

EL IMPACTO DE LAS TIC EN LA CONFIGURACIÓN CLÁSICA DEL DERECHO. ESPECIAL REFERENCIA AL PRINCIPIO DE TERRITORIALIDAD

Víctor Almonacid Lamelas

*Secretario de la Administración Local, categoría superior
Director del Observatorio de Administración Electrónica y Transparencia de COSITAL*

Xavier Sancliment Casadejús

*Ingeniero de Telecomunicaciones, Electrónica e Informática
Licenciado en Psicología y Executive MBA
CEO Peakway*

Este trabajo ha sido seleccionado para su publicación por: don Carlos FRANCISCO MOLINA DEL POZO, doña M.^a José ACHÓN BRUÑÉN, don Xabier ARZOZ SANTISTEBAN, don Jorge BOTELLA CARRETERO, don JAVIER CREMADES GARCÍA y don Vicente MORET MILLÁS.

EXTRACTO

La multiplicidad de poderes legislativos consolidada a finales del siglo pasado (con el Derecho internacional y el europeo) alcanza su mayor grado de complejidad con la masificación de internet y el surgimiento de un probablemente necesario nuevo marco de autorregulación, algo similar a un nuevo «legislador» o poder legislativo, constituido por los gigantes de la red. La existencia de esta nueva rama del Derecho (¿lo es?), pero por encima de todo la desaparición del espacio físico, choca directamente con el clásico principio de territorialidad que caracterizaba al Derecho tal y como lo hemos conocido. Al respecto surgen infinidad de preguntas y cuestiones, algunas jurídicamente muy interesantes y otras que ciertamente nos causan bastante preocupación. Lo principal es, ante todo, ser conscientes de esta nueva situación de «extraterritorialidad», y a partir de ahí resolver las nuevas relaciones jurídicas o con efectos de Derecho que se produzcan. El debate sobre la necesidad de una *internacional ciberlaw*, o de la respuesta inmediata de cada Estado ante cada situación, o la mera confianza en este sistema hasta cierto punto «autorregulado», es una cuestión que podemos simplemente plantear y dejar abierta, si bien parece claro que la respuesta más atinada solo puede venir por una inteligente combinación de todas las soluciones. En realidad esta materia es inabordable en un solo estudio, por lo que en el presente nos hemos centrado en las relaciones de Derecho privado –contractuales y extracontractuales–, y el impacto de la problemática en relación con la propiedad intelectual y en el Derecho Penal. Trataremos de demostrar que el «Derecho de las TIC» no es una nueva rama del Derecho, sino más bien un nuevo escenario donde se producen relaciones y efectos jurídicos.

Palabras claves: derecho TIC, internet, territorialidad, sociedad de la información, contratos por internet, propiedad intelectual y delitos informáticos.

Fecha de entrada: 30-04-2015 / Fecha de aceptación: 30-06-2015

THE IMPACT OF ICT IN CLASSIC SETTING LAW. SPECIAL REFERENCE TO THE PRINCIPLE OF TERRITORIALITY

Víctor Almonacid Lamelas

Xavier Sancliment Casadejús

ABSTRACT

The multiplicity of legislative powers established by the end of the last century (with International and European Law) reached its highest level of complexity with the massification of the internet and the emergence of a new and necessary self-regulatory framework, probably something similar to a new «legislator» or «legislative power» consisting of the giants of the network. Does this mean that the existence of this new branch of law is, above all, the disappearance of physical space, colliding directly with the traditional principle of territoriality that characterized law as we have known it.

Regarding the infinity of questions and issues, some legal and others which are very interesting indeed, have caused the arise of considerable concern. The main point is, first of all, to be aware of this new situation of «extraterritoriality», and thereafter meet the new legal or law effects of these new relationships. The debate on the need for International Cyberlaw, or the immediate response to the new situations or amere confidence in this «self-regulated» system to some extent. It is an issue that can simply be raised and left open, although there is clearly a more judicious answer which can only a result of a clever combination of all solutions.

In fact this area is not going to be covered in just one project, so we have focused on the relationships of Private Law –extracontractual and contractual–, and the impact of the problems related to intellectual property and criminal law. We try to prove that «ICT Law» is not a new area of law, but rather a new scenario where relations and legal effects are produced.

Keywords: ICT legislation, Internet, territoriality, knowledge society, e-commerce, intellectual property and cybercrime.

Sumario

- I. Introducción
- II. Obligaciones contractuales
 - A. Regla general: Punto de conexión aplicable; libertad de elección de las partes
 - B. Excepciones a la regla general: Ley aplicable a falta de elección
- III. Incidencia del principio de territorialidad en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
 - A. Servicios de la sociedad de la información
 - B. Contratación electrónica
- IV. Obligaciones extracontractuales
 - A. Ley aplicable a obligaciones derivadas de hechos dañosos
 - B. Ley aplicable a las obligaciones derivadas de gestión de negocios ajenos, enriquecimiento injusto y *culpa in contrahendo*
- V. Propiedad intelectual
 - A. Reglamento de Bruselas I. Propiedad intelectual, lugar de infracción o comisión del ilícito
 - B. Dificultad de la determinación del *forum loci acti* / *forum loci damni* en internet
 - C. Ley aplicable: Artículo 8 de «Roma II» (obligaciones extracontractuales)
- VI. Delitos TIC y delitos a través de las TIC
 - A. Posiciones doctrinales que defienden la innecesariedad de una nueva regulación, «desregularización»
 - B. Posiciones doctrinales que defienden la necesidad de una nueva regulación específica en esta materia
 - C. Nuestra posición
- VII. Conclusiones

Bibliografía

El derecho es el conjunto de condiciones que permiten a la libertad de cada uno acomodarse a la libertad de todos

Immanuel Kant

I. INTRODUCCIÓN

El ámbito de producción normativa ha evolucionado hacia sistemas progresivamente más complejos desde la separación de poderes y la institucionalización de un legislativo independiente. De forma concreta, España es un país territorialmente complejo. En la multiplicidad de poderes normativos que se han ido consolidando entendemos que en la actualidad destacan dos de ellos por encima del resto: el más elevado (normas de Derecho internacional y normas de Derecho europeo) y el más próximo (ordenanzas municipales). Pensamos que estas ordenanzas, y en general el ejercicio de la potestad reglamentaria por parte de las entidades públicas, no solo ayuntamientos, que la detentan, son extremadamente útiles para adaptar la legislación estatal, en ocasiones genérica y distante, a las circunstancias y situaciones que presenta una determinada realidad o entorno (territorial o sectorial). El ejercicio de esta potestad reglamentaria debería practicarse, entendiéndose, de forma moderada, a fin de no sobrecargar en exceso el ordenamiento jurídico.

El siguiente hito evolutivo, que causa un impacto sin precedentes en el ámbito legal, es internet. En el año 2015 ya no vivimos únicamente en el mundo físico, sino también en el mundo virtual, el cual sin embargo es tan real como el anterior. Cada uno de nosotros tiene al menos dos o tres identidades digitales, por medio de las cuales también actuamos –muchas veces con efectos de Derecho–, además de una firma electrónica –eDNI o equivalente– que nos habilita para operar en el mundo jurídico electrónico con total capacidad.

Bert Koenders, ministro de Asuntos Exteriores del Gobierno de los Países Bajos, en un congreso sobre ciberespacio llegó a describir que «el reto principal de las sociedades del siglo XXI es cómo hacer que internet sea libre, abierto y seguro. "Libre", para que todo el mundo tenga acceso a internet y las oportunidades sin precedentes que ofrece. "Abierto", para que la información pueda fluir sin obstáculos entre los usuarios en un único ciberespacio, y "seguro", porque los datos personales estén protegidos y la privacidad, salvaguardada».

Pero la desaparición del espacio físico choca directamente con el clásico principio de territorialidad que caracteriza al Derecho tal y como lo hemos estudiado hasta el momento. En este sentido podemos hablar de «extraterritorialidad» de la red, o bien, incluso de manera aún más correcta, de «multiterritorialidad». ¿Cómo resolver esta cuestión? ¿Es necesaria una *internacional ciberlaw*, o quizá algún tratado u órgano internacional puntual, o el ordenamiento jurídico vigente tiene respuesta suficiente y adecuada ante la actual realidad sociotecnológica? ¿El «Derecho de

las TIC» es una nueva rama del Derecho que merece incluso la configuración de una jurisdicción propia? ¿Cómo es posible que un usuario español de WhatsApp se someta a las normas sobre protección de datos del estado de California? ¿Dónde residen y qué ley se aplica a los «prestadores de servicios»? ¿Y a los ciberdelincuentes?

