Revista Jurídica de la Universidad de León, núm. 5, 2018, pp. 191-226

RELATORÍAS DE LAS IV JORNADAS NACIONALES DE DERECHO Y CIBERSEGURIDAD

Evento académico celebrado los días 24 y 25 de octubre de 2018 en el Auditorio de León (día 24) y en el Salón de Grados de la Facultad de Derecho de la Universidad de León (día 25). Coordinado por la Prof.ª Dra. Dña. Isabel Durán Seco, Profesora Contratada Doctora (acreditada Profesora Titular) de Derecho Penal en la Universidad de León y por D. Francisco Pérez Bes, Secretario General del Instituto Nacional de Ciberseguridad de España

PRIMERA PONENCIA: **«Más allá de las criptomonedas. Potencial del *blockchain* e implicaciones en ciberseguridad»**
Ponente: **D. Carlos Kuchkovsky**, CTO de Nuevos Negocios Digitales de BBVA
Relatora: **Dña. Nerea Yugueros Prieto**, doctoranda de la Universidad de León (Área de Derecho Procesal del Departamento de Derecho Público General)

D. Carlos Kuchkovsky comienza señalando que el grupo en el que trabaja dentro del BBVA, Negocios Digitales, consiste en la creación de empresas con nuevos modelos de negocio, intentando de diferentes maneras, bien a través de construcción interna o adquiriendo, invirtiendo o haciendo *"partner"* generar un portfolio de nuevas oportunidades. En el caso de construcción interna, se encuentran trabajando en diferentes países, entre los cuales se encuentran San Francisco y Madrid, disponiendo de diversos emprendedores, los cuales se ocupan de la creación de nuevas aplicaciones, como sería COBOL, aplicación destinada a la seguridad de datos personales.

El ponente hace referencia a la practicidad que nos proporciona el *blockchain* a la hora de ayudarnos en los problemas de seguridad que sufrimos en la actualidad. Entre los ejemplos, nos menciona que gracias al *blockchain*, contamos con la capacidad para evitar tecnologías *blockchain* a través de alteración de servicios, así como mejora la

autenticación o la autorización de diferentes sistemas. A su vez, también eficiencia la infraestructura de claves públicas.

Mediante la ponencia se intenta generar una opinión entre los asistentes referente al nuevo internet o a la nueva economía que está generando, tecnología *blockchain* y los tokens. Debiendo, por tanto, definir cuáles son los nuevos retos de seguridad y las nuevas oportunidades que genera este nuevo internet.

El ponente hace referencia a un artículo encontrado, hace cuatro años, en una revista de cierta relevancia en el sector, que indicaba que, tras la web social, es decir, la web 3.0 que todos conocemos, venía la web de la confianza (The Trust Web). A su juicio, es algo impactante, dado que en ese momento todo el mundo defendía, que la web 3.0 sería la web semántica, es decir, muy categorizado y con nuevas sintaxis. Más le impacto que D. Tim Berners-Lee, padre de HTTP, se postulara en la idea de que internet estaba "roto", y por ello comenzó a investigar en los conceptos de internet de la confianza, sin olvidar la premisa de D. Tim Berners-Lee. Se entendió que la intención inicial de cuando se creó internet, era la posibilidad de la transmisión de información entre distintos ordenadores. El ponente resalta la palabra información dado que, en aquellos tiempos, únicamente se preocuparon del intercambio de información y no en la posibilidad de realizar pagos a través de internet. El reparo que ello conlleva es que, en la actualidad, a incluir el intercambio de valor y la identidad en este internet, es donde surgen los problemas de seguridad.

Asimismo, el ponente hace referencia a D. Vinton Cerf, científico que obtuvo el Premio Turing gracias al protocolo TCP/IP. Dado que en su momento no se consideró la existencia de Facebook o páginas similares, sino que únicamente se preocuparon en que los paquetes llegaran de un ordenador a otro para que transmitieran información.

Uno de los puntos principales que los pioneros argumentan es que nos estamos moviendo a la tercera era de internet. Ello conlleva la existencia de un gran número de datos, los cuales no se pueden utilizar ni interoperar. Ello supone una gran complejidad dado que la sociedad, entrega sus datos a cambio de aplicaciones gratuitas. Hay grandes iniciativas que intentan romper ese oligopolio.

Lo que intentan las plataformas es generar un nuevo internet descentralizado. Para ello debemos comprender que es el "internet del valor". El ponente nos indica que, a través de una red social, o una aplicación de mensajería, podemos transmitir información la cual puede ser útil para llegar a un acuerdo entre las partes, pero después es necesario acudir a una red de intercambio de valor (financiera) para transmitir el valor pactado en la red de información. Una de las cosas que permite la tecnología *blockchain* es que las dos redes, es decir, la de acuerdos sociales y la de intercambio financiero se unan en una única tecnología. Por ello, entiende el ponente, que se deben tener claras las oportunidades y los riesgos que se asumen en estas operaciones. Desde la perspectiva de la ingeniería, se entiende que se está generando un nuevo ordenador mundial, donde poder ejecutar unas aplicaciones seguras y donde los datos estén disponibles.

El ponente en su exposición se hace valer de un diagrama para explicar que en todas las capas de este podemos encontrar el *blockchain*.

El ponente hace referencia a los *Smart Contract*, los cuales no son contratos ni inteligentes, sino son códigos que se ejecutan en un sistema distribuido descentralizado donde está firmado de manera bilateral o trilateral por X partes, y una vez que está firmado se despliega en el ordenador global. Como caso práctico, el ponente indica que se usan con regularidad los *Smart Contract* en las cadenas de suministros. Por ejemplo, grandes vendedores y compradores, tiene mucha desconfianza cuando se hacen acuerdos entre países, ya que ninguna de las partes quiere proporcionar o bien el dinero o el material de antemano. Por ello, con el *Smart Contract* se definen unas condiciones donde en este caso, se solventarían con sensores en el contenedor de transporte, es decir, cuando el mismo se encuentre el puerto el 10% del pago se efectúa, cuando se encuentre en camino otro tanto, hasta alcanzar la totalidad del pago a su llegada. Si el paquete, en el transcurso del envío ha sufrido algún tipo de deterioro, sería objeto de las penalizaciones que se hubieran pactado en dicho contrato.

Lo que se consigue con una capa global, así como con los sistemas globales, es un mundo programable. Dado que nos encontramos en sociedades basadas en datos. Los datos son el nuevo valor. Los datos en crudo no valen nada y por ello hay que procesarlos. La primera capa de procesamiento es la información, es decir, saber que ha pasado; la segunda capa es el conocimiento, intentar entender que ha pasado; y la tercera la sabiduría, tener la capacidad de que sistemas analicen la información.

El ponente retomando las diferencias entre la web 2.0 y la web 3.0, hace referencia a las aplicaciones descentralizadas. Por ejemplo, hace referencia a las IPFS (*InterPlanetary File System*), los cuales intentan hacer un sistema distribuido descentralizado de almacenamiento, ya sean en un ordenador personal o en un ordenador de una empresa.

Como se puede apreciar a lo largo de la ponencia, todo versa alrededor de los datos, siendo en la actualidad un tema importante dado que se están ocasionando problemas en la seguridad, como son el robo de datos atentando a la privacidad, eliminación de identidad en las empresas, entre otros. Por ello, en la actualidad la sociedad puede elegir a quien y para que ceden sus datos.

El ponente hace referencia a los *token*, los cuales representan el valor en la actualidad. Estos pueden ser adquiridos por inversores, o pagar a usuarios tempranos con ellos, regalar a la sociedad a cambio de incentivos, etc. Lo más importante es que gracias a los token, no son necesarios los intermediarios, es decir, el intercambio de valor puede fluir entre los factores de un sistema, como ocurre con Spotify, Netflix, entre otros. Para finalizar hace referencia a que, gracias a los token, las empresas o particulares pueden obtener retornos de inversión por su tiempo y no únicamente retorno de inversión por inversión de capital.

Comentarios de la relatora

De la ponencia de D. Carlos Kuchkovsky puedo desgranar que realmente los primeros interesados en este tipo de tecnologías es el sector financiero, dado que su creación se basó en ser soporte de las criptomonedas. Ello no quiere decir que, con el tiempo, puedan integrarse en otros sectores, dado que facilitan y resuelven de manera considerable los problemas que surgen a lo largo del día. Por ejemplo, en la actualidad nos encontramos rodeados de dispositivos inteligentes, como son los móviles, vehículos, viviendas, entre otros; los cuales se encuentran interconectados. Siendo por tanto necesario un soporte de identidad digital, para que así, cuando se realice cualquier tipo de transacción, los datos personales no queden expuestos y accesibles a cualquier sujeto, de ahí la gran importancia de *blockchain*, dado que proporcionan esa seguridad de protección de datos.

SEGUNDA PONENCIA: **«La internet abierta»**
Ponente: **Dr. D. Pablo García Mexia**, Vicepresidente del Capítulo Español de Internet Society, jurista digital
Moderadora: **Prof.ª Dra. Dña. María Mercedes Fuertes López**, Catedrática de Derecho Administrativo de la Universidad de León
Relator: **D. Alfredo Estévez Jiménez**, Investigador de la Universidad Nacional Autónoma de México

El Dr. Pablo García Mexia inició su intervención señalando que el tema es una especie de "atalaya fantástica", esto en virtud de todo lo que ha estado sucediendo en internet en los últimos 20 años. Y matiza: hablar de la internet abierta, del acceso a la red, es una especie de ventana privilegiada para ver y conocer los problemas y conflictos que han venido cerniéndose sobre la red en estos últimos 20 años. Al considerar y conceptuar internet como una red abierta, a raíz de su éxito se han presentado amenazas, ante lo cual se formulan las siguientes preguntas: ¿Qué se ha estado haciendo para combatir estos problemas del futuro? ¿Qué significa internet abierta?

La internet tiene la cualidad de que es distribuida de alguna manera gratuita desde el arranque, muy flexible gracias a la computación o de paquetes que no dañan circuitos; siendo sobre todo abierta gracias a una característica tecnológica que es lo que los ingenieros llaman "el principio de extremo a extremo" que permite una enorme compatibilidad al permitir que cualquier dispositivo de cualquier naturaleza se pueda conectar. Hoy en día ya empiezan a conectarse hasta animales y las personas estando

cada vez más conectadas, los objetos de cualquier índole como ordenadores, dispositivos móviles, etc.

Esta característica es precisamente lo que adorna la red desde su arranque u origen y es esa compatibilidad la que se considera de algún modo la característica esencial de la red y que debe preservarse como característica esencial.

El ponente pregunta: ¿Cuáles son las amenazas que se van echando encima de la red? Señalando tres: 1. Por un lado estarían las que se refieren a los estándares, a los protocolos que hacen que internet sea más discernible. 2. La siguiente capa es la etapa física, la capa de infraestructura, no hay que olvidar que existe no solo por el software que se inventa hace 40 o 50 años sino gracias a que existen cables, tubos, éter, espectro radio eléctrico que transportan sondas, por los que se conectan dispositivos. 3. En tercer lugar la capa de contenidos que llamamos la etapa humana, o sea lo que volcamos en la red.

Las amenazas de la etapa lógica serian lo que podríamos decir las presiones de algunos estados a los que les incomoda fundamentalmente que por el hecho de que la red naciera en Estados Unidos, esta nación haya tenido preeminencia sobre el gobierno de la red y se dice gobierno porque si en algo se caracteriza internet en cuanto a su gobernanza es precisamente por ser muy cáustica, ha estado siempre controlada y gobernada por ingenieros y por lo tanto los juristas y los gobiernos y los estados han estado siempre muy al margen de ella.

