecho de la competencia desleal es completamente diferente. Excede del objeto de nuestro trabajo entrar en la mencionada problemática, limitándonos a ponerla de relieve y a recomendar, encarecidamente, la obra de la Dra. Vázquez Ruano.