En las siguientes líneas trataremos de demostrar que no se debe regular lo ya regulado, pero tampoco acaso pasar por alto una nueva realidad huérfana –parcialmente– de regulación, lo cual le daría al presente cierta vocación *de lege ferenda*. En todo caso, la mayoría de problemas actuales se resuelven con la legislación vigente y por la vía de la interpretación, ya que tenemos la suerte de contar con tres fantásticas fuentes del Derecho perfectamente aplicables a esta nueva posible rama que algunos han bautizado como «Derecho de las TIC»: el Código Civil, el Derecho europeo y los mismos principios generales del Derecho, y es que frente a la revolución tecnológica quizá lo más sensato es regresar al Derecho natural y, por qué no decirlo, al sentido común.

II. OBLIGACIONES CONTRACTUALES

Partiendo de la teoría clásica que parte de la dicotomía *contratos entre presentes-contratos entre ausentes*, tenemos que con la incorporación de las TIC al ámbito comercial y contractual –público y privado– predomina claramente el segundo tipo de relaciones contractuales. Es importante determinar la ley aplicable al contrato, en cuanto que la misma regirá su interpretación, el cumplimiento, las sanciones derivadas del incumplimiento de obligaciones, la evaluación del daño, la extinción de las obligaciones, el ejercicio de acciones y las consecuencias de la nulidad del contrato.

En materia de derechos reales, nuestro ordenamiento jurídico ha optado tradicionalmente por un criterio que también es esencialmente real, vinculado en numerosas ocasiones con el principio de territorialidad. Aunque los preceptos del Código Civil en esta materia han quedado básicamente desfasados, especialmente el artículo 10 –epígrafe 5 en relación con las obligaciones contractuales y epígrafe 9 por lo que respecta a las obligaciones extracontractuales–, todavía establecen reglas más o menos válidas que en determinados supuestos pueden servir de cauce interpretativo.

En efecto, en materia de obligaciones contractuales, el artículo 10.5 parte de la primacía del principio de autonomía de la voluntad de las partes, si bien establece una serie de puntos de conexión con el contrato en cascada descendente, fijando en última instancia como cláusula de cierre el lugar de celebración del contrato. El principio de territorialidad queda pues perfilado de la siguiente forma y orden:

- La ley a que las partes se hayan sometido expresamente, siempre que tenga alguna conexión con el negocio de que se trate.
- En su defecto, la ley nacional común a las partes.
- A falta de ella, la de la residencia habitual común.
- En último término, la ley del lugar de celebración del contrato.

En esta cuestión, el impacto del comercio electrónico y la contratación telemática –partiendo de la premisa de que las partes contrayentes están lo suficientemente alejadas como para residir bajo ordenamientos jurídicos distintos– queda en los últimos tiempos minimizado, al menos en el importante ámbito económico europeo, por una buena regulación contenida esencialmente en la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información –en la que a su vez se basa la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), y en el Reglamento CE 593/2008 del Parlamento y del Consejo de 17 de junio de 2008 («Roma I»). Nos vamos a centrar en este último.

El Reglamento recoge normas de conflicto aplicables a los distintos supuestos de obligaciones contractuales, estableciendo como punto de conexión principal y como regla general la libre elección de las partes y solo en su defecto y a falta de la misma otros puntos de conexión diversos –en ocasiones utilizando la «conexión en cascada», del mismo modo que el Código Civil–. El legislador europeo ha optado por una cláusula de cierre, en la que, como regla general, si hay un país estrechamente vinculado a la relación contractual de la que se deriva esta obligación, se aplique su legislación, por ser considerada la que tiene una conexión más estrecha con la aquella y, por ende, la que por razones lógicas debe ser la más adecuada para aplicar al caso concreto. El legislador además ha previsto ciertos supuestos especiales en casos de contratos específicos como contratos de mercancías, contratos de pasajeros, consumidores y usuarios, contratos de seguros, etc.

Quede constancia de que el citado Reglamento se aplica a las obligaciones contractuales en materia civil y mercantil en las situaciones que impliquen un conflicto de leyes, pero no se aplica a las materias fiscales, aduaneras y administrativas, ni a la prueba ni al proceso. Asimismo se aplica a los contratos desde el 17 de diciembre de 2009 y tiene eficacia *erga omnes*. Esto es importante: cualquier norma dispuesta por el Reglamento deberá aplicarse aunque no pertenezca a un Estado miembro.

En definitiva, el Reglamento que analizamos dispone una regla general y diversas excepciones:

A. REGLA GENERAL: PUNTO DE CONEXIÓN APLICABLE; LIBERTAD DE ELECCIÓN DE LAS PARTES

El contrato se regirá por la ley elegida por las partes. La ley podrá aplicarse a la totalidad o solamente a una parte del contrato. Las partes podrán, en cualquier momento, convenir que el contrato se rija por una ley distinta. Además:

- La ley del país que esté más estrechamente vinculado al objeto del contrato deberá respetarse aunque las partes elijan la ley de un país distinto como ley aplicable.
- En caso de que el objeto del contrato afecte a uno o varios Estados miembros, y se elija la ley de un Estado no miembro, esta no podrá contradecir las disposiciones del Derecho comunitario.

B. EXCEPCIONES A LA REGLA GENERAL: LEY APLICABLE A FALTA DE ELECCIÓN

Sin perjuicio de otras especialidades en virtud de contratos específicos –como apuntamos: contratos de mercancías, pasajeros, seguros, consumidores y usuarios– en defecto de libre elección y a falta de ley elegida por las partes las partes, se aplicará la de la residencia habitual de la parte que deba realizar la prestación característica del contrato. Esta regla será aplicable a contratos de compraventa, prestación de servicios, franquicia o distribución. No obstante encontramos algunas especialidades:

- Los contratos que tengan por objeto un bien inmueble se regirán por la ley del país donde esté sito el bien inmueble (*lex rei sitae*), salvo en los casos de arrendamiento temporal y privado –máximo seis meses consecutivos–. En estos casos, el contrato se regirá por la ley del país donde el propietario tenga su residencia habitual.
- Los contratos de venta de bienes mediante subasta –incluida la subasta electrónica, regulada en nuestro caso por normas como la Ley del Patrimonio de las Administraciones Públicas o la normativa bancaria– se regirán por la ley del país donde tenga lugar la subasta.
- En el caso de determinados instrumentos financieros regidos por una única ley, esta será la que se aplique.

El Reglamento cierra con una cláusula residual, estableciendo que para el caso de que ninguna o varias de las normas anteriores se apliquen a un contrato, este se regirá por la ley del país donde tenga su residencia habitual la parte que deba realizar la prestación característica del contrato. No obstante, si el contrato presenta vínculos más estrechos con un país distinto del que sugieren dichas normas, se regirá por la ley de dicho país. Se seguirá este mismo principio lógico cuando no se pueda determinar la ley aplicable.

Por otro lado, en el caso de los contratos específicos antes aludidos, se aplican normas especiales que determinan la norma de conflicto que debe ser aplicada en cada caso. La regla general sigue siendo la libre elección de las partes, y en su defecto se establecen reglas de cobertura de supuestos. En estos casos, el Reglamento ofrece opciones para elegir la ley aplicable y determina la norma que regirá el contrato en defecto de elección:

- Contratos para el transporte de mercancías: en defecto de elección, la ley aplicable será la ley del país donde el transportista tenga su residencia habitual, siempre y cuando el lugar de recepción o el lugar de entrega, o la residencia habitual del remitente, también estén situados en ese país. Si no se cumplen estos requisitos, se aplicará la ley del país donde esté situado el lugar de entrega.
- Contratos para el transporte de pasajeros: las partes podrán elegir como ley aplicable la del país donde el pasajero o el transportista tengan su residencia habitual,

la del país donde el transportista tenga el lugar de su administración central, o la del país donde se encuentre el lugar de origen o el de destino. En defecto de elección, el contrato se regirá por la ley del país donde el pasajero tenga su residencia habitual, siempre y cuando el lugar de origen o el lugar de destino también estén situados en ese país. No obstante, si el contrato presenta vínculos manifiestamente más estrechos con un país distinto del anteriormente indicado, se aplicará la ley de ese otro país.