Estados Unidos ha sido muy cauto en esta gestión de la red, teniendo un papel de custodio, de guardia final, pero ni eso ha satisfecho a lo largo de los últimos 15 años, sobre todo a partir del año 2000 a algunos estados autoritarios y algunos que no lo son, como por ejemplo la India que no está contenta con este modelo de la red, han venido presionando para que organismos que gestionen el sistema DNS de dominio o sistema de matrícula que permiten que los dispositivos se conecten entre sí, tomen en cuenta sus criterios a la hora de gobernar la red. Quien domine ican domina DNS, quien domina matriculas domina internet. Estos Estados han venido haciendo presión para que no solo sean criterios tecnológicos sino criterios políticos los que gobiernen la red. No son criterios de países occidentales basados en el estado de derecho y de la libertad, de la igualdad y la democracia.

La siguiente oleada de presiones en los últimos 15 años se ha venido cerniendo sobre lo que podríamos llamar la capa física. La tensión está entre las operadoras, las empresas de telecomunicaciones que han venido viendo cómo se reduce a través de la voz su negocio tradicional que tenían en descuido hace 30 o 40 años a raíz de la aparición de las empresas de internet, como son Google, Amazon, Microsoft y las que van entrando, las chinas y que ahora son las mayores en el mundo; estas empresas que ni siquiera existían ahora están entre las 10 mayores del mundo, generando tensiones, por lo que algunas operadoras han venido diciendo que por el uso de la red debiera pagarse un peaje y tal vez así no habría tráfico. Este sería el segundo frente de tensión.

El tercero, el de la capa humana y sobre las presiones y los contenidos (quizá si la dominan los juristas en esta sala) Las presiones sobre contenidos me gusta exponerlos

a través de doble perspectiva, a través de los velos que se han ido cerniendo sobre estos contenidos a raíz del bloqueo de ciertas páginas que puedan estar en la red motivados por criterios políticos públicos desde estados democráticos y no democráticos.

En estados democráticos está habiendo bloqueos más o menos justificados por seguridad nacional, por ejemplo "retiremos esta red porque tiene contenidos terroristas", hay muchas iniciativas que se han ido adoptando recientemente en Europa sobre este tema por supuesto de modo justificado. Así estamos hablando de bloqueo de contenidos en la red y por tanto una traba a esa internet que se diseña abierta, estos bloqueos se pueden deber también a propiedad intelectual, (este contenido está reproduciéndose y afectando derechos de autor) Otro caso tiene que ver con la libre expresión y la propiedad intelectual que avala a los autores, otro ejemplo, la privacidad, una variedad creada en Europa, llamada del derecho a dormir y que implica directamente el retiro de contenidos y que supone límites muy difíciles de trazar entre lo que debe retirarse y proteger la privacidad de alguien y los derechos del pasado de alguien, el derecho a saber determinados acontecimientos de ciertas personas más o menos públicas que puedan estar contenidos en la red.

En síntesis, bloqueos por políticas públicas a raíz de motivos más o menos justificados o discutibles propios de países democráticos o países no democráticos.

Las técnicas de bloqueo. En Internet Society hemos hecho un estudio concienzudo sobre cuáles son los 5 métodos básicos para retirar contenidos en línea, a través de las url, de otra plataforma de internet, a través de inspección profunda de paquetes, etc.

A raíz de la necesidad de los estados en casos como la seguridad nacional de imponer bloquear contenidos en línea, internet ha ido parcializándose o astillándose; un problema que ha venido aquejando a internet desde su origen es el hecho de que al ser una red mundial ha sido muy difícil seguir ciertos ilícitos y delitos que pueden ser reprobables como consecuencia de que existen jurisdicciones y soberanías de Estados, esto ha ido haciendo difícil la persecución de hechos más o menos reprobables y que puedan tener un reflejo grave, esto va alejando cada día más a internet de ese ideal inicial que sería una red punta y simplemente debe limitarse a transportar contenidos, ese es el fondo de su ADN.

Continúa señalando que la siguiente amenaza sobre los contenidos es lo que llaman las fallas, se habla de silos, del hecho que internet se ha ido erigiendo en una especie de tanques de contenido inconexos y estamos entre que si me enfado de Facebook no puedo bajar contenidos y llevarlos a otra red que me guste; internet se ha ido transformando en un reino de imperios individuales que no conectan entre sí y contrarían el empeño inicial con que fue diseñada.

El Dr. Pablo García pregunta qué se ha ido haciendo para arreglar el problema: en primer lugar, hace alusión a que Barack Obama en 2014 dijo, que Rusia, China o algún otro Estado quieren que internet se estatalice, pues adelante, se abrió una negociación en 2016 que permitió que Estados Unidos ya no sería garante único pero tampoco Rusia o China o cualquier otro Estado tenga la exclusividad en lo que se

refiere al código de internet: La primera condición de Obama fue que internet fuera una red abierta y hasta ahora así sigue; la segunda condición es que se mantuviera el modelo multilateral de gestión que hasta ahora se venía utilizando, que no solo fueran los Estados sino también la comunidad académica y las empresas quienes pudieran gestionar el control de la red. Otra vía de salvaguarda sería considerar que el acceso a las redes es un derecho ciudadano, La Organización de las Naciones Unidas ha intercedido porque esto se reconozca, el consejo de Europa, países como Estonia desde el 2000 y España 2003, pueden bajar contenidos de 1 mega y Finlandia a partir de 2015 tiene bajadas de hasta 100 megas y tienen que garantizar que cualquier residente en este país pueda bajar contenidos de hasta 100 megas.

Al respecto existe un debate, hay quienes dicen (algunos países y o líneas jurisprudenciales como el Tribunal Europeo de Derechos Humanos), esto es consecuencia al derecho de la libre expresión, porque el internet es el campo más importante y más útil para mantener este derecho pues que sea consecuencia de él y por supuesto la libre información; otros en cambio dicen, no, es que el internet no solo depende hoy de la libre expresión y de la ley de información, internet depende también de la política y por tanto de los derechos políticos, depende de la empresa, incluso de la propiedad intelectual y estarán echando en falta la educación.

Internet tiene suficiente entidad como para ser hoy en día un derecho autónomo, resulta que la libre protección de datos en debate en cortes generales como proyecto incluye este acceso a la red en una carta de derechos digitales que en modo creativo en lo que es al fin una ley de protección de datos, pero interesante.

Otro aspecto es la neutralidad de la red: Que trata de garantizar un acceso no discriminatorio, o sea que no puedes tratar distinto ciertos contenidos, el sistema no puede ralentizar contenidos, internet no puede priorizar un tráfico sobre otro si al final acaba teniendo uno u otro de esos resultados. Resumiendo, que internet siga siendo ciega, que no preste atención al contenido que está transportando, esto implica que las operadoras no puedan gestionar tráfico. Las operadoras tienen que gestionar tráfico porque de lo contrario internet se pararía. ¿Qué motivos hay que justifiquen una intervención y por tanto harían que esa gestión sea razonable? uno es indiscutible, la seguridad, otro, la transgresión de las redes, por lo que las operadoras tienen que intervenir para evitar que las redes se saturen y por lo tanto se bloqueen, por lo que las operadoras tienen que regular el tráfico.

Y en tercer lugar el cumplimiento legal. Hay ocasiones en que las normas exigen la posibilidad de gestionar esas redes por motivos siempre que sean justos. La norma Europea 2015-2020 regula esto y lo garantiza en Europa, aunque hay algunos supuestos más discutibles; los paquetes que las operadoras nos ofrecen como consumidor por ejemplo para ver TV nos permite acceder a la red, permite ver ciertos programas y ahí empieza el problema porque las operadoras suelen hacerse de facultades de gestión de las redes para garantizar la calidad del servicio (término clave) que como consumidores tenemos derecho a disfrutar y aquí hay un margen muy amplio para que las operadoras gestiones de modo muy amplio sus operaciones.

La segunda conducta gris o prácticas de cero rating o facturación cero, es cuando si te pasas de megas no vas a pagar de más siempre y cuando consumas de la empresa que contrataste, por ejemplo, si estás en Facebook y ves otras redes con otros contenidos, y luego regresas a facebook, te cobro, esto sería ilegal según el reglamento europeo siempre y cuando no se restrinjan las operaciones de elección de los consumidores. Europa se queda sola en la defensa de la neutralidad de la red porque la norma norteamericana del 2017 se ha cargado a la normativa primera que ha existido, que hace que Estados Unidos dé expansión global. La nueva administración la ha suprimido y por eso Europa está junto con Brasil y algún Estado significativo haciendo defensa de la neutralidad de la red.

Ante esto es muy importante una privacidad centrada en el ciudadano que ayuda a la internet abierta y al acervo de la red, que como ciudadanos debemos disfrutar y en este sentido el nuevo reglamento ha expuesto por ejemplo la visión de privacidad y de toda normativa que implica centrar al ciudadano; esto es muy importante, esta obsesión que el reglamento pone en que seamos nosotros quienes controlemos nuestros datos realmente ayuda sobre todo a la hora de crear nuevos derechos, (por cuestión de tiempo se centrará en uno solo), el derecho de portabilidad del dato, podría decirse es el mejor torpedo que se ha creado para disolver esos silos (no está proponiendo que desaparezcan Google, Amazon ni Facebook) lo que da a entender es que esto nos da una libertad como usuarios de poder deambular por la red, por internet sin tener que depender como hasta ahora de los grandes gigantes.

A partir de esto se puede hablar de un derecho a la propiedad sobre los datos, el reglamento no lo ha hecho, pero podría ser un antecedente, hay muchas empresas que han crecido gracias a la propiedad de nuestros datos y deberían compartir algo con nosotros, como dicen en California, los españoles somos una especie de trabajadores de datos. La autoridad Catalana de competencia ha dicho que los datos deberían formar parte del activo de las empresas y deberían valorarse a la hora de valorar por ejemplo a Facebook, a Amazon a Telcel, que no valen por los edificios ni el personal que tienen sino valen por los datos de gestión y que son nuestros datos, al hablar de una internet más abierta y si nosotros pudiéramos patrimonialmente decidir (gracias a esta propiedad) a quien le damos nuestros datos, no solo a Google o Facebook o Telcel etc. Estaríamos favoreciendo nuevos entrantes, agilizando y equilibrando el mercado y haciendo una red más abierta.

El Dr. García Mexia abunda que el futuro está marcado por 2 elementos clave: La corregencia tecnológica, resalta la OCDE que del 4 al 14 estaremos con ansias de expandir internet sobre todo en banda ancha a lo largo y ancho del mundo, pero a partir del 2014 y hasta el 2024 estaremos marcados por una convergencia tecnológica que va a hacer que las redes de datos y redes de voz converjan y exijan grandes plataformas que van a provenir en algunas partes del mundo audiovisual, de los clásicos ordenadores o de las empresas del mundo de la red, pero que terminarán siendo lo mismo; telefónica es el mejor ejemplo, en line telco quiere hacer cosas como las hace Google o Amazon y si al final en las plataformas todos acabaran haciendo de todo y lo mismo, ¿Por qué no aplicar reglas para todos? Podrían ser reglas razonables de competencia, de consumo, etc. ¿Por qué no plantear una normativa de telecomunicación? ¿No sería necesario regular expresamente a las plataformas como

se ha venido propugnando en Europa a raíz de la iniciativa del mercado digital casi con fobia a las empresas norteamericanas?, tal vez las mismas reglas para todos serían razonables, reglas que serían las de competencia, las de consumo, las de propiedad intelectual y más.

En la intervención, el ponente se refiere al Blockchain, que es una base de datos actualizada y pulcra que corre instantáneamente por internet de manera que cualquiera puede alterar un contenido sin necesidad de centralización, puede influir en que sin necesitar ican o dns gracias a blockchain los ciudadanos usuarios de la red podrían almacenar sus contenidos en su propia nube, el sistema de matrícula pierde fuerza y por tanto pierden fuerza las presiones y de esa manera se haría internet más abierta gracias a esa tecnología; sin embargo, todo esto debe manejarse con cautela.