- Contratos de consumo entre consumidores y profesionales: se regirán por la ley del país en que el consumidor tenga su residencia habitual, siempre que el profesional ejerza o dirija sus actividades comerciales a ese país. Basándose en la libertad de elección, las partes también podrán acordar que el contrato se rija por otra ley, siempre que esta ofrezca el mismo nivel de protección a los consumidores que la de su país de residencia habitual.
- Contratos de seguro: en defecto de elección, se regirán por la ley del país en el que el asegurador tenga su residencia habitual. No obstante, si el contrato presenta vínculos manifiestamente más estrechos con un país distinto del anteriormente indicado, se aplicará la ley de ese otro país.
- Contratos individuales de trabajo: la ley aplicable será la libremente pactada por las partes (principio de libertad de elección), pero solo cuando el trabajador obtenga el mismo nivel de protección que con la ley aplicable en defecto de elección. En este último caso, el contrato se regirá por la ley del país en el cual o, en su defecto, a partir del cual el trabajador realice su trabajo habitualmente. Si esto no pudiera determinarse, el contrato se regirá por la ley del país donde esté situado el establecimiento a través del cual haya sido contratado el trabajador. No obstante, si el contrato presenta vínculos manifiestamente más estrechos con un país distinto del anteriormente indicado, se aplicará la ley de ese otro país.

Por último, en este apartado debe mencionarse que desde el punto de vista material las normas de conflicto establecidos en el Reglamento únicamente se aplicarán a las obligaciones contractuales civiles y mercantiles. Quedan excluidas de su ámbito de aplicación las obligaciones en relación con el estado civil y la capacidad de las personas físicas; relaciones familiares y análogas y alimentos; regímenes económicos matrimoniales, testamentos y sucesiones; instrumentos negociables como letras de cambio, cheques, pagarés, arbitraje y la elección del tribunal competente; el derecho de sociedades, asociaciones y otras personas jurídicas, obligaciones de un mandante o empresa frente a terceros; *trusts* o uniones de empresas; tratos previos a la celebración de un contrato (precontratos), *culpa in contrahendo*; y contratos de seguros exceptuando los que se definen en el artículo 2 de la Directiva 2002/83/CE sobre seguros de vida.

Una vez acotado el lugar de celebración del negocio jurídico, quedaría pendiente la determinación del momento de la perfección, cuestión que debemos dejar para un futuro estudio por cuanto hemos optado por centrar el presente en el análisis del principio de territorialidad. Parece

claro, no obstante, que cuando en el contrato u otro negocio jurídico multilateral interviene *per natura* la firma de varias partes, como manifestación formal de su voluntad, la perfección y el inicio de los efectos jurídicos del contrato electrónico se producen a partir de la firma electrónica de la última persona física que –en su nombre o en representación de una persona jurídica– tenga atribuida la capacidad para asumir las obligaciones derivadas de aquel. Esta sería también la fecha del contrato. Todo ello de acuerdo con el Reglamento UE 910/2014 del Parlamento y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. En esta cuestión, la LSSI vino a regular sendas necesidades ya entonces incipientes: la contratación electrónica y los servicios de la sociedad de la información. No obstante, en un contexto que cambia y avanza en clara progresión geométrica, en el que las nuevas realidades exigen una revisión ágil y veloz, incluso la modificación del año 2007 –Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información– se torna insuficiente.

III. INCIDENCIA DEL PRINCIPIO DE TERRITORIALIDAD EN LA LEY 34/2002, DE 11 DE JULIO, DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO

Recordemos que el objeto de esta importante ley es la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica en lo referente a las obligaciones de los prestadores de servicios –incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones–, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

A. SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

En este apartado examinaremos brevemente el principio de territorialidad en la norma y aquellos supuestos en los que se acude a este principio o punto de conexión para determinar su ámbito de aplicación. Así, encontramos alusiones a este principio tanto en el ámbito de aplicación de la norma como en distintos apartados de la misma. A saber:

- La ley es de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos. Se entenderá que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que estos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

- Asimismo, la LSSI es de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España. Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad. Se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.
- La utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador. Los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.
- De nuevo volvemos a encontrar el principio de territorialidad en cuanto a los prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo, en cuyo caso se aplicará cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes: derechos de propiedad intelectual o industrial, emisión de publicidad por instituciones de inversión colectiva, actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios, obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores, y régimen de elección por las partes contratantes de la legislación aplicable a su contrato.
- El principio de territorialidad vuelve a mencionarse en materia de derechos reales, ya que, en todo caso, la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español.

B. CONTRATACIÓN ELECTRÓNICA

El artículo 26 de la ley que analizamos establece literalmente que «para la determinación de la ley aplicable a los contratos electrónicos se estará a lo dispuesto en las normas de Derecho internacional privado del ordenamiento jurídico español».

La siguiente referencia al principio de territorialidad la encontramos en el artículo 29 de la ley, al determinar el lugar en el que se entienden celebrados los contratos electrónicos en los que intervenga como parte un consumidor, los cuales se presumirán celebrados en el lugar en que este tenga su residencia habitual. En caso de no intervención del consumidor o usuario el contrato se entiende perfeccionado en el lugar donde esté establecido el prestador del servicio.

En cuanto a la resolución extrajudicial de conflictos, y por lo que se refiere a jurisdicción arbitral, se establece la posibilidad de que las partes de manera dispositiva puedan someter sus conflictos a arbitraje. Estos arbitrajes son los previstos en la legislación de arbitraje y de defensa de los consumidores y usuarios, así como otros procedimientos de resolución extrajudicial de conflictos que se instauren por medio de códigos de conducta u otros instrumentos de autorregulación.

A modo de conclusión, la aplicación estricta del principio de territorialidad –parece claro que la LSSI está *demasiado* inspirada en este principio– permite a un Estado imponer su regulación a un proveedor de servicios de internet que opera en su territorio. Nuestro pensamiento crítico es que tanto el Derecho internacional como el europeo han dado demasiado margen regulatorio a los Estados frente al fenómeno internet, independientemente de que hablemos de relaciones con efectos jurídicos o de una simple navegación informativa que, por la vía de la interacción, podría tenerlos. Un Estado puede incluso impedir el acceso desde su territorio a ciertos sitios web determinados que considere nocivos o ilegales, lo cual es técnicamente complejo, pero posible. Es una potestad de los Estados amparada en el principio de territorialidad del Derecho internacional, pero razones más elevadas como el principio/derecho de libertad o el derecho fundamental de libertad, o la misma democracia, aconsejan lo contrario. La pregunta que surge es: ¿existe un derecho fundamental a usar libremente internet? Opinamos sin duda que la respuesta es sí, pues tal derecho no puede considerarse sino una manifestación del de libertad, el cual está a su vez recogido en todas las declaraciones internacionales de derechos humanos.

IV. OBLIGACIONES EXTRA CONTRACTUALES

Volviendo al Código Civil, tenemos que en materia de obligaciones extracontractuales el artículo 10.9 establece un criterio claro dividido en tres principios:

- Las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven.
- La gestión de negocios se regulará por la ley del lugar donde el gestor realice la principal actividad.
- En el enriquecimiento sin causa se aplicará la ley en virtud de la cual se produjo la transferencia del valor patrimonial en favor del enriquecido.

Nuevamente cabría hablar de superación de la norma interna por el Derecho europeo, que, una vez más, precisamente por su amplio ámbito territorial, parece el más idóneo para regular las relaciones *intra* e incluso extracomunitarias. Se trata de normas que además reúnen dos importantes características adicionales: una formal, ya que al tratarse mayoritariamente de reglamentos no precisan de su trasposición al derecho interno, y una temporal, ya que se trata de normas de reciente (o relativamente reciente) aprobación. En este caso, y en relación con el presente apartado, nos referiremos al Reglamento CE 864/2007 del Parlamento y del Consejo, de 11 de julio de 2007 («Roma II»).

A fin de conocer la norma de conflicto aplicable en materia de obligaciones extracontractuales, y siguiendo la sistemática del citado reglamento, distinguiremos entre obligaciones derivadas de hechos dañosos –culpa o daño extracontractual– y la ley aplicable a las obligaciones derivadas de gestión de negocios ajenos, enriquecimiento injusto –conocido por muchos civilistas como supuestos típicos de cuasicontratos– y la *culpa in contrahendo*:

A. LEY APLICABLE A OBLIGACIONES DERIVADAS DE HECHOS DAÑOSOS

1. Ley aplicable a las obligaciones que admiten autonomía de la voluntad

En aquellas obligaciones que admitan la autonomía de la voluntad la ley aplicable será la libremente elegida por las partes (expresa o tácitamente), ya sea posterior al hecho generador del daño, o anterior siempre que sea un acuerdo libremente negociado y las partes realicen actividades comerciales. Los límites de esta elección serán los derechos de terceros, las normas contractuales imperativas de un ordenamiento si la situación es interna y está enteramente vinculada a ese ordenamiento, las normas internacionales imperativas del Estado del foro si la situación es internacional, y las normas comunitarias imperativas si la situación es intracomunitaria –exclusivamente vinculada con varios Estados miembros–. Como regla supletoria, en defecto o falta de acuerdo o voluntad pactada por las partes, se aplicará la ley de la residencia habitual común del responsable del daño y de la persona perjudicada; y en defecto de residencia habitual común, la ley del lugar donde se produce el daño. Como cláusula de escape, podrá aplicarse cualquier ley diferente de las anteriores si existe un vínculo manifiestamente más estrecho con la ley de otro país.

En cuanto al supuesto específico de la responsabilidad por productos defectuosos, será aplicable la residencia habitual común del responsable del daño o de la persona perjudicada. No obstante, a continuación distingue si el responsable del daño pudo o no prever razonablemente la comercialización del producto. En el primer caso será aplicable la ley del país de la residencia habitual de la persona perjudicada si el producto se comercializó en dicho país. En defecto de lo anterior, se aplica la ley del país donde se adquirió el producto. Si el producto se comercializó en dicho país, y en defecto de lo anterior, la ley del país donde se produjo el daño –nótese de nuevo la utilización de los puntos de conexión en cascada–. Si el responsable del daño no pudo prever razonablemente la comercialización del producto en los países anteriores, se aplicará la ley del país donde tenga su residencia habitual el responsable del daño. No obstante, el legislador establece la cláusula de escape del «vínculo más estrecho» y establece que podrá aplicarse cualquier ley diferente a todas las anteriores si existe un vínculo manifiestamente más estrecho con la ley de otro país.

2. Ley aplicable a las obligaciones que no admiten autonomía de la voluntad

En materia de competencia desleal y actos restrictivos de la competencia, se distingue entre los que afectan al mercado, a un competidor o a la competencia:

- Actos de competencia desleal que afecten al mercado: se aplica la ley del país en el que las relaciones de competencia o los intereses colectivos de los consumidores puedan resultar afectados.
- Actos de competencia desleal que solo afecten a un competidor: la aplicación de la conexión objetiva general anteriormente señalada.
- Actos restrictivos de la competencia: se aplicará la ley del mercado afectado.

En materia de infracciones de los derechos de propiedad intelectual, se distingue la infracción de derechos nacionales o de alcance comunitario:

- Si se infringen derechos nacionales: se aplicará la ley del Estado para cuyo ámbito se reclama la protección (*lex loci protectionis*).
- Si se infringen derechos de alcance comunitario: se aplicará la ley del lugar de la infracción.

B. LEY APLICABLE A LAS OBLIGACIONES DERIVADAS DE GESTIÓN DE NEGOCIOS AJENOS, ENRIQUECIMIENTO INJUSTO Y *CULPA IN CONTRAHENDO*

La regla general sigue siendo la autonomía de la voluntad, admitiendo como cláusula de escape la aplicación de la ley del país con la que el caso presente vínculos más estrechos. Como reglas específicas, se distingue entre enriquecimiento injusto, gestión de negocios ajenos y *culpa in contrahendo*:

1. Enriquecimiento injusto y gestión de negocios

Si deriva de una relación previamente existente entre las partes, regirá la ley aplicable a dicha relación. En su defecto, la ley de la residencia habitual común de las partes, y en defecto de lo anterior la ley del país donde se produjo el enriquecimiento injusto o en el que se haya realizado el acto de gestión.

2. *Culpa in contrahendo*

Regirá la ley aplicable al contrato celebrado o que hubiera llegado a celebrarse, y en su defecto será de aplicación la regla de la conexión general antevista.

Cabe recordar que desde el punto de vista material el Reglamento analizado regula la responsabilidad extracontractual en materia civil y mercantil, señalando el mismo que a efectos del

reglamento se entenderá por *daño* toda consecuencia derivada de un hecho dañoso, el enriquecimiento injusto, la gestión de negocios o la *culpa in contrahendo*. Por hecho generador del daño se entenderán no solo los hechos o daños actuales, sino los que hechos o los daños que puedan llegar a producirse. Quedan no obstante excluidas de su aplicación, por un lado, determinadas obligaciones de Derecho público –materias fiscales, aduaneras y administrativas, la responsabilidad penal, la responsabilidad del Estado por actos *iure imperii*–; y, por otro lado, en cuanto a obligaciones civiles y mercantiles, las relaciones familiares, las comparables a estas y las alimenticias, los regímenes económicos matrimoniales y los comparables a estos, los testamentos y sucesiones, las letras de cambio, cheques, pagarés y otros instrumentos negociables, el Derecho societario y las relaciones generadas en los *trusts*, los daños nucleares, las violaciones de los derechos relacionados con la intimidad y la personalidad.

Importante es recordar que desde el punto de vista territorial, este reglamento también tiene eficacia *erga omnes*, con aplicación de carácter universal, cualquiera que sea la ley reclamada por la norma de conflicto. Finalmente, desde el punto de vista temporal el reglamento se aplica a la responsabilidad extracontractual derivada de hechos dañosos acaecidos a partir del 11 de enero de 2009.

V. PROPIEDAD INTELECTUAL

En materia de propiedad intelectual, el principio de territorialidad, entendido en sentido estricto, ha venido siendo un punto de conexión de referencia a la hora de determinar la norma de conflicto aplicable. Sin embargo, el impacto de las TIC nos lleva a plantearnos nuevas preguntas relacionadas con la determinación de los puntos de conexión hasta ahora válidos para la determinación de la legislación aplicable y la jurisdicción competente.

El principal problema legal que plantea internet, amén de su viralidad y realidad cambiante por momentos, es su «extraterritorialidad», universalidad y globalización. Hablando de propiedad intelectual, puede que estemos ante uno de los debates jurídicos más afectados por la utilización de las TIC, incluso si no abordamos otra problemática que la que representa exclusivamente internet.

La propiedad intelectual es un derecho que en ocasiones se vulnera, pero es difícil determinar el lugar exacto en que ocurren los hechos constitutivos de una presunta infracción, porque evidentemente no nos encontramos ante un espacio físico o tangible, sino ante una realidad virtual que escapa a nuestros criterios de determinación clásicos preestablecidos y que nos plantea la duda de si los puntos de conexión conocidos pueden servirnos, una vez más, en el ámbito de las TIC. La respuesta oscila entre «no» y «no en todos los casos», circunstancia que abre o debería abrir una discusión jurídico-doctrinal que plantee estas nuevas cuestiones y que sea abordada preferiblemente por toda la comunidad internacional –la jurídica, pero también la tecnológica y la social–.

En efecto, el problema de la extraterritorialidad y «plurilocalización» de internet afecta totalmente al principio de territorialidad y los puntos de conexión aplicables hasta ahora en el ámbito de propiedad intelectual –*loci delicti commissi* y *loci protectionis*–, puntos de conexión que

casaban bien con el citado principio, pero que plantean numerosas dudas en el ámbito de las tecnologías, puesto que se discute no ya solo cómo queda afectado, sino incluso si sigue siendo un principio adecuado y coherente a esta nueva realidad virtual, en la que el espacio físico o territorial se desdibuja hasta quedar diluido e indeterminado por completo. ¿Es necesario acuñar nuevos términos o principios o adoptar nuevos puntos de conexión para esta nueva realidad?, ¿puede seguir aplicándose –evidentemente de forma readaptada– el principio de territorialidad hasta ahora imperante? Son preguntas que el legislador y la nueva comunidad internacional deben plantearse habida cuenta de que las consecuencias jurídicas que derivan de la determinación del ámbito de la legislación aplicable y de la jurisdicción competente son de importancia capital.