Y señala que si a través de blockchain se obtiene la información, para que necesito intermediarios, si puede acabar habiendo redes sociales que no necesitan al facebook, al router en turno o a la red como empresa, porque yo puedo compartir con confianza los contenidos en la red, para que necesito a ese particular, si puede haber buscadores confiables que empleen esa tecnología para que necesito buscadores específicos, si puede haber mercados en línea que utilicen esta tecnología y confío en que quien vende es realmente el propietario no necesito a Amazon; por ejemplo, gracias a la criptografía no necesito mercados centralizados. La gran aportación de blockchain es: redes ultra distribuidas, descentralizadas que permiten alterar contenidos porque están criptográficamente basadas, lo que se altera está tecnológicamente garantizado, porque si alguien dice que tiene algo es porque es así realmente.

Finalmente, el Dr. Pablo García Mexia realiza las siguientes conclusiones:

Las amenazas van a más, ¿Resistirá Marruecos? está quieto, las cosas no van bien para la neutralidad de la red, ya que los bloqueos políticos no solo siguen sino que aumentan, está muy de moda bloquear políticamente la red de un modo más o menos justificado, se está abriendo una nueva corriente que es imponer a los demás mis propias normas, un ejemplo muy claro, con el derecho al olvido, Europa está pretendiendo imponer el derecho al olvido a lo largo y ancho del mundo. Los defensores de esta tesis dirán que si no el olvido no servirá para nada, si resulta que si un ciudadano japonés se puede enterar de cosas que yo no quiero que se sepan en Europa pues al final pues no sirve de nada al cabo internet es global, y pregunta ¿Tengo derecho de imponer a ese japonés que no se entere de cosas que tal vez el quiera o tenga derecho a saber y que afecten a ciudadanos europeos? Sería como decir, mis leyes son absolutamente para todos y las suyas solo para usted, es una corriente que se está viendo no solo en Europa también en casos de propiedad industrial.

En este sentido y entendiendo que la gobernanza multilateral es un asunto de occidente, el derecho ciudadano de acceso a la red tiene un sentido de libertad y democracia en los países donde hay democracia y libertad. Aunque no somos perfectos, de momento son los occidentales los que garantizan estas dos condicionantes como salvaguarda.

La tarea de la red, las salvaguardas son nuestras, las montan los norteamericanos y ahora las defendemos nosotros junto con Brasil. Hay competencia en China, pero se entiende de manera diferente en España o en un contexto como es Europa.

Ver con optimismo sería que todos nos rijamos por una sola batería de normas que vincule a todas las plataformas y ayude a la internet abierta, porque disminuirían las tensiones sobre todo por parte de las empresas de telecomunicaciones, operadoras que quizá estén menos tentadas a imponer medidas que de alguna manera impidan una apertura o flujo de tráfico en internet que merecemos acostumbrados como ciudadanos.

Blockchain debe ser una internet abierta en la medida que puedan disminuir intermediarios, en la medida en que esos factores tecnológicos blockchain puedan descentralizar aún más internet autenticar y a la vez criptográficamente garantizar la seguridad, probablemente estemos en tiempos mejores.

Comentarios del relator

De la exposición del Dr. Pablo García Mexia destaca el papel protagónico de internet tanto en las comunicaciones como en el desarrollo de las sociedades occidentales. A ello no escapa la influencia que la internet tiene en los diferentes ámbitos de la vida de las naciones como son el ámbito de la política, del gobierno, de las políticas, públicas, de los derechos de autor, de la educación, entre muchas otras más, que llevan a replantear los enfoques respecto del uso de la red como un derecho estrechamente vinculado con el derecho a la información. Así también destaca la internet abierta como una tendencia que contrapone por un lado el derecho universal de los ciudadanos a hacer uso libre de los contenidos, a la tentación de los Estados a controlar y regular sus accesos, tomando relevancia la normativa europea sobre la que se privilegia el uso de la red con libertad y democracia, propias de las democracias occidentales.

MESA REDONDA: **«Obligaciones del empresario en la implantación de medidas. Su responsabilidad»**
Ponentes: **Dña. Ana del Ser López**, Ilma. Sra. Presidenta de la Ilma. Audiencia Provincial de León
Prof.ª Dra. Dña. María A. Trapero Barrales, Profesora Titular (acr. Catedrática) de Derecho Penal de la Universidad de León
Moderadora: **Dña. María Isabel Morán**, Ilma. Sra. Fiscal Jefe de la Fiscalía Provincial de León
Relatores: **D. Alfredo Alpaca Pérez**, Investigador Contratado Predoctoral en la Universidad de León (Área de Derecho Penal del Departamento de Derecho Público) (*relata la ponencia de Dña. Ana del Ser López*)
Dña. Stephanía Serrano Suárez, Investigadora Contratada Predoctoral FPI de la Universidad de León (*relata la ponencia de Dña. María A. Trapero Barreales*)

Dña. Ana del Ser López inicia su presentación destacando el aspecto central de esta: la responsabilidad por no tomar las medidas legales oportunas. Esa responsabilidad

puede derivarse para una empresa no solo por el incumplimiento de la normativa legal, sino también por la inobservancia de normas básicas de seguridad que impiden, por ejemplo, los ciberataques. La ponente señala que, en la actualidad, nos situamos en un entorno tecnológico que nos exige una adaptación urgente. Las tecnologías van tan rápido que legislativamente no es posible ir a la misma velocidad. Por este motivo, la ciberseguridad en las empresas tiene que ser una prioridad, que exige, por parte de todos, un compromiso muy claro. Cada empresa debe controlar su propia organización, esto es, debe saber los riesgos a los que se expone en la concreta actividad en la que se desarrolla. Pero no solo las empresas: lo mismo es exigible también a los organismos públicos y a otras entidades privadas. Es importante, por eso, controlar los aspectos técnicos de la ciberseguridad, cuestión que, como señala la ponente, parece ser lo más demandante.

Con esta visión amplia, se deben determinar, según la ponente, los riesgos para las empresas, es decir, los puntos débiles. Una vez se tenga esto claro, será posible evaluar e implementar medidas necesarias para evitar los ataques, para la protección de datos, etc. A nivel legislativo o judicial, la respuesta que se le da a la responsabilidad en la que incurren las empresas, según del Ser López, es una respuesta en la que se tienen que aplicar las acciones clásicas con las que se trabajan hasta el momento. Al respecto, la ponente menciona un ejemplo que, si bien no se produce en una empresa, es también aplicable a lo que sucede en esta: la filtración de datos de la víctima en el caso de "La manada".

La ponente destaca que el interés mediático por este caso fue excepcional. Los gabinetes de prensa a disposición de los jueces se encargaron de otorgar a los medios la información en condiciones de igualdad. Del Ser López explica que un gabinete de prensa está constituido por periodistas que conocen las necesidades de otros colegas y que trabajan para el Consejo General del Poder Judicial (en adelante, "CGPJ"), que es el órgano de gobierno de la judicatura. Pues bien, explica del Ser López que en España los jueces cuentan con el expediente digital, recurso que, en comparación con otros países de Europa, ha sido implementado en un tiempo considerablemente rápido. Sin embargo, precisamente por esa rapidez, es que se producen situaciones en las que los jueces no han controlado los riesgos. Este escenario es, según la ponente, absolutamente extrapolable a lo que sucede en las empresas. En el caso que la expositora utiliza como ejemplo, la Letrada de la Administración de Justicia de la Audiencia, remitió el texto de la sentencia al gabinete de prensa del Tribunal Superior de Justicia. En ese sentido, se le solicitó expresamente a este gabinete (que prefiere por lo general trabajar con el texto original y no con una versión escaneada, por ejemplo) que tuviera especial atención con el contenido de la sentencia y borrara los datos personales de la víctima.

Del Ser López señala que, al estar "digitalizada" la administración de justicia, los jueces aplican la firma digital y hay un código seguro de verificación en el documento original que nadie sabía (por lo menos no el gabinete de prensa ni tampoco la Audiencia) que permitía, a través de una página web de la Administración navarra, acceder al texto original de la sentencia con todos los datos de la víctima. En algún medio de comunicación, relata la ponente, salió la noticia de que la Agencia Española de Protección de Datos (en adelante, "AEPD") estaba investigando los hechos para

imponer multas y estaba indagando, también, por los jueces. En este punto, la ponente considera pertinente explicar que los jueces, en lo que respecta a los ficheros judiciales, salen del ámbito en el que la ANPD puede multar. De esta manera, dice del Ser López, se garantiza la independencia del Poder Judicial. Por lo tanto, en el ámbito judicial, es el CNPJ el que investigaría un caso como este. La ponente relata que es cierto que la AEPD ahora mismo está investigando todos los "rebotes" de los datos de la víctima (así como los vídeos) fuera del ámbito judicial (es decir, no a los jueces). Esto puede conducir, en su opinión, a una responsabilidad expresada en una multa (impuesta por la AEPD), por esa filtración de datos. En el caso de los jueces, por el contrario, si dentro de su actividad se filtra la información, entonces ellos tendrán una responsabilidad disciplinaria, pero bajo la autoridad del CGPJ y no de la AEPD. La ponente señala que los medios de prensa frecuentemente confunden ambas cuestiones, por lo que, en su opinión, es importante y pertinente aclarar la situación.

Retomando el caso, del Ser López señala que se abrió una investigación por parte del CGPJ para determinar lo que había pasado. En un primer informe, la mencionada entidad atribuyó toda la responsabilidad a la Letrada de la Administración de Justicia, lo que, en opinión de la ponente, parecía no ser un resultado justo. Luego, el CGPJ emitió otro informe y señaló que en este caso se produjo un "fallo de carácter sistémico", lo que, según la ponente, quiere decir que "falló todo", esto es, que todos los ámbitos de competencia involucrados en este caso fueron afectados.

Del Ser López señala que los factores que llevaron a esa conclusión fueron varios. Por un lado, al haber mucho interés mediático, se explica la rapidez con la que se exigía la sentencia. Este sería un primer factor determinante. Después, ese "fallo sistémico" se explica también por la falta de medios técnicos. Esto se manifiesta, según la ponente, de esta manera: en el expediente digital, no se pueden disociar los datos, esto es, no se puede dejar la firma digital del documento y que los otros aspectos funcionen al margen. Además, no existían medidas de seguridad en la Administración navarra que impidieran el acceso de cualquiera a la página web: no tenía filtros de acceso y nadie se había percatado de ello. Luego, nadie (los letrados, los periodistas de los gabinetes de prensa, los presidentes de Audiencia, ni los jueces) tienen formación en firma digital, por lo que desconocen el riesgo. A parte de todo esto, continúa la ponente, hay una administración prestacional (que la pueden tener las Comunidades Autónomas que tienen transferidas competencias a la Administración de Justicia, lo que sucede en Castilla y León) aparte de la autoridad de control, por lo que el sistema de control está disociado: la autoridad de control es el CGPJ, pero la administración prestacional, quien implanta los sistemas o "digitaliza", es, en el caso de Navarra, la administración autonómica de Navarra. Se implementan sistemas digitales, pero de forma disociada a la autoridad de control que es el CGPJ. Al no haber una instancia general que se encargue de una coordinación más amplia, no se sabe exactamente quién puede ser responsable por los fallos o el mal funcionamiento.

En todo caso, del Ser López señala que, en el último informe de la CGPJ antes mencionado, se señalan una serie de medidas de seguridad a adoptar, esto es, una guía de recomendaciones para los jueces. Esto es muy importante pues, por ejemplo, la ponente señala que ella dispone de un pequeño portátil en el que cuenta con acceso a los expedientes digitales. Ella puede emplear la firma digital a través de una tarjeta.

Pues bien, la expositora comenta que nadie le ha indicado si, por ejemplo, puede firmar mientras viaja en tren o estando en el extranjero, o si fotocopia una sentencia y la tira al basurero de casa. Del Ser López busca resaltar con este ejemplo que no ha sido informada debidamente sobre las cautelas que debe tener en cuanto al empleo del expediente digital. Pues bien, el CGPJ ha decidido abordar el asunto y por eso elabora una guía de recomendaciones para la carrera judicial y además cambia el protocolo de comunicación. Es decir, informa a los periodistas de los gabinetes de prensa quiénes son los responsables y cómo se tienen que notificar.

Con las consideraciones expuestas, del Ser López quiere destacar que los fallos que ocurren dentro de la Administración de Justicia pueden ocurrir, con sus particularidades, evidentemente, también en las empresas. Así, afirma que la empresa debe concretar los riesgos de cada actividad. Ciertamente, las empresas privadas podrían no tener tanto riesgo con la filtración de datos como tiene la Administración de Justicia con los ficheros judiciales, pero cada empresa debe concretar los riesgos derivados de su actividad. En ese sentido, se debería elaborar un plan de obligaciones básicas e impartir las instrucciones necesarias para que se cumplan esas obligaciones y así evitar los riesgos propios de un ataque informático, por ejemplo (que podría incluir, sin dudas, la filtración o el apoderamiento ilícito de datos personales).

Entonces, la ponente pretende destacar las obligaciones que debe cumplir la empresa y las responsabilidades como consecuencia del incumplimiento de esas obligaciones. La ponente alude a un decálogo propuesto por INCIBE, referido a unas normas básicas que se deberían cumplir en el ámbito empresarial. Estas serían: localizar la normativa de seguridad dependiendo de la actividad de cada empresa, controlar los accesos a los equipos, tener copias de seguridad, contar con protección por antivirus, protección antimalware, actualización del software, control de los soportes, el registro de actividad para detectar anomalías y, en caso ocurra alguna contingencia, garantizar la continuación del negocio teniendo las correspondientes copias de seguridad. La ponente señala que estas no son normas legales, sino que son disposiciones de sentido común que son conforme a la realidad tecnológica en la que vivimos.

Aparte de esta normativa básica, del Ser López señala que sí que hay unas obligaciones legales, cuyo incumplimiento genera responsabilidad. Así, comenta que la más destacada en este ámbito es la normativa referida al control de datos, esto es, el Reglamento General de Protección de Datos, que es un reglamento europeo que se aplica directamente pues el Estado lleva cierto retraso en la aprobación que adapta el Reglamento y que detalla las cuestiones un poco más genéricas al ordenamiento español que es la Ley Orgánica de Protección de Datos (que, para su adopción, ha pasado ya la fase del Congreso y solo falta el Senado). Esta normativa sobre protección de datos, según la ponente, es la que prevé más consecuencias (esto es, responsabilidad) para las empresas. De entre otras muchas, la ponente solo hace referencia, por su importancia, a la Ley de servicios de la sociedad de la información y la Ley de propiedad intelectual.

Del Ser López reconoce entonces diversos planos sobre la responsabilidad que se pueden abordar. El primero es la responsabilidad penal, que no abordará en su ponencia. Luego, destaca la responsabilidad que se deriva del incumplimiento,

principalmente, la de carácter administrativo, cuyas multas son bastantes altas. Este tipo de responsabilidad, al ser un supuesto de infracción de la normativa de protección de datos, se hace efectiva por medio de multas impuestas por la AEPD. Es posible reconocer también, según la ponente, una responsabilidad laboral contractual, en el caso en el que los trabajadores de una empresa infringen principios de confidencialidad o no cumplen con las normas básicas de seguridad que la empresa les dice que deben cumplir. Es una responsabilidad laboral en la medida que la exija la empresa al empleado. Y es una responsabilidad contractual cuando contrata la seguridad con terceros.

Ahora bien, del Ser López señala que concentrará su atención en la responsabilidad civil, por ser su especialidad. Este tipo de responsabilidad, según la ponente, no se exige mucho en los tribunales. Sin embargo, pese a las nuevas formas de aparición de los daños (nuevos retos o nuevas amenazas en el ámbito de la tecnología), la ponente señala que se pueden recurrir a las acciones clásicas, especialmente, la responsabilidad por daño. Esta se puede dar por incumplimiento de normas básicas de seguridad y también por incumplimiento de normas legales. Por ejemplo, en el caso de que después de un ciberataque, las empresas siguen sin tomar medidas y se afecte a una compañía aérea, lo que hace que muchos pasajeros se queden sin poder viajar. En este caso se puede declarar la responsabilidad por daño de la compañía aérea, por no haber adoptado las medidas de seguridad (no legales) básicas por negligencia (cuestión que, evidentemente, ha de ser probada). Ahora bien, en el caso de obligaciones legales, por ejemplo, una filtración de datos, el perjudicado puede actuar de la misma manera: una cosa es la responsabilidad administrativa (que no le concierne al perjudicado) y otra, que puede ir de manera paralela, es la responsabilidad por daño, actuada ante los tribunales. En este último caso, no hay que esperar la resolución administrativa y, además, la indemnización es independiente de la multa que se pueda imponer a la empresa en sede administrativa. Se tratan de dos vías distintas. Aun así, las empresas, señala la ponente, siguen sin adoptar medidas. Esto puede explicarse por los posibles altos costos de tal adopción (actualización de software a precios elevados, falta de sensibilización, por ejemplo).

La ponente señala finalmente que la ley que se aprobará próximamente, una vez que supere la fase del Senado, alude a la responsabilidad que deriva de los principios que establece el Reglamento de Protección de datos, pero que hoy, como se dijo, se pueden aplicar directamente. Del Ser López ya ha reconocido algunos aspectos relevantes para la empresa. Primero, el principio de responsabilidad activa. Esta cambia el sistema de funcionamiento de las empresas en materia de protección de datos: la empresa debe probar o acreditar que ha cumplido con las obligaciones que le exige el reglamento, esto es, que ha evaluado adecuadamente su tratamiento de datos personales, que las medidas de seguridad son adecuadas y eficaces, que aplica una política interna clara en materia de privacidad, que exige cumplimiento a los encargados del tratamiento de los datos, entre otros. Es decir, según la ponente, se produce una inversión de la carga de la prueba: no se exige al demandante que acredite el incumplimiento, sino que es la empresa la que debe probar que la política que aplicó, la aplicó correctamente. Según del Ser López, este aspecto es el que en mayor medida puede afectar al momento de exigir responsabilidad a las empresas. Aunque

aún no se haya visto su funcionamiento en la práctica, se trata de un aspecto novedoso desde la perspectiva judicial.

También se derivaría responsabilidad de otro de los aspectos contemplados en el reglamento: la obligación de comunicar, en determinados supuestos, las violaciones de seguridad. Esto refleja una mayor seguridad probatoria para aquel que se ve afectado y ve que sus datos no se han protegido o se han tratado mal. En este escenario, como señala la ponente, se vuelve a invertir la carga de la prueba si no hay comunicación de esa violación de seguridad. Otro aspecto es el referido al consentimiento expreso: no cabe el consentimiento tácito en materia de protección de datos. Este es, según la ponente, otro cambio importante del que se puede derivar responsabilidad para la empresa, pues será esta la que tenga que acreditar, en un determinado supuesto, que contaba con el consentimiento expreso y limitado para el tratamiento de los datos. Del Ser López comenta también sobre algunos aspectos transnacionales del Reglamento que facilitarían las reclamaciones en el supuesto de empresas que pueden no estar en la Unión Europea pero que estarían obligadas a tener un representante en este ámbito, para así facilitar las reclamaciones en estos casos. Finalmente, la acción seguiría siendo la misma: la de responsabilidad civil por daño. Al respecto, la ponente considera que podría ser interesante el ejercicio de acciones colectivas. Este, recurso, sin embargo, en España puede ser problemático, pues la regulación es, en su opinión, defectuosa. Asimismo, la ponente señala que este tipo de acciones tendría como principal desventaja el no poder identificar la indemnización concreta para todos los perjudicados. Se trata de un tema, en todo caso, que debe ser meditado de cara al futuro.

Del Ser López señala, citando a la Comisaria de Justicia de la Unión Europea, que necesitamos normas modernas para responder a nuevos riesgos. En España se tiene en este momento el Reglamento y la Ley Orgánica que se está desarrollando. Hay una gran expectativa por ver los alcances de la aplicación práctica de la regulación, esto es, la actitud de los ciudadanos ante los nuevos derechos (esencialmente: si hay reclamaciones o no). En la práctica, señala la ponente, no se cuenta aún con un incremento de los procedimientos de reclamo por perjuicios por alguna infracción de las que aquí se ha comentado. Por otro lado, del Ser López alude aquí al Director de Operaciones de la Agencia de Seguridad de las redes y de la información de la Unión Europea, quien sostuvo que los usuarios en Europa se están empezando a despertar y a dar cuenta que quieren más seguridad. Esto, señala la ponente, podría contrastarse con el hecho de que las empresas por lo general no denuncian los ataques cibernéticos, sino que estos se denuncian a nivel particular cuando se accede a una cuenta corriente, por ejemplo. Este hecho debe ser destacado pues, como indica del Ser López, si no hay denuncia la Fiscalía no puede actuar.

Finalmente, la ponente destaca que la empresa funciona por lo general con sociedades de capital (por ejemplo, la sociedad anónima limitada que, en el caso de responsabilidad, responde con su patrimonio). Ahora bien, en el caso de que la empresa no cuente con un patrimonio suficiente para enfrentar un supuesto de responsabilidad, del Ser López plantea la cuestión de si es posible derivar la responsabilidad del administrador de la empresa, algo que ella considera viable. Esto es así pues las acciones clásicas, previstas en la Ley de Sociedades de Capital, también

se aplicarían a estos supuestos. Ahora bien, con respecto a la responsabilidad civil, la ponente señala que existen dos posibilidades de exigir al administrador de la sociedad que responda por el perjuicio causado por la empresa: la acción social y la acción individual. La primera es aquella en la que la propia sociedad se dirigiría contra el administrador negligente para que repare el perjuicio causado por esa negligencia. La segunda es aquella en la que cualquier perjudicado le puede exigir al administrador por el daño que ha provocado el incumplimiento, tanto de obligaciones legales como de normativa interna de seguridad. ¿Qué administradores responden? Responderían, según del Ser López, el administrador formal de la empresa y también podría hacerlo el administrador de hecho.

Comentarios del relator

Como bien ha destacado la ponente, muchas veces el Derecho tiene que hacer frente a los nuevos retos impuestos por el desarrollo económico con el instrumental clásico que, a primera vista, podría parecer insuficiente para brindar soluciones satisfactorias a los nuevos problemas. En ese marco, Dña. Ana del Ser López ha destacado que, en el ámbito del Derecho civil, se han mantenido las tradicionales instituciones de la responsabilidad (contractual y extracontractual) en la que podría incurrir la empresa en estos nuevos escenarios, caracterizados por la irremediable utilización de medios electrónicos, tecnológicos e informáticos. El caso de la protección de datos personales, que constituye indudablemente y hoy más que nunca, un derecho fundamental, parece ser un ámbito sensible para el Derecho, principalmente, porque su manejo y conservación se produce mediante la utilización de herramientas modernas que, eventualmente, tanto en el ámbito público (el de la Administración de Justicia, por ejemplo) como –principalmente– en el ámbito privado (el de las empresas), pueden haber fallos que desencadenen situaciones perjudiciales para los titulares del mencionado derecho. Por este motivo, tanto las entidades públicas como las privadas tendrán que adaptarse a la nueva regulación europea sobre protección de datos. Como correctamente ha destacado la ponente, esta nueva regulación se sostiene, entre otras cuestiones, en el principio básico de la responsabilidad activa, lo que hace que las entidades, públicas y privadas, tengan que aplicar medidas (que, por cierto, pueden ser flexibles y funcionales a las necesidades de la empresa, pero en todo caso deben ser eficaces) con las que se pueda garantizar el derecho a la privacidad. En definitiva, la Ley Orgánica de Protección de Datos de Carácter Personal (que creó la AEPD), el Real Decreto 5/2018, de 27 de julio (de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, con la que se pretendía brindar cobertura legal a los aspectos que debían ser urgentemente regulados para que pueda ser aplicada la normativa europea, y no esperar a la aprobación de la Ley Orgánica) y la futura Ley Orgánica (que se encuentra en fase de tramitación parlamentaria) constituyen instrumentos fundamentales para resguardar no solo el derecho de protección de datos personales, sino también otros de gran importancia como el derecho al olvido (que es una de los principales asuntos que se abordan en el nuevo reglamento europeo sobre protección de datos).