Surge, pues, la necesidad imperiosa de abordar esta cuestión y plantear soluciones a un problema de candente actualidad. Nos apoyaremos en cuanto al desarrollo de esta cuestión nuevamente en dos normas de Derecho europeo: el Reglamento UE 1215/2012, del Parlamento y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil –entra en vigor el 10 de enero de 2015, derogando el anterior Reglamento 44/2001–; y el citado Reglamento «Roma I». Asimismo, dividiremos el presente epígrafe en tres apartados:

A. REGLAMENTO DE BRUSELAS I. PROPIEDAD INTELECTUAL, LUGAR DE INFRACCIÓN O COMISIÓN DEL ILÍCITO

El lugar de infracción del hecho ilícito o lugar de comisión del delito venía siendo el punto de conexión por excelencia en esta materia. Punto de conexión estrechamente vinculado al principio de territorialidad –lugar de comisión de la infracción–, porque hasta ahora la realidad preexistente entendía que únicamente podía ocurrir el hecho típico en un lugar determinado, físico, que podía ser perfectamente absorbido por el principio de territorialidad a fin de determinar la legislación aplicable y la jurisdicción competente.

Así se establece también en el artículo 7.2 del Reglamento n.º 1215/2012 del Parlamento Europeo y del Consejo de 12 de diciembre del año 2012 en materia de competencia judicial, reconocimiento y ejecución de resoluciones judiciales en materia civil y mercantil («Bruselas I») en los siguientes términos: «Una persona domiciliada en un Estado miembro podrá ser demandada en otro Estado miembro en materia delictual o cuasidelictual, ante el órgano jurisdiccional del lugar donde se haya producido o pueda producirse el hecho dañoso»; permitiendo por tanto al actor o demandante acudir al tribunal donde ha ocurrido o pueda ocurrir el hecho dañoso –en el mismo sentido el anterior artículo 5.3 del Reglamento de Bruselas de 2001–.

Este criterio excesivamente «territorialista» ha sido criticado por la moderna doctrina al no casar bien con el mundo virtual, por lo general «plurilocalizado» y «extraterritorial», donde en numerosas ocasiones es difícil determinar el lugar de comisión del hecho o cuando los lugares implicados son varios, y raramente una cuestión está vinculada solo a un lugar o espacio territorial. En efecto, con internet y las TIC por lo general pueden estar afectados varios territorios e inclu-

so Estados en la comisión de un hecho ilícito, y no siempre es determinable –ni determinante– el «lugar donde ocurrieron los hechos».

La mayor parte de la doctrina y de la jurisprudencia opta por interpretar el artículo 7.2 del Reglamento de «Bruselas I» en un sentido amplio y flexible, y con carácter unánime ha optado por interpretar el citado artículo siguiendo la teoría de la ubicuidad y alternatividad, de manera que el lesionado-actor podrá optar entre los tribunales del país de la acción o los tribunales del resultado del ilícito –o lo que es lo mismo: lugar de comisión de la acción infractora o lugar donde se hubiera sufrido el perjuicio–.

Los autores que defienden esta doctrina o teoría de la «alternatividad» –que en nuestra opinión se adapta muy bien al problema de la extraterritorialidad de internet– se basan en el principio seguido por el reglamento de facilitar el mejor cumplimiento del mismo a fin de facilitar la determinación del tribunal competente y limitar el número de foros disponibles, algo que además de beneficiar al demandado y una mejor administración de justicia, es coherente con los objetivos del reglamento.

B. DIFICULTAD DE LA DETERMINACIÓN DEL *FORUM LOCI ACTI* / *FORUM LOCI DAMNI* EN INTERNET

En definitiva, en el ámbito de las TIC se hace especialmente difícil determinar el lugar concreto de comisión de los hechos, razón por la cual la mayoría de la doctrina entiende que dicho lugar debe identificarse con el lugar donde se hayan introducido los contenidos perjudiciales por parte del causante del daño.

Aunque esta parece una opción sensata, no está exenta de críticas y posibles desventajas: la dificultad de determinar el lugar exacto de comisión de los hechos, la inseguridad jurídica que podría generar la falta de adecuación de ese foro establecido en una regla general sin tener en cuenta otros correctivos, la posibilidad de degenerar en el temido *forum shopping* o el amplio juego del *forum actoris*, entre otras. A fin de evitar estos efectos indeseables la mayoría de la doctrina, siguiendo la jurisprudencia del TJUE, ha propuesto la alternativa del lugar donde se hayan producido de manera «sustancial» los daños sufridos.

C. LEY APLICABLE: ARTÍCULO 8 DE «ROMA II» (OBLIGACIONES EXTRA-CONTRACTUALES)

El artículo 8.1 del citado Reglamento «Roma II» aplicable a las obligaciones extracontractuales recoge un principio a su vez estrechamente vinculado con el principio de territorialidad: el *lex loci protectionis*, principio de conexión con la ley del país para cuyo territorio se reclama la protección. Este principio, que presenta ventajas tales como la seguridad jurídica, la consolidación del mercado de la UE y una buena interrelación con el principio de territorialidad, tampoco está

exento de carencias, si bien la mayoría de la doctrina lo estima preferible al también tradicional –y muy enraizado con principio de territorialidad– *lex loci delicti commissi*.

Sin embargo, el impacto de las TIC y el «fenómeno internet» convierte también en insuficiente el principio *lex loci protectionis*. Como señala la mejor doctrina, el principal problema de la aplicación de este principio está estrechamente vinculado –de nuevo– con la dificultad de localización en el ámbito de internet, sobre todo cuando el perjuicio se haya producido en diferentes lugares y sean varios los países que reclamen la protección de estos derechos. El legislador no ha tenido en cuenta, pues, el problema de la *plurilocalización* de internet ni el impacto real de las TIC. Uno de los errores clásicos de los intérpretes jurídicos de la nueva realidad sociotecnológica es precisamente la asunción de la premisa de que la dificultad que *ab initio* se plantea es la falta de territorialidad, cuando en realidad la mayoría de veces debemos lidiar con precisamente un problema de multiterritorialidad. En la práctica deberá ser el órgano judicial –preferiblemente el TJUE– el que decida en cada caso concreto, con los inconvenientes y la inseguridad jurídica que ello conlleva a pesar incluso de la categoría del citado tribunal y de su idoneidad, más que ningún otro, para sentar doctrina.

El legislador de la UE opta pues por un claro criterio de «búsqueda de la territorialidad», tanto en cuanto al ámbito de la ley aplicable como en lo que se refiere a la jurisdicción competente. Así, el Reglamento de Bruselas I –art. 7.2 (anterior 5.3 del Reglamento de Bruselas de 2001)– opta por el principio de *forum delicti commissi*, mientras que el Reglamento de Roma II aplicable a las obligaciones extracontractuales, en su artículo 8.1, opta por la regla de la *lex loci protectionis*. Ambas soluciones están fuertemente incardinadas en el principio de territorialidad, y es por ello que debemos criticar su falta de adecuación al mundo virtual –caracterizado como hemos visto por la extraterritorialidad y la plurilocalización–. El legislador está optando en definitiva por propuestas típicas y tradicionales que nada tienen que ver con la nueva realidad sociotecnológica. Debemos pedir e incluso proponer soluciones alternativas que se ajusten con mayor precisión a la nueva realidad, o al menos practicar una interpretación de la normativa vigente más acorde con estas nuevas necesidades.

VI. DELITOS TIC Y DELITOS A TRAVÉS DE LAS TIC

Nuestro ordenamiento jurídico sigue en materia penal y de policía un criterio esencialmente territorial, criticado por algunos como excesivamente *legeforista* y soberanista. Así, el artículo 8 del Código Civil establece que las leyes penales, de policía y las de seguridad pública obligan a todos los que se hallen en territorio español. No es un mal punto de partida, pero evidentemente el ya citado carácter supranacional, transfronterizo e internacional de las TIC obliga también a replantearse esta regla general.