La Prof.ª Dra. Dña. María A. Trapero Barreales inicia su exposición señalando que, si es difícil plantear la responsabilidad penal de la propia empresa o de las personas físicas que desarrollan su actividad dentro de la empresa, más complicado es aún

todavía si esa responsabilidad viene derivada de la utilización de nuevas tecnologías. La ponente plantea la posibilidad de la responsabilidad por no haber adoptado medidas de seguridad en materia de ciberseguridad que hubieran evitado la comisión de delitos por parte de las personas, sobre lo cual señala que desde el punto de vista jurídico-penal no existe tal responsabilidad, en razón a que siempre se tienen que mantener y aplicar los principios limitadores y garantísticos del derecho penal. Fundamentalmente, el principio de legalidad y el principio de responsabilidad subjetiva, principio de culpabilidad o principio de responsabilidad personal. Estos principios constituyen obstáculos para establecer responsabilidades penales. Visto desde la otra perspectiva estas son garantías, porque el derecho penal en última estancia supone intromisión en la esfera del ciudadano, y al delincuente se le debe respetar y reconocer su libertad en tanto sigue siendo ciudadano.

Si nos acercamos al planteamiento de las obligaciones en materia de seguridad, la primera forma de incumplir una obligación, se podría pensar que es saber que se va a cometer un delito (ciberdelito) y no impedirlo. Sin embargo, el delito de omisión pura planteado realizado dolosamente está completamente descartado. La obligación penal de impedir delitos sin riesgo propio, sin riesgo de terceras personas, solamente surge cuando el delito que se va a cometer es un delito contra la vida, contra la salud o la integridad física, un delito contra la libertad o un delito contra la libertad sexual. Los delitos informáticos o ciberdelitos no están conectados o relacionados con estos bienes jurídicos, solo el de pornografía infantil podría estar conectado con la libertad sexual. Luego, no existe obligación de impedir delitos relacionados con el ámbito de la ciberdelincuencia.

Refiere la Prof. Trapero Barreales que, en el ámbito de la empresa, podemos exigir responsabilidad penal a la propia persona jurídica que sabe que se está cometiendo o se va a cometer un delito de los relacionados con la ciberdelincuencia (conducta dolosa para que no haya ningún problema de imputación y de atribución de responsabilidad penal). Un sector de la doctrina considera que la responsabilidad de las personas jurídicas no es una auténtica responsabilidad penal o tiene otra naturaleza jurídica, sin embargo, el Código Penal español desde el año 2010 (modificado y ampliado en el año 2015), señala un número cerrado de delitos que puede cometer la persona jurídica, entre ellos están los mas importantes y representativos en materia de ciberdelincuencia. Advierte la ponente que lo cierto es que para atribuir responsabilidad penal a la persona jurídica se requiere la intervención de una persona física.

Y para ello, hay dos vías de imputación o atribución de responsabilidad, una de ellas sería por parte de los representantes legales de la persona jurídica u otras personas asimilables a los representantes legales, quienes tienen capacidad para tomar decisiones en nombre de esa persona jurídica, así como la capacidad o la función organizativa y de control. Estas personas tendrían que actuar en nombre de la persona jurídica y en su beneficio directo o indirecto.

La segunda vía de imputación, es cuando un subordinado de estos representantes, o personas asimiladas a los representantes legales, actuando en el ejercicio de su propia actividad empresarial, su propia actividad laboral o social, dice la ley, en nombre de

la empresa, en beneficio directo o indirecto de esta, comete el delito, y lo hace, porque estas personas que están en la cúspide de los que depende este sujeto no han cumplido con sus obligaciones de supervisión y control. Aquí tenemos incumplimiento con imprudencia grave, la conducta de supervisión es imprudente, pero el delito se va a imputar a título de dolo, tenemos un incumplimiento de obligaciones de vigilancia, control, por parte de una persona que tiene esas competencias dentro de la empresa.

Refiere la Prof. Trapero Barreales que no va a ser habitual que se establezca responsabilidad penal a las personas jurídicas, debido a que desde el año 2015, tenemos previsto en el Código Penal una causa de exoneración de la responsabilidad penal de la persona jurídica, esto es, el programa de cumplimiento y su aplicación. Dentro de ese programa de cumplimiento se tendrá que incluir medidas de prevención en materia de ciberdelitos, ya que es una de las modalidades delictivas que puede cometer la persona jurídica. Delitos que no son solo son blanqueo de capitales y tráfico de drogas que son los casos más habituales, sino también existen delitos de daños informáticos, acceso a datos reservados, delitos de odio, delitos de pornografía infantil hasta financiación del terrorismo, entre otros.

Fuera del ámbito de la responsabilidad penal de las personas jurídicas, es de interés la responsabilidad penal de las personas físicas, de los empresarios o de otras personas dentro de la estructura empresarial. Las características de la empresa, ya sea que tenga una estructura compleja o no, son importantes para establecer las posibles responsabilidades penales. En el ámbito de una estructura empresarial más o menos desarrollada, puede existir un departamento dedicado a la ciberseguridad o una persona con la función de adoptar las medidas elementales, que no son obligaciones legales, pero permiten la subsistencia de la empresa.

En la responsabilidad penal de personas físicas nos podemos encontrar muy rara vez con la situación de los delitos especiales, que requieren que su autor reúna una determinada condición, y precisamente esa condición o cualidad recae en la propia empresa, en la persona jurídica, pero no es la personas jurídica la que comete el delito, porque ese trabajador o ese administrador de la empresa no lo hace en su representación ni en beneficio de la persona jurídica, luego el administrador no podría ser responsable de ese delito. En materia de ciberdelincuencia hay pocos delitos especiales, algunos relacionados con la propiedad intelectual, delitos que se comenten a través de los prestadores de servicios de la comunicación o de servicios de información y en materia de descubrimiento y revelación de secretos. En los delitos especiales para poder atribuir o imputar responsabilidad penal, existe el problema de establecer el autor y el autor en este caso directamente tendría que ser la propia persona jurídica.

Respecto a los delitos comunes, se puede dar el caso del ciberdelito cometido dentro de la empresa, por una persona que pertenece a la propia estructura empresarial o una tercera persona (ataque externo) y ese delito se comete atacando o vulnerando exclusivamente bienes jurídicos que pertenecen a la propia empresa o empresario. Lo que ha sucedido es que los responsables de la gestión y administración de la empresa no han adoptado las medidas básicas, elementales para una protección mínima del negocio, por ejemplo, tiene ordenadores de acceso abierto, sin claves de acceso a la

documentación de los ordenadores, los programas de los ordenadores no se encuentran actualizados o no tiene antivirus. Lo cual genera que la empresa se exponga a cualquier ataque, constituyéndose un delito de daños informáticos que afecta exclusivamente a esta.

En este caso la empresa tiene la condición de sujeto pasivo, es la víctima del delito, pero, cuando la víctima se pone a sí misma en peligro y no adopta las más elementales medidas de seguridad, de prevención de riesgos, puede generar que se excluya la responsabilidad por falta de tipicidad, se planteen problemas de imputación objetiva y se analice el fin de protección de la norma, por lo que se puede concluir que el delito de daños no protege a este sujeto pasivo que se ha puesto a sí mismo en peligro. Sin embargo, añade la ponente, que la existencia de distintos niveles de conocimiento de los ciudadanos en cuanto al tema digital, hace que se presente una situación de desconocimiento absoluto de la situación de peligro, y por tanto no se pueden adoptar medidas de prevención, control y contención de ese peligro, circunstancia que se debe valorar a la hora de establecer, analizar o no la imputación objetiva.

Continúa la ponente exponiendo otros supuestos, por ejemplo, en el que, dentro de la empresa, uno de sus empleados lleva a cabo la conducta delictiva (ciberdelito), pero además de afectar derechos o bienes jurídicos de la empresa, afecta a terceros, que pueden ser los clientes de la empresa o los ciudadanos en general. Ese empleado ha cometido ese delito entre otras cosas favorecido o apoyado en que la empresa no había aplicado medidas de seguridad para controlar o minimizar el riesgo de ese ciberdelito o en todo caso son insuficientes. Al trabajador o a el empleado de la empresa externo obviamente le vamos a imputar ese delito porque lo ha cometido dolosamente. Sin embargo, podemos imputar también responsabilidad penal al superior jerárquico si es un empleado que tenía la obligación de controlar, vigilar y supervisar la actividad de su subordinado, o en todo caso, al responsable máximo de la empresa porque al fin de cuenta tiene obligaciones de vigilar y controlar la actividad empresarial que se desarrolla. Para atribuir o imputar responsabilidad penal a estas personas que no han adoptado las medidas preventivas, tenemos que entrar en el terreno de la comisión por omisión.

La comisión por omisión se puede basar en este caso en que el responsable del departamento que no ha adoptado esas medidas preventivas o en última instancia el empresario, tiene una posición de garante de bienes jurídicos, y esa posición de garante se deriva de dos vías, por un lado, tiene posición de garante y por tanto está obligado a evitar que se produzca ese daño, esa lesión al bien jurídico. La segunda vertiente de donde podemos derivar la posición de garante es la función de control de fuentes de peligro que están en su ámbito de dominio y la actividad empresarial es una fuente de peligro. Por eso, el desarrollo de la actividad empresarial, implica riesgos para bienes de terceras personas, clientes u otros ciudadanos. Entonces, el máximo responsable o los responsables intermedios tienen que controlar ese peligro, esto genera problemas, pues tendremos que decidir de qué manera se interviene en ese delito, si es una posición de garante tendríamos que calificar su intervención como autor. Habrá casos en los que efectivamente es el autor, pero en otras ocasiones estará participando en el delito, en la comisión por omisión el principal problema con el que nos encontramos es el debate de si se castiga la comisión por omisión a título de participación. Si es a título de autor se

podría investigar con la misma pena que el propio ejecutor material con conducta activa, si es como participación tendríamos que valorar si es una participación en calidad de cooperación necesaria o en calidad de cómplice.

La parte objetiva la podríamos construir a través de la comisión por omisión, pero nos encontramos con el obstáculo de la parte subjetiva, principio de responsabilidad objetiva, generalmente esa persona que no adopta esas medidas de prevención que no controla esos focos de peligro, que no cumple la función de protección del bien jurídico, no lo hace dolosamente, a lo sumo podríamos decir que su actuación (omisión) es imprudente, y ello genera un problema: los ciberdelitos están tipificados en su forma dolosa, no en su forma imprudente, si además es una participación imprudente en un delito doloso cometido por un tercero, pero la participación es imprudente en comisión por omisión, no se podría castigar, además teniendo en cuenta que si no se castiga la autoría imprudente, menos se va a castigar la participación imprudente.

Solamente podría recurrir a un delito para castigar la autoría en comisión por omisión imprudente y es el delito de daños informáticos, porque ese tiene que ser doloso, podría recurrir al genérico delito de daños que pide imprudencia grave y que pide que cause un daño superior a 80.000 euro, si se reúnen esas dos condiciones podré castigar a ese responsable de la empresa o al propio empresario por no cumplir con las obligaciones derivadas de esas funciones de protección del bien jurídico o esa función de control de fuente de peligro habrá facilitado o habrá realizado el mismo el daño al bien jurídico.

Comentarios de la relatora

El planteamiento de la Prof. Trapero Barreales nos ofrece una visión muy importante en cuanto a la utilización de las TIC y sus riesgos para el normal funcionamiento de las entidades y organismos públicos y privados. En este contexto es en el que se produce la ciberdelincuencia o criminalidad informática[1], fenómeno que golpea de manera intensa el mundo empresarial, financiero y económico. En palabras de Romeo Casabona y de Miguel Beriain, se está abriendo un nuevo campo a la delincuencia patrimonial y socioeconómica, siendo estas modalidades las principales: a) manipulaciones de datos y/o programas, o 'fraude informático'; b) copia ilegal de programas, 'piratería informática'; c) obtención y utilización ilícita de datos, o 'espionaje informático' (industrial, de mercado o financiero), entre otros[2]. La cuestión dogmática expuesta por la Prof. Trapero Barreales pone de presente la variada manifestación

[1] Tejada de la Fuente, Elvira. Novedades en la tipificación de determinados delitos vinculados a la criminalidad informática en el Código Penal Español: evolución legislativa y adaptación a la normativa internacional. E: Daniela Dupuy (Dir.), Cibercrimen. Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet, editorial B de F, Buenos Aires, 2016, pag.33.

[2] Ver: Romeo Casabona, Carlos María y de Miguel Beriain, Íñigo. El cibercrimen en el ámbito económico y patrimonial. Universidad del País Vasco. Disponible en: https://ocw.ehu.eus/pluginfile.php/2612/mod_resource/content/1/OCW-CiberEmpresa_Tema01_v2.pdfmhttps://ocw.ehu.eus/pluginfile.php/2612/mod_resource/content/1/OCW-CiberEmpresa_Tema01_v2.pd

delictiva y la actual respuesta del derecho penal conforme al difícil establecimiento de responsabilidad penal para la empresa (persona jurídica) o para el administrador (persona física), exponiendo los problemas dogmáticos y la clara necesidad de mantener ante todo firmes los principios y garantías del derecho penal, que protege los derechos del delincuente como ciudadano. Finalmente, considero que el desafío que presenta la utilización de las TIC obliga a un replanteamiento de categorías dogmáticas clásicas, que abarquen los fenómenos modernos en el ámbito de la ciberdelincuencia. Dicho replanteamiento requiere de construcciones jurídicas creativas y adecuadas, pero que ante todo sólidas, creíbles y estables, que permitan hacer frente a las demandas de nuevas modalidades criminales.

TERCERA PONENCIA: **«Los intermediarios en la era de la desinformación: *fake news*, redes sociales y medios de comunicación»**
Ponente: **D. Diego Fernández López**, CEO de InfoBierzo.com, HoyCastillayLeon.com y Birttu.com.
Moderador: **Prof. Dr. D. Salvador Tarodo Soria**, Profesor Titular de Derecho Eclesiástico del Estado de la Universidad de León
Relator: **D. Juan Pablo Uribe Barrera**, Personal Investigador en Formación de la Universidad de León (Área de Derecho Penal y Departamento de Derecho Público)

El moderador, Profesor Tarodo Soria, abre el debate y, tras una breve presentación del ponente, le otorga el uso de la palabra. El ponente empieza su intervención situando a las *fake news* como un fenómeno de naturaleza global que es propio del contexto social actual. Para señalar los rasgos que más interesan de este contexto, manifiesta el ponente que basta con recordar que nos encontramos en una sociedad que comúnmente es denominada como *sociedad digital* y/o *sociedad de la información*. Estas etiquetas apuntan muy claramente hacia un hecho: estamos en el momento de la historia humana en que mayor flujo informativo ha existido. Ante las sociedades, para decirlo con otras palabras, que le han podido dar las mejores condiciones a sus miembros para poder acceder a información.

Esta facilidad, tanto para producir como para distribuir información, hace que se llegue incluso a puntos de saturación. Así, es tal la cantidad de información a la que cualquier miembro de estas sociedades se ve expuesto, que es fácil que se vea avasallado. Que sienta que, ante la magnitud del constante flujo informativo, no tiene el tiempo suficiente como para poder reflexionar, para establecer los criterios que le permitan identificar si está ante datos, reseñas, noticias o testimonios que merecen su confianza. Esta saturación, avasallamiento y ausencia de un espacio de reflexión nos dan la pista definitiva de cómo se administra generalmente la información en estas sociedades: lo cuantitativo tiene prelación, y en cierto sentido fija, lo cualitativo.

A la luz de este marco, señala Fernández López, es que podemos entender como un asunto mucho más antiguo, como lo es el de las *fake news*, puede convertirse hoy en un problema para la sociedad, en un problema de *ciberseguridad*. El valor que tiene la información en nuestra sociedad, y las mencionadas condiciones que derivan hacia

la ausencia de reflexión del receptor de mensajes, le otorgan un nuevo matiz y una nueva dimensión a este asunto.

Aprovechando esta introducción, el ponente invita a pensar en la fase de distribución de las *fake news*, antes incluso que en su producción y las razones detrás de esta. Diversos estudios han demostrado que, para su distribución, estas informaciones no encontraron nunca un mejor mensajero y reproductor que el usuario de redes sociales que, en las condiciones de saturación y falta de reflexión expuesta, comparte contenidos sin verificar su credibilidad. Sí las *fake news* tienen hoy la dimensión que tienen, nos dice una y otra vez Fernández López, es porque nosotros, como receptores y emisores de información, no estamos pudiendo o queriendo hacer la tarea que nos correspondería. No estamos consiguiendo ser un filtro eficaz.

Concentrándose puntualmente en el tema de la distribución, el ponente ubicó, a través de imágenes y ejemplos, algunas cuestiones adicionales que pueden llegar a ser muy útiles para comprender este fenómeno. De especial interés fue su comentario respecto al papel que cumplen los informadores y los personajes públicos que gozan de buena credibilidad entre los miembros de una determinada comunidad. Estos tendrían, por así decirlo, una especial responsabilidad. Cuando ellos dan fe de una noticia, otras personas lo hacen, lo que hace que, de un lado, se le otorgue un halo de credibilidad a una noticia que en realidad es falsa, y del otro, se magnifique y se expanda generando respuestas y reacciones en cadena frente a acontecimientos inexistentes.

Cambiando ahora el eje del asunto, enfocándose no ya en la distribución sino en la producción de las *fake news*, el ponente avanzó sobre otras cuestiones sumamente interesantes. En primer lugar, con diversos ejemplos enseñó que, aunque se trata de un asunto global, no debe perderse nunca de vista el hecho de que este fenómeno ocurre en ámbitos más próximos y cotidianos de lo que podríamos pensar. En segundo, a través de una interesante tipología que fue presentando junto a diversos ejemplos, enseñó hasta cuatro modalidades distintas de *fake news*, mismas que pueden ser singularizada atendiendo a la intención de quienes la producen.

El primer tipo de *fake news* es el que se realiza con fines eminentemente comerciales. Con un ejemplo tomado de un reporte sobre las diferentes actividades realizadas en festivales, se mostró como en realidad lo que se pretende en muchas noticias no es informar sobre acontecimientos relevantes, sino atraer al público con información poco valiosa sobre materias que pueden resultar de su interés para, una vez que se ha captado su atención, poder ofrecerle, de manera subrepticia, determinado producto.

El segundo, quizá con el que estamos más familiarizados, es el que se realiza como una broma o como un ataque más o menos ofensivo a cierto(s) personaje(s). Con un ejemplo de una noticia falsa según la cual una mujer se había implantado un tercer seno, Fernández López ilustró muy bien el punto de que, entre los diferentes tipos de *fake news*, este puede ser es en principio el tipo menos ofensivo, especialmente cuando se trata de bromas que no tienen mayores consecuencias.

El tercero, del que haremos un mayor comentario en la conclusión de esta breve reseña, consiste en la *fake news* periodística, que es la que realiza cierto medio de

comunicación para llamar la atención de más segmentos del público y mejorar sus estadísticas con fines económicos. El uso de imágenes falsas, el reporte de situaciones completamente imaginarias o exageradas hasta el punto de ser ya abiertamente falsas caracteriza este tipo de noticia falsa.

Finalmente, el cuarto y último es el que, en opinión del ponente, puede resultar más peligroso y alarmante. Este consiste básicamente en las *fake news* realizadas con el objetivo de manipular ideológicamente al público. Haciendo un paralelo con el universo distópico orwelliano, Fernández López mostró como Rusia utilizaba las *fake news* a gran escala para crear opinión a su favor y en contra de sus rivales políticos como los Estados Unidos de América. Producir debates en foros en que el "ganador" siempre es el que sostiene la posición rusa, inventar fuentes, crear "medios de comunicación" para luego citarlos como fuente en otros "medios de comunicación" y así dar mayor impresión de rigurosidad, son tan solo algunas de las estrategias citadas con estos fines.

Comentarios del relator

Para finalizar esta breve reseña con un comentario a título personal, me gustaría volver a centrar la atención en el tema de las *fake news* y el periodismo, pues es especialmente atractiva la reflexión a la que invita la ponencia en este punto. Si pudiéramos seguir con esa caracterización general que hacía el ponente de nuestras sociedades, agregaríamos que estas también se caracterizan por haber generado el eclipse de las grandes verdades. En lugar de grandes dogmas, parece que somos más una sociedad de múltiples narrativas y relatos. De verdades relativas, parciales, interpretables, opinables. En este contexto, en donde todo parece opinable, en donde la palabra verdad se escribe con minúscula, cuando le pedimos a un periodista que no produzca noticias falsas: ¿Le estamos diciendo que produzca noticias verdaderas? ¿Qué es una "noticia verdadera"? ¿Qué pasa si dos periodistas producen "noticias verdaderas" opuestas? ¿Alguna de ellas es necesariamente una *fake news*? En el marco de estas preguntas, cuya respuesta estaría muchísimo más allá de los intereses de este texto, vale la pena simplemente apuntar a que la esencia de la *fake news* no está dada por su falsedad, de allí que su contrario no sea la noticia "verdadera", sino por su falsedad *deliberada*, por el ánimo de engañar o mentir, de allí que su contrario sea el periodismo que, más allá de que pueda producir o no verdades en el sentido más duro del término, sea hecho con honestidad.

CUARTA PONENCIA: **«Seguridad de la información y menores. Una visión judicial del uso de las nuevas tecnologías en los procedimientos civiles»**
Ponente: **D. José Enrique García Presa**, Ilmo. Sr. Magistrado-Juez de los Juzgados de León
Moderador: **Prof.ª Dra. Dña. Marta Ordás Alonso**, Profesora Titular (acr. Catedrática) de Derecho Civil de la Universidad de León
Relatora: **Dña. Gracia Fernández Caballero**, Abogada, doctoranda de la Universidad de León, Colaboradora Honorífica del área de Derecho Procesal de la Universidad de León

La quinta ponencia de las Jornadas de Derecho y Ciberseguridad corrió a cargo del Ilmo. Sr. Magistrado-Juez D. José Enrique García Presa, que comenzó su exposición agradeciendo la invitación a participar en las mismas y anunciando que desglosaría su intervención en dos partes claramente diferenciadas, comenzando por «el uso de las nuevas tecnologías en los procedimientos civiles, referido en concreto a la introducción la prueba tecnológica en el proceso judicial» y, en segundo lugar, ahondando en «la seguridad de la información y los menores».

El Magistrado comienza reflexionando sobre que, en unas jornadas de carácter multidisciplinar como estas, que abarcan tanto el Derecho como la ciberseguridad, no podía faltar una ponencia sobre la manera en que las nuevas tecnologías están presentes en el ámbito judicial, cómo pueden introducirse las nuevas tecnologías en los procedimientos judiciales y, en concreto, en materia probatoria.