A pesar del marcado carácter territorial de la materia penal, los intentos del legislador por adaptarse a la nueva realidad se han hecho patentes en esta rama del Derecho más que en ninguna otra. Algunos Estados de la UE han tratado alianzas de colaboración en materia de policía y de colaboración para la prevención de determinados delitos en internet. Fue precisamente un Estado europeo, Alemania, el primero del mundo que decidió crear una policía del ciberespacio

dedicada a perseguir fundamentalmente la violencia y la pornografía en internet. En un proyecto de ley se preveía un sistema de detección de actividades ilegales en la red que obligaría a los proveedores a denunciar este tipo de contenidos.

Desde el punto de vista de nuestro ordenamiento jurídico, cabe analizar al menos de manera sucinta esta cuestión. Así, desde un punto de vista preventivo, los artículos 37 y siguientes de la LSSI prevén un régimen específico de infracciones y sanciones, así como medidas provisionales y de carácter claramente preventivo para aquellos servidores que no respeten la ley. Establece además el artículo 8 de la misma ley que en caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación –la salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional; el respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social; o la salvaguarda de los derechos de propiedad intelectual–, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. La LOPD prevé igualmente –en sus arts. 43 y sigs.– un régimen de sanciones e infracciones para aquellos sujetos o servidores que no respeten dicha normativa, estableciendo incluso la posibilidad de inmovilización de ficheros.

En el ámbito estricto del Derecho penal, partimos históricamente del principio de soberanía de los Estados, del cual derivaba el *ius puniendi*, que siempre fue una facultad-autoridad-poder de cada Estado, de manera que tradicionalmente –y de acuerdo con el principio de territorialidad y personalidad– el Estado extendía su *potestas* sobre todo hecho delictivo que acaeciera dentro de su territorio y a todo ciudadano que ostentara su nacionalidad. A excepción de algunos crímenes –genocidio, crímenes de lesa humanidad, entre otros– y de algunos tratados internacionales, cada Estado era soberano y esta potestad de Derecho público se extendía a *sus ciudadanos* y salvo contadas excepciones *dentro de sus fronteras*.

Tal y como hemos visto, el principio de soberanía ha quedado no obstante desfasado con esta nueva realidad que no atiende a espacios físicos, y que se caracteriza por su naturaleza *a priori* «deslocalizada». Asumiendo ya a estas alturas del trabajo que en nuestros días los presupuestos, los escenarios, el elemento subjetivo, y en general todo nuestro planteamiento previo del Derecho ha sufrido una auténtica transformación, vemos como de forma concreta la rama del Derecho penal queda completamente afectada por esta nueva realidad. En este sentido, es cierto que el desarrollo y auge de las TIC nos ha planteado supuestos delictivos nunca antes previstos por el legislador, completa o supuestamente nuevos, según los casos, y que como mínimo nos han obligado a plantearnos la existencia o no de un vacío legal, y obviamente la necesidad de colmarlo en el primer caso.

Habida cuenta de que en el anterior epígrafe dedicado a la propiedad intelectual ya hemos analizado los distintos puntos de conexión de infracciones y hechos establecidos por el legislador comunitario –y sus ventajas y desventajas–, analizaremos en el presente epígrafe las posturas o posiciones doctrinales para la solución de esta nueva (¿?) realidad en el ámbito de los hechos ilícitos y cómo afecta al principio de territorialidad, hilo conductor del presente estudio.

A. POSICIONES DOCTRINALES QUE DEFIENDEN LA INNECESARIEDAD DE UNA NUEVA REGULACIÓN, «DESREGULARIZACIÓN»

En primer lugar, encontramos posiciones doctrinales que entienden que nuestro ordenamiento jurídico cuenta ya con suficiente regulación específica en la materia, y que de hecho no estamos ante supuestos nuevos, sino ante unos mismos supuestos con diferentes formas de manifestación de un mismo hecho lesivo.

Así, según esta postura doctrinal, en el caso de determinados hechos ilícitos, por ejemplo suplantación de identidades a través de redes sociales, no estaríamos ante supuestos nuevos vacíos de regulación o lagunas legales. Suplantación de identidad, acoso, imagen, honor, intimidad... son instituciones o derechos que se encuentran incuestionablemente recogidos y protegidos por la legislación vigente, y no necesitan de mayor protección por el hecho de haberse servido de una plataforma tecnológica. Si bien la viralidad y difusión a través del medio se amplifica hasta niveles insospechados hasta el momento, estas mismas circunstancias ya se encuentran reguladas en nuestro ordenamiento.

Así, por ejemplo, la Ley orgánica de protección al honor y la propia imagen, cuando establece que a la hora de determinar la responsabilidad y la indemnización por el daño causado se tendrá en cuenta, entre otras circunstancias «la difusión del medio»; o en numerosos tipos penales, nuestro Código Penal ya regula supuestos en los que se tiene en cuenta el medio empleado, la difusión de este medio, el uso concreto de las tecnologías como medio o plataforma para llevar a cabo el supuesto de hecho delictivo, tipificándolo en numerosas ocasiones como un supuesto agravado que lleva por tanto aparejado un plus en la imposición de la pena.

Son todos ellos supuestos –hechos típicos, antijurídicos, culpables y punibles–, que se encuentran debidamente tipificados y regulados, y que no necesitan de una mayor regulación. Las injurias, calumnias y demás hechos delictivos no son otra cosa distinta por servirse de las TIC como medio o instrumento del delito. No estamos, pues, ante un vacío legal como defienden algunos; el «tipo penal» desde el punto de vista sustantivo o material no varía. En consecuencia, no es necesaria una nueva regulación de un mismo supuesto que daría lugar a una duplicidad innecesaria e inútil. Cuestión diferente es la previsión de circunstancias modificativas de la pena o supuestos agravados en los casos de utilización de las TIC en la comisión de tales hechos delictivos. En el caso de la responsabilidad civil derivada de este tipo de ilícitos nos encontramos ante el mismo supuesto.

Cabe señalar además que nuestro ordenamiento jurídico cuenta con principios generales del derecho –muy consolidados y positivados algunos–, que avalan esta teoría. Analicemos por ejemplo el principio de analogía consagrado en el Código Civil (art. 4.1), muy cuestionado en cuanto a su aplicación al ámbito penal pero que no obstante en estos casos podría resolver algún problema. Obviamente la analogía deberá ser muy patente antes de imponer una sanción penal con base en este principio, siempre previa ponderación razonada de la concurrencia del interés público, la defensa de los derechos de las personas, y el carácter totalmente tecnológico, incluso

inédito, de la infracción. Una postura más conservadora –y en términos estrictos más correcta– es esperar a que el legislador reaccione y tipifique expresamente este nuevo acto ilícito. Pero quizá no sea necesario en todos los casos. No olvidemos jamás –y menos en este momento– el principio general consagrado en el artículo 3 del propio Código Civil, en materia de interpretación del Derecho, que establece que todo nuestro ordenamiento jurídico debe ser interpretado de acuerdo con la realidad social e histórica del momento que se trate.

B. POSICIONES DOCTRINALES QUE DEFIENDEN LA NECESIDAD DE UNA NUEVA REGULACIÓN ESPECÍFICA EN ESTA MATERIA

Por otro lado, encontramos autores que propugnan un cambio radical, la necesidad de una nueva regulación específica y universal, a modo de una nueva *lex mercatoria*, un Derecho internacional de internet, o como se ha venido denominando recientemente *internacional ciber-law*. Este sector doctrinal entiende que es imposible seguir aplicando las normas de Derecho internacional o interno de los distintos Estados cuando este Derecho clásico se enfrenta a las nuevas tecnologías, al presentar estas un planteamiento totalmente nuevo y diferente que exige una regulación específica.

Estos autores entienden que las normas tradicionales de Derecho internacional y nacional de los Estados establecen puntos de conexión territorial, normalmente estatal o nacional, pensados para funcionar en un mundo físico, real, con un territorio y una población específica, delimitada y fácilmente determinable. Esta posición doctrinal entiende que estos criterios tradicionales no son aplicables –o al menos no son fácil ni adecuadamente aplicables– a un nuevo escenario posmoderno, globalizado, *en un nuevo espacio supranacional y transnacional*: el ciberespacio.

No puede hablarse ya, ni aplicarse, el principio de territorialidad –no como lo veníamos entendiendo–, y ni siquiera sería adecuado, porque ya no nos encontramos ni con un territorio ni con un espacio físico delimitado, sino con un *supraespacio* universal y globalizado que trasciende estos términos. En definitiva, estos autores defienden que estamos ante una nueva realidad que exige una nueva regulación.