A modo de introducción, el ponente parte de unos datos generales sobre la implantación de la administración electrónica, destacando que en España se está haciendo un gran esfuerzo en su desarrollo, señalando que el informe bienal sobre Administración electrónica de las Naciones Unidas ha situado a España en los primeros puestos en el ranking mundial, con datos como que más de 24 millones de españoles disponen de DNI electrónico, y el 90% de los trámites con la AGE pueden realizarse ya de forma electrónica. Todo ello ha sido posible gracias al marco jurídico de que se ha dotado la administración pública, partiendo de la puesta en marcha de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

Ciñéndose al ámbito de la justicia, señala el Magistrado que los ciudadanos tienen como derecho fundamental acceder a la tutela judicial efectiva por los tribunales; para lo que es necesario dotar a los ciudadanos de la posibilidad de acreditar sus pretensiones. En este sentido, hoy en día, con el imparable avance de las nuevas tecnologías, uno de los medios probatorios que los ciudadanos pueden emplear para acreditar el derecho que les asiste ante a los tribunales es la prueba electrónica o digital. Para que los ciudadanos puedan hacer uso de esos nuevos medios probatorios, alude el Magistrado a que es necesaria la modernización de la administración de Justicia y, en dicho contexto, uno de los elementos de mayor relevancia es la incorporación a las oficinas judiciales de las nuevas tecnologías.

El CGPJ es quien tiene la responsabilidad de dotar a los jueces y tribunales de los medios tecnológicos necesarios para atender las necesidades de los administrados y de todos los operadores jurídicos que intervienen en la vida diaria de los Juzgados y Tribunales. El CGPJ lidera iniciativas para facilitar la integración e interoperabilidad entre los diferentes sistemas de gestión procesal, y entre éstos y otros sistemas de información relacionados con el funcionamiento de la administración de justicia a través del ya conocido "punto neutro judicial" que, en materia de prueba, ofrece una información sumamente valiosa y, sobre todo, en cuanto a contenidos de naturaleza económica.

El Magistrado, entrando de lleno en la materia en cuestión objeto de la ponencia, reflexiona sobre que resulta una verdad indiscutible que nos encontramos ante una sociedad digital que presenta una dimensión específica en el ejercicio de la función

jurisdiccional, y de manera fundamental en lo que se refiere a la proposición y práctica de la prueba en el proceso civil, que puede además resultar decisiva. Razona García Presa que, en esta materia, la normativa va muy por detrás de la realidad. Lo cierto es que la regulación legal no camina al mismo ritmo que la vertiginosa evolución en materia de nuevas tecnologías. Partiendo de que la CE recoge en el art. 24.2 el derecho a utilizar los medios de prueba pertinentes para la defensa de las pretensiones, que se manifiesta en el derecho a proponer la prueba que estimemos oportuna y a practicarla en caso de que sea admitida; lo cierto es que en la actualidad, las comunicaciones habituales a través de las redes sociales, correo electrónico, teléfono móvil, etc. ocasionan diariamente numerosos conflictos probatorios que están dando lugar a una jurisprudencia no del todo uniforme.

En cuanto a las fuentes de prueba electrónica en el procedimiento civil, centra el ponente que nos referimos a los correos electrónicos, pantallazos, mensajes de texto, WhatsApp, o cualquier otro sistema de mensajería instantánea, páginas web, etc., para los que rigen igualmente los principios generales de la prueba de conformidad con el art. 326 LEC.

Señala el ponente que, en todo caso, existe otra cuestión conceptual necesaria para entender este tema, y es la diferencia entre medio y fuente de prueba. Fuente de prueba es un concepto extrajurídico, puede ser una persona o una cosa que está fuera del procedimiento, es una realidad anterior, exterior e independiente al proceso; frente al medio de prueba, que es la actividad concreta a desarrollar ante el juzgador, siendo un concepto jurídico-procesal que existe "en y para" el proceso. Como ejemplo, entre otros, señala el Magistrado que, en una prueba documental, la fuente de prueba será el documento, y el medio de prueba será la aportación de ese documento a las actuaciones del procedimiento. Los medios de prueba aparecen regulados en el art. 299 LEC, que en su apartado 2 ya hace referencia a cómo las nuevas tecnologías se prevén como medio probatorio en el procedimiento civil, así como en su apartado 3 se alude en todo caso a "cualquier otro medio no expresamente previsto". Se permite así la aportación al procedimiento de medios de prueba diferentes a los no expresamente previstos, en los que podremos incluir aquellos que con el avance de la tecnología no aparezcan expresamente previstos.

Igualmente, en su introducción, alude el Magistrado a la definición clásica de prueba, señalando que es la actividad procesal con la que las partes intentan acreditar sus pretensiones, convenciendo al juzgador sobre la veracidad de los hechos que alegan. Continúa señalando las características de la prueba civil, que se pueden establecer como, en primer lugar, la unidad de su regulación en la LEC; en segundo lugar, la necesidad de la prueba, en cuanto a que una prueba debe ser necesaria y pertinente, esto es, tener relación con la tutela judicial que se pretende obtener en el procedimiento, de este modo, aquella prueba que no se considere necesaria podrá ser rechazada por el juzgador como señala el 283 LEC; como tercera característica de la prueba, la misma deberá ser practicada en unidad de acto aunque, señala el Magistrado, existen algunas excepciones en la propia LEC para aquellas que no puedan practicarse en el acto del juicio y deban llevarse a cabo en un momento posterior, con la salvedad de la prueba de reconocimiento judicial, que debe practicarse con carácter anticipado al acto del juicio o de la vista. Como cuarta

característica señala la inmediación, que se traduce en que la prueba como norma general debe ser practicada ante el Juez, por ejemplo, interrogatorios de parte, testificales, periciales; a salvo de algunas actuaciones en materia probatoria que pueden ser realizadas en presencia del Letrado de la Administración de Justicia, como puede ser el reconocimiento de documentos privados. En quinto lugar, la prueba debe estar sometida a los principios de contradicción y publicidad, las pruebas deben verificarse siempre en presencia de la contraparte y se practicarán en vista pública; y, como característica y garantía final de la prueba se encuentra su documentación, es decir, actas del LAJ y grabación en soporte electrónico, lo que en ocasiones también provoca problemas derivados de fallos en estos soportes electrónicos que pueden conllevar incluso nulidades de actuaciones.

Sentado el concepto y características generales de la prueba civil, señala el ponente que pasa a referirse ahora, en concreto, la prueba electrónica. Para aproximarse al concepto de prueba electrónica, apunta el Magistrado que debemos de tener clara la definición de lo que es el documento electrónico y, una vez tengamos esto claro, hay que determinar cómo se incorpora al procedimiento civil como medio de prueba. De este modo, el art. 3.5 de la Ley 59 /2003 de firma electrónica, define el documento electrónico como "[…] la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado", y en su art. 8 establece que "[…] el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio". Determina finalmente el Magistrado que puede definirse la prueba electrónica como toda aquella información con valor probatorio que se encuentre incluida en un medio electrónico, o es transmitida por dicho medio. Concluyendo que existen pues dos modalidades de prueba electrónica, por un lado, los datos almacenados en sistemas o aparatos informáticos y, por otro, la información transmitida electrónicamente a través de las redes de comunicación. Apunta el ponente que, si bien su concepto aparece en la Ley 59/2003, lo cierto es que no existe en nuestro ordenamiento una regulación unitaria de la prueba electrónica lo que, puntualiza, no significa que no esté prevista en la normativa vigente, sino que aparece diseminada en distintos cuerpos legales. Ciñéndose al procedimiento civil, señala el Magistrado el art. 230 de la LOPJ y los arts. 382 y 384 de la LEC.

Se llega así a la aportación y práctica de la prueba electrónica en el proceso civil. De este modo, la primera cuestión es analizar las fases de la prueba electrónica, para lo que el ponente aclara que ha seguido un trabajo del Magistrado Joaquín Delgado Martín ; siendo la primera fase la obtención de la información, para lo que las partes han de acceder a la información siempre de forma lícita, es decir, sin vulneración de ningún derecho fundamental; la segunda fase será la incorporación de los datos al procedimiento, para ello debe de cumplir los requisitos generales de la prueba, a los que ya se ha aludido; y, la tercera fase es la valoración de los datos incorporados, que es la valoración de esa prueba por parte del juez o tribunal.

Para acceder a proceso, la prueba electrónica deberá pasar lo que se ha denominado "test de la admisibilidad de la prueba digital", que se basa en tres parámetros: en primer lugar, la integridad, que se traduce en que el soporte en que figura la prueba que pretende introducirse en el procedimiento no haya sido alterado de modo alguno;

en segundo lugar, la autenticidad, es decir, es necesario que se constate la realidad del contenido que figura y que, además, ese contenido pertenezca al sujeto del que se dice que ha emanado dicha declaración; y, finalmente, la licitud, a la que ya se ha aludido al anteriormente, pero que se manifiesta expresamente en este test de admisibilidad. En cuanto a la valoración de la prueba electrónica, alude el Magistrado a los métodos tradicionales para valoración de la prueba en general: la prueba legalmente tasada y la libre valoración de la prueba, que se refiere a que la prueba debe ser valorada conforme a la libertad de valoración, la sana crítica, que corresponde al juzgador.

Continúa el ponente analizando la postura procesal de los pates cuando se pretende introducir un medio de prueba electrónico en el procedimiento, puesto que una parte puede aportar la prueba electrónica y la contraparte tiene el derecho a impugnarla. Por ejemplo, en cuanto a los pantallazos de conversaciones en redes sociales, que en realidad se consideran mera prueba documental, la parte contraria puede impugnarlos alegando que la información que se refleja ha sido alterada, o que son incompletos, o bien que la información contenida no ha sido emitida por quien se dice. En tales casos se hace necesario por la parte que lo aporta acreditar la veracidad de dicho medio probatorio, y que se lleva a cabo generalmente mediante una prueba pericial informática. Señala el ponente que la forma principal de aportación de la prueba electrónica suele ser la aportación de su impresión en papel y, para que esté correctamente aportada, deben adjuntarse los datos electrónicos que se correspondan a esa impresión en soporte digital, en un cd que permita comprobar la veracidad e integridad de los datos aportados. Para finalizar la primera parte, el Magistrado hace referencia a la STS de 19 de mayo de 2015 sobre la fuerza probatoria de los pantallazos de conversaciones a través de redes sociales, que textualmente establece que "la prueba de una comunicación mediante sistemas de mensajería instantánea debe ser abordada con todas las cautelas, debido a que la posibilidad de una manipulación forma parte de la realidad de las cosas", afirmando el Alto Tribunal que "el anonimato que utilizan estos sistemas y la libre creación de cuentas hacen posible aparentar una comunicación en la que un único usuario puede llegar hasta a estar relacionándose incluso consigo mismo", considerando indispensable realizar una prueba pericial sobre los documentos que se aporten para acreditar el verdadero origen de la comunicación y la identidad real de los interlocutores y la integridad de sus contenidos. Estableciendo el TS de este modo, los criterios que deben emplearse para admitir los mensajes a través de redes sociales como prueba, dada la alta facilidad para su manipulación.

Pasa ahora el ponente a tratar la segunda parte de su intervención, dedicada a la seguridad de la información y los menores. Reflexiona el Magistrado sobre el cambio en la forma de las comunicaciones en la actualidad pues, a diferencia de cómo nos comunicábamos antes, ya no hablamos por teléfono, cada vez conversamos menos cara a cara, y hoy en día chateamos, whatsappeamos, tweeteamos, etc.; señalando además que estos nuevos medios de comunicación no sirven solo para comunicaciones personales, sino que también se realizan a través de los mismos comunicaciones comerciales, celebración de contratos e, incluso, se cometen delitos. Además, todas estas comunicaciones, e incluso las grabaciones de vídeo y fotografías, actualmente se concentran en un único terminal: el móvil y la tablet, que se han convertido en el regalo estrella de cumpleaños, Navidades, comuniones, etc., sin que

las familias sean realmente conscientes de los riesgos que puede tener para un menor disponer de los mismos.