C. NUESTRA POSICIÓN

Nuestra postura debe ser y es ecléctica, con claro predominio de la teoría *desreguladora*.

Por un lado porque las llamadas, por la doctrina regulatoria, nuevas tecnologías, *no son tan nuevas*. Es por ello que nos gusta más la expresión TIC, que sencillamente alude a las tecnologías de la información y la comunicación, las cuales además son en cada momento las que son. Llamar «nueva» a la tecnología móvil o a internet alimenta la creencia popular de que el mundo del Derecho va siempre al menos con 10 o 20 años de retraso con respecto al resto de la sociedad. La capacidad de reacción idónea es la que al mismo tiempo resulte rápida y adecuada, pero cuanto

más se retrasa la aceptación de la realidad, curiosamente peor se entiende, y por ello más posibilidades hay de que la reacción sea desproporcionada.

Un aspecto que sí compartimos con la doctrina del *internacional ciberlaw* es la premisa de que ciertamente el Derecho fue concebido para funcionar en un mundo físico, un mundo que estos autores denominan «real». Pero fallan, en nuestra opinión, al no considerar real aquello que choca con el concepto tradicional de realidad, lo cual no es irreal sino precisamente una nueva realidad, en la que se producen hechos reales que, de no serlo, evidentemente no se podrían sancionar. Algunos de estos hechos sí que son inéditos –hasta hace unos años–, y es aquí donde hablaríamos de *delitos informáticos*: *phishing*, *spam*, *bulling* y varios tipos de fraudes electrónicos. Pero no son delitos nuevos, evidentemente, las injurias, las calumnias o las distintas modalidades de apología. Se trata de viejos conocidos que se mueven como pez en el agua en los nuevos formatos. Internet quizá fomenta su comisión, y como mínimo agrava claramente la difusión, y por tanto el daño, pero esto ya está previsto con la tipificación de tipos agravados. A continuación procedemos a describir una serie de «nuevos» delitos, los más relevantes, cuya mención consideramos de interés y actualidad. Se trata de las siguientes conductas:

- *Cardsharing* es una conducta ilícita con fines comerciales, consistente en compartir una tarjeta de abonado entre dos o más receptores, donde un receptor A tiene alojada una tarjeta de abonado y los receptores B, C, etc. se conectan al receptor A para utilizar también esa tarjeta de abonado, evidentemente sin el consentimiento del prestador del servicio.
- *Ciberbullying* es el uso de medios telemáticos (internet, telecomunicaciones y telefonía móvil, videojuegos, redes sociales, etc.) para ejercer el acoso psicológico entre menores, de la índole que sea. En el caso que intervenga un adulto ya no estamos hablando de *ciberbullying* y hablaríamos de acoso o ciberacoso.
- *Child-grooming* consiste en contactar con menores de 13 años a través de internet. El término es derivado de *child grooming* o *internet grooming*. Ese contacto es llevado a cabo por un adulto a fin de hacerse con la confianza de un menor y obtener favores sexuales. Los favores pueden ir desde la obtención de fotografías y vídeos hasta encuentros en persona. Una manera de limitar este tipo de acoso es controlar el uso de las webcam de los equipos, desconectándolas o tapándolas en el caso de los ordenadores portátiles.
- *DoS* o *DDoS* son ataques de denegación de servicios, según si existen diferentes orígenes del ataque. El ataque se dirige a un sistema informático, o red, ocasionando que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad por el elevado consumo del ancho de banda en la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.
- *Phishing* o suplantación de identidad, es una tipología de abuso informático cometido mediante el uso de un tipo de «ingeniería social» caracterizado por intentar

adquirir información confidencial de forma ilegal (como puede ser una contraseña o datos de medios de pago).

- *Ransomware* palabra que proviene del inglés *ransom* (rescate). Es una especie de operación de «secuestro exprés» consistente en secuestrar información disponible en el ordenador infectado. Un programa se ha encargado de cifrarla con una clave desconocida de modo que se exige un pago al propietario para poder obtener la clave y así recuperar la información. Tiene su sentido sobre todo pensando que no es habitual la realización de copias de seguridad.
- *Sexting* consiste en el envío a otra persona, con consentimiento, de imágenes propias de indole sexual. Es evidente que con el uso generalizado de los *smartphones*, como elemento tecnológico de uso cotidiano cada vez más extendido entre la población y su uso para mandar instantáneas y fotografías de cualquier situación, puede conllevar a situaciones delictivas. Cabe recordar que una fotografía, una vez enviada, queda en poder de otra persona y se pierde el control sobre ella. El delito está en manejar dicha fotografía para ocasionar daños al autor de la misma... y evidentemente fotografías de carácter sexual, son fuente de este delito.

La economía del cibercrimen a nivel mundial asciende a 500 mil millones de dólares anuales; se dice que en poco tiempo va a rebasar la del narcotráfico y la de la trata de personas. Pero aún hay más: ¿cuál es la tendencia en cibercriminalidad en el futuro? Por un lado, los ataques dirigidos, conocidos con la denominación de amenazas avanzadas persistentes (del inglés, *advanced persistent threats* –APT–) que se diferencian de los ciberataques normales por el hecho de que poseen un objetivo definido, es decir, no persiguen a cualquier objetivo disponible intentando mantenerse sin ser detectado por largo periodos de tiempo.

También, que los usuarios comienzan a confiar en los sistemas de pago *on-line* para adquirir productos y servicios, estos se vuelven más interesantes para quienes desarrollan *malware* en busca de un beneficio económico. Finalmente, internet de las cosas, donde los nuevos dispositivos que se conectan a internet y almacenan información se vuelven vectores de ataques atractivos para los cibercriminales (vehículos, *smart TV*, sistemas biométricos o Google Glass, por poner algunos ejemplos).

Nos encontramos pues ante un cambio de medio o «formato», por un lado, y una nueva realidad, nuevas conductas típicas, por otro. El Derecho y la interpretación del Derecho resuelven prácticamente todas las cuestiones y situaciones que se plantean.

VII. CONCLUSIONES

El ciberespacio es actualmente, en nuestro mundo desarrollado, un verdadero Estado de bienestar del siglo XXI y, al igual que la Europa de mediados del siglo pasado, también está sometido a amenazas y problemas. Y si tenemos en cuenta que estamos ante un medio como inter-

net, que evoluciona y revoluciona nuestras vidas a un ritmo inimaginable, queda claro que hace casi imposible diseñar soluciones de largo recorrido.

Probablemente, el ciberespacio sea el recurso, desde una visión estratégica, más importante de los Estados y las naciones, tanto para aquellas cuya población no tiene acceso aún a la red como para las más post-industriales. Y cada día se conocen nuevas amenazas al *statu quo* existente. Vivimos una realidad cambiante, que va muy por delante del Derecho y de la capacidad de reacción del sistema, en la que ni siquiera los *hackers* son ya los de antes, unos personajes que se dedicaban únicamente a espiar, ahora son capaces de la más tremenda destrucción: información de carácter médico, información de nuestras tarjetas de crédito hasta ser capaces de acceder a nuestros sistemas de información de las empresas e incluso a nuestros equipos particulares, llegando a la petición de un cuantioso rescate a cambio de poder volver a tener acceso y disponer de la información de nuestros equipos informáticos, un tipo de delito que no ha dejado de incrementarse en los últimos dos años. El *cibercrimen* evoluciona mucho más deprisa que las medidas de seguridad que intentan combatirlo. Vivimos una época de mucha aceleración digital. En muchos casos pensamos y creamos servicios primero antes de verificar si son seguros.

El exceso de confianza de las empresas y los usuarios es la fuente principal del éxito de los grupos criminales en internet, que no solo han aumentado el número de sistemas comprometidos, sino que también aprovechan a las mismas personas para vulnerar o distribuir sus códigos maliciosos. Y es que la situación en el mundo de seguridad no ha mejorado debido a que los criminales se han sofisticado, mientras las empresas y usuarios se mantienen escépticos ante la posibilidad de ser vulnerados.

Además de la falta de mecanismos de coordinación que realmente sean eficaces para luchar contra este fenómeno, también se produce un proceso de profesionalización del *hacker*, que tiene un perfil mucho más comercial y con un trasfondo menos ideológico. La competencia también afecta a los ciberdelincuentes digitales y su entorno es tan duro y «profesional» como si trabajasen en Wall Street. El sector público, el financiero y las grandes compañías, son sus principales objetivos.

Pero muchas veces no hace falta ni un buen *hacker*. Existen informes que indican que 7 de cada 10 usuarios están dispuestos a entregar datos de su ubicación, nombres personales, acceso a sus perfiles de Facebook y de otras redes sociales a cambio de tener una aplicación gratuita. Incluso, casi un 20% de los usuarios llegan a reconocer desconocer por completo que existen aplicaciones capaces de obtener información en tiempo real de su ubicación.

Como sociedad hemos trasladado muchas de las cosas que hacemos en el mundo físico a internet, incluido el crimen. Lo extraño es que la gente entiende los riesgos de salir de su casa y dejar las ventanas y puertas abiertas, pero no están cerrando esas puertas en su vida digital. En algunos casos, como en las redes sociales, son los mismos usuarios los que hacen el trabajo de los cibercriminales.

Hablamos de «delitos TIC», porque parece que preocupa mucho. Entendemos, desde luego, que sea así, sobre todo a partir de determinadas conductas que alimentan el terrorismo por internet (apología, captación, etc.), y contra las que el legislador español ha considerado convenient-

te reaccionar a través de la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Pero el fenómeno internet afecta absolutamente a todas las ramas del Derecho, como hemos intentado demostrar en el presente estudio. De forma concreta, la propiedad intelectual es una de las materias del Derecho privado que más se ve afectada por las TIC. Otro tema estrella es el de la protección de datos. En efecto, el derecho fundamental a la protección de la intimidad, y del honor, y de los datos, queda absolutamente en entredicho por el uso social de internet. Esto es así hasta el punto de afirmar que la intimidad, en la actualidad, no puede estar garantizada ni por la ley (por muy restrictiva que sea) ni por el sistema, por lo que lo más sensato es ser consciente de este riesgo, asumirlo y actuar en consecuencia. Aquí la culpa quizá sea más del usuario que del legislador, aunque este, dicho sea de paso, actúa sorprendentemente como si pensara que se le pueden «poner puertas al mar».

Y en este contexto surge precisamente un nuevo «legislador» o poder legislativo, impropio pero real, lo cual supone sin duda uno de los paradigmas más interesantes que presenta la nueva realidad sociotecnológica desde el punto de vista jurídico. Nos referimos a los gigantes de la red. Hablábamos de protección de datos, y nos preguntamos qué importa la normativa española o incluso la europea al respecto, cuando usted acepta las condiciones de uso de WhatsApp o Facebook y, como vimos *ut supra*, simultáneamente acepta también, expresa o implícitamente, someterse a la normativa de protección de datos del estado de California. Y hablamos de condiciones de uso, conste, no de condiciones de privacidad. Hoy en día pasan muchas cosas pero muchas de ellas «pasan» en internet. Internet se rige por sus propias reglas y si usted se pasa de la raya en Twitter sepa que le cancelarán la cuenta. No será una sanción gubernativa sino de la propia red social. Seamos conscientes de quién marca las reglas del juego hoy en día.

En definitiva, este *Derecho TIC* y sus numerosas derivaciones, lo decimos honestamente, es la asignatura pendiente de muchos juristas... De los jueces, de los abogados, de los fiscales, de los funcionarios... La crítica es constructiva y se presenta a tiempo, porque hoy día es un tema más importante pero la progresión de esta tendencia es geométrica, con lo cual no solo crece sino que lo hace de forma exponencial. Y ello no porque se trate de una nueva rama del Derecho, sino porque es la nueva forma que adoptan los hechos jurídicos pertenecientes a todas las ramas (p. ej.: injurias a través de redes sociales). Las personas están y se relacionan en internet y por tanto los efectos jurídicos de esas relaciones también.

El ciberespacio no tiene fronteras y las relaciones, lícitas o ilícitas entre diferentes sujetos, tampoco. Con la irrupción de las TIC en el mundo, nos hallamos ante un fenómeno que no entiende de espacios, fronteras o ciudadanos, y que puede afectar a la vez a una multiplicidad de Estados o a ninguno en concreto, y a una pluralidad de sujetos de diversa nacionalidad.

En este sentido, el clásico principio de territorialidad, uno de los pilares esenciales del Derecho clásico, queda totalmente desvirtuado. El problema no es, no obstante, la pérdida del elemento geográfico del Derecho, sino más bien todo lo contrario: el fenómeno que hemos denominado «multiterritorialidad».

Por otro lado, el principio de territorialidad se basaba en el de soberanía, el cual ha quedado igualmente desfasado con esta nueva realidad, y que aconseja más que nunca derivar la *potestas* de los Estados «hacia arriba»: Derecho internacional –especialmente los tratados de derechos humanos–; Derecho europeo; e incluso gigantes de internet –Google, Twitter, Instagram, WhatsApp y otros dominadores de la red de algún modo sustituyen a los poderes legislativos con sus normas y condiciones de uso–; y también «hacia abajo», en este caso mediante una interpretación *sensata* del Derecho por parte de cada persona –principal pero no exclusivamente del ámbito profesional legal–, sin olvidar una mayor educación social –más en valores que en tecnología–. Considérese el presente como un alegato, en tiempos modernos, precisamente al derecho más antiguo, el primigenio: el Derecho natural. Esperemos que nuevas instituciones como el «derecho al olvido» –el cual hemos decidido no abordar a fin de no alargar innecesariamente el presente estudio– no supongan en realidad el olvido del Derecho.

Y para esa «interpretación sensata» a la que aludimos, como bien recuerda paradójicamente una de las leyes más antiguas, las normas deben interpretarse en relación con el contexto y la realidad social del tiempo en que ha de ser aplicada (art. 3 del Código Civil).

No era el objetivo del presente estudio desvirtuar el Derecho clásico, sino más bien al contrario: reforzarlo. Es por ello que hemos criticado instituciones del Derecho que se han querido mantener a toda costa o, en el otro extremo, que se han creado o pretenden crear *ex novo* de una manera, a nuestro juicio, totalmente artificial. Dicho con un juego de palabras: tememos que el derecho al olvido suponga el olvido del Derecho. La ley y la jurisprudencia son importantes, qué duda cabe, pero es responsabilidad de la doctrina y de los juristas prácticos interpretar correctamente el sistema de fuentes mediante los principios generales del Derecho, en cuyo caso esta posible desviación estará controlada. Y «correctamente» es con tino, comedimiento y sentido común. El sentido común es fuente del Derecho. No es el momento, pues, de ser ni demasiado conservador ni demasiado innovador, sino de realizar con tino las oportunas transformaciones o adaptaciones en nuestro nuevo modo de entender el Derecho. Y el mundo.

Bibliografía

ANNAN, K. [2003]: «Las TIC en las políticas de cooperación al desarrollo: Hacia una nueva cooperación en la Sociedad en Red», *Cuadernos Internacionales de Tecnología para el Desarrollo Humano*, 2. Ingeniería Sin Fronteras (ISF).

APC: *Carta de APC sobre derechos en Internet*, <http://www.apc.org/es/node/5795>

Convenio 80/934/CEE sobre la ley aplicable a las obligaciones contractuales abierto a la firma en Roma el 19 de junio de 1980.

D'ARCY, J. [1969]: *Declaración Cumbre Mundial Sociedad de la Información I Fase*, Ginebra: Naciones Unidas.

NACIONES UNIDAS [2003]: *Declaración de Viena sobre Derechos Humanos*, Viena.

– [1993]: *Declaración sobre el Derecho al Desarrollo*, Resolución 41/128, Nueva York.

UNESCO, [1996]: *Les Droits de l'Homme à communiquer*, París.

UNFPA [2002]: *La UNESCO y la Sociedad de la Información para todos*, París: UNESCO.

Ley 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.

Libro Verde sobre la transformación del Convenio de Roma de 1980 sobre la ley aplicable a las obligaciones contractuales en instrumento comunitario y sobre su actualización [COM(2002) 654 final – no publicado en el Diario Oficial].

Reglamento (CE) n.º 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales («Roma I») (Diario Oficial L 177 de 4 de julio de 2008).

Reglamento (CE) n.º 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales («Roma II»).