Alude el Magistrado a que el 30 de noviembre de 1988 fue declarado el día mundial de la seguridad de la información y, desde entonces, se celebra con el objeto de concienciar sobre la importancia de esta seguridad y de los sistemas y entornos que operan sobre ella, intentando transmitir y consolidar hábitos de seguridad informática desde los niveles más básicos hasta los más avanzados. Señalando que uno de los públicos más expuestos son los menores, que desde edades muy tempranas ya se relacionan a través de las redes sociales. El desmesurado uso de los dispositivos ya referidos, sumado a una conexión permanente a internet, tiene una gran repercusión en nuestros hábitos y conductas, además de suponer un riesgo para la intimidad y seguridad personal, que resulta más preocupante en el caso de los menores, ya que por su edad aún no tienen formada su personalidad, son inmaduros intelectualmente y eso en muchos casos no les permite percibir a los riesgos que se enfrentan cuando navegan. Señala el ponente algunos datos estadísticos al respecto, como que el 95% de los menores en España son usuarios habituales de internet, y solo el 46% de estos menores posee conocimientos en cuanto a configuración de la privacidad de sus terminales y perfiles en redes sociales; señalando otras estadísticas, como un estudio reciente realizado por el Principado de Asturias, entre usuarios con edades entre los 10 y los 18 años, que revela que el 95 % disponían de teléfono propio, y el 71 % afirmó que la familia nunca les supervisaba su uso; datos que claramente resultan preocupantes y alarmantes, apuntando el Magistrado que estas estadísticas revelan un uso exagerado del teléfono móvil por los menores, y a edades tempranas.

Siguiendo con su exposición, reflexiona el ponente sobre el derecho a la libertad, que se configura ya como elemental en la Declaración Universal de los Derechos Humanos, y asimismo lo recoge como fundamental nuestra CE en su art. 17. La tecnología ofrece indudables ventajas y oportunidades para la formación, pero también puede limitar el derecho a la libertad que, en una sociedad cada vez más digitalizada, parece que empieza a atenuarse.

En el ámbito de los menores, el marco legal puede concretarse en la Declaración de los Derechos del Niño de la ONU, la Ley Orgánica 1/1996, de Protección Jurídica del Menor y la Ley Orgánica 8/2015 de modificación del sistema de protección de la infancia y la adolescencia, entre otras normas. En el caso de los menores, la digitalización de la vida y la afectación al derecho a la libertad resulta especialmente relevante porque se trata de un colectivo vulnerable debido precisamente a su falta de madurez. Reflexiona el Magistrado, aludiendo a Tristan Harris, sobre como las alertas del móvil dicen al cerebro en qué fijar la atención en cada momento, programándose la mente con dichas alertas, suponiendo una sutil restricción de la libertad que además crea adicción a los dispositivos. La libertad se ve asimismo afectada por la hiperconexión a la red, que para los menores es aún más grave dada su vulnerabilidad, y el control por parte de los padres se ve cada vez más comprometido debido a la brecha digital que existe entre generaciones. Además, no puede olvidarse que los menores también tienen derecho a la intimidad y privacidad, que debe conjugarse con el deber de protección de los progenitores. Sin olvidarse de que la hiperexposición de los menores en las redes sociales, no se da siempre por parte de los propios menores,

sino incluso por parte de los padres que muestran la vida de sus hijos e incluso algunos la rentabilizan. Además de los riesgos que conlleva la utilización de internet y redes sociales en cuanto a la obtención de datos de las familias y menores, que luego se emplean para crear perfiles utilizados con fines comerciales.

Si bien continúa el ponente reflexionando sobre la problemática que genera esta realidad digital en la que vivimos, señala que, a pesar de la crítica realizada, tampoco puede suponer impedir que los menores renuncien a las ventajas que por otro lado les ofrece internet. Jurídicamente la patria potestad obliga los padres a velar por los derechos de sus hijos y, en el ámbito del Juzgado de Familia, en el que el ponente desarrolla sus funciones, si bien no existen abundantes procedimientos en los que se discuta sobre el empleo de las redes sociales y los menores, sí ejemplifica el ponente un caso en el que el que un progenitor presentó un solicitud al juzgado para que el otro progenitor retirara unas fotografías del hijo común de ambos de Facebook, y que, en lo sucesivo, se solicitara autorización judicial para que el menor y su imagen pudieran acceder a redes sociales. Reflexiona el ponente que, obviamente, este tipo de peticiones no se dan en el marco de una pareja con una convivencia normalizada, si no en una pareja en la que existe una mala relación. Señalando el Magistrado que debió de atenderse a la petición, y exigir al progenitor que había colgado las fotografías en la red que las retirara, pues se entendió que es una cuestión que afecta a la patria potestad y, por tanto, deben estar ambos progenitores de acuerdo, debiendo solicitar en adelante autorización del otro progenitor para esta clase de cuestiones.

Concreta el ponente los riesgos a los que se enfrentan los menores con el uso de la red en tres grandes grupos: el ciberacoso, la pérdida de privacidad y el acceso a contenido inapropiado. Dentro del ciberacoso se encuentra el cyberbullying, la suplantación de identidad, el sexting y el grooming. El cyberbullying lo resume el ponente como el ciberacoso escolar, realizado por compañeros de clase a través de diferentes redes sociales; la suplantación de identidad consiste en hacerse pasar por otra persona con la intención de controlar o afectar a la víctima; el sexting es la distribución de contenido erótico o sexual sin consentimiento de la víctima, que a veces es incluso empleado para extorsionar a la víctima; y al grooming es el acoso a un menor por parte de un adulto con fines sexuales. En cuanto a la pérdida de privacidad, señala el Magistrado que puede ser voluntaria, la información que los menores suben conscientemente a la red, sin conciencia de que compartir esa información por estos medios les expone ante extraños; e involuntaria porque esa información que suben sea recabada de ellos por terceros. El acceso a contenido inadecuado se refiere a la facilidad para acceder a contenidos sexuales, xenófobos, ilegales, etc.

Además, señala el Magistrado los riesgos de navegar por parte de los menores, dada su inmadurez intelectual, apuntando como otros riesgos la existencia de "juegos" peligrosos para su salud, que han llegado incluso a causar fallecimientos, como el juego de la ballena o el abecedario del diablo, que resultan absolutamente espeluznantes, y requieren control paterno.

El Magistrado reflexiona sobre que, para prevenir estos riesgos a los que están expuestos los menores en la actualidad, resulta imprescindible que desde su entorno familiar y escolar se les eduque en el uso razonable y adecuado de las nuevas

tecnologías, implantando un control de su uso cuando sea posible, mientras sean menores de edad, sin que se trate ni de investigarles ni entrometerse en su vida, si no de realizar una labor educacional, pedagógica y de supervisión, que garantice el desarrollo de su libre personalidad y su potencial de aprendizaje.

Finaliza el ponente refiriéndose a la protección de los datos de los menores, señalando que la edad mínima para prestar consentimiento para el tratamiento de datos personales, sin el consentimiento de los progenitores, en España son los 13 años; lo que es criticado por parte de la doctrina ya que Europa marca los 16 años –si bien permitiendo rebajar la edad a los estados miembros por ley, siempre que no sea inferior a los 13– dado el reforzamiento en esta materia que se está llevando a cabo en los últimos tiempos. Si bien, existe otro sector de expertos que apoyan la medida y entienden que hay que dar un voto de confianza a los menores, para los que las nuevas tecnologías son un instrumento habitual, y las TICs juegan un papel inevitable en el desarrollo de su personalidad. Siendo imprescindible que gocen de protección de su privacidad tanto por parte del Estado, como a través de la educación, pero sin arrebatarles su autonomía.

Concluye el ponente señalando que el 20 de noviembre de 2019 cumplirá 30 años la Convención de los Derechos del Niño que es el instrumento internacional que más adhesiones ha generado en la historia, y que ha propiciado más factores en cuanto a cambio social, fundamentalmente en lo referente a los ideales de justicia e involucración de más personas en la protección de los derechos de los menores; apuntando como colofón una frase del Plan de Acción de la Cumbre Mundial a favor de la Infancia de 30 de septiembre de 1990: "no hay causa que merezca más alta prioridad que la protección y el desarrollo del niño, de quien dependen la supervivencia, la estabilidad y el progreso de todas las naciones y, de hecho, de la civilización humana".

Comentarios de la relatora

El imparable avance de la vida digital se manifiesta en diferentes facetas de nuestra vida, pero de una forma muy significativa en nuestras comunicaciones y en concreto en la manera del llevarlas a cabo. Las tradicionales cartas y llamadas telefónicas se sustituyen ahora por chats, aplicaciones de mensajería instantánea y redes sociales. Estos cambios afectan sin lugar a dudas a nuestra vida en sociedad y suponen un auténtico reto tanto a nivel de prueba en el proceso judicial, como en términos de seguridad de la información en lo que se refiere a los menores.

Con esta ponencia se pone una vez más en evidencia cómo la normativa va un paso por detrás de los avances tecnológicos y de su implantación en la vida social cotidiana, siendo necesaria una actualización de los requisitos y unificación normativa sobre los criterios para la incorporación de las comunicaciones digitales como prueba a los procedimientos judiciales, en aras de evitar que deba ser la jurisprudencia la que marque a golpe de sentencia los mismos, dotando de mayor seguridad jurídica a un aspecto fundamental del proceso judicial como es la prueba. Lo que en última instancia redunda en el derecho fundamental a la tutela judicial efectiva.

Por otro lado, se han puesto de manifiesto los riesgos que estas nuevas formas de comunicación pueden conllevar para los menores. Desde ataques a su privacidad, que

puedan incluso repercutir en su futura vida adulta, como a la comisión de delitos contra los niños a través de los medios digitales. Como ya proclama la Declaración de Derechos del Niño, la protección y desarrollo de los niños debe ser una de las prioridades de nuestra sociedad, pues de ellos depende nuestro futuro. Por lo que las medidas y mandatos de protección contenidos ya en nuestras leyes y tratados internacionales refrendados, deben cumplirse y suponer una verdadera implementación de estas en la educación, tanto institucional como familiar, de nuestros menores.

QUINTA PONENCIA: **«*Blockchain*: seguridad y derecho a la privacidad»**
Ponente: **D. Fernando Cuadrado Malasaña**, Abogado especialista en TIC
Moderador: **D. Gonzalo Collado de la Guerra**, Ilmo. Sr. Abogado del Estado
Relatora: **Dña. Lidia García Martín**, Personal Investigador en Formación de la Universidad de León (Área de Derecho Administrativo del Departamento de Derecho Público)

D. Fernando Cuadrado Malasaña inicia su ponencia anunciando el fenómeno de la blockchain y la consecuente revolución que ello ha supuesto. Como punto de partida el ponente recuerda las palabras del expositor anterior sobre el papel clave de Vinton Cerf al crear el Protocolo de Transmisión (TCP), el Protocolo de Internet (IP) y, en síntesis, el internet de los datos. Surge a tal fin el discurso inspirador de la blockchain, el internet del valor, a través de la cual se puede enviar de forma instantánea dinero y criptomonedas por medio de un canal seguro y confidencial, traspasando las fronteras internacionales. La justificación a la blockchain el ponente la sitúa en la necesidad de contar con una interfaz capaz de enviar dinero al extranjero sin necesidad de realizar transferencia bancaria alguna[3].

Acompañado de una presentación de Power Point, el ponente alude a la capacidad de la blockchain como máquina de crear confianza. Es necesario hablar del derecho a la privacidad y a la transparencia pues todas las sociedades han tenido graves problemas de confianza y ello puede solucionarse por medio de la blockchain. La confianza es el factor más importante en la revolución de las Tecnologías de la Información y la Comunicación[4] en pleno siglo XXI. El ponente recuerda las palabras de Melanie Swan al afirmar que cada diez años de las TICs hay un cambio de paradigma.

En este sentido, el primer paradigma de las TICs, fueron los *mainframe* de I*nternational Business Machines* Corporation[5]. Posteriormente, la segunda gran revolución por parte de IBM la encontramos cuando el joven Bill Gates crea el primer ordenador PC compatible. Bill Gates desarrollaría durante su trayectoria profesional diferentes programas informáticos con otros jóvenes que culminarían en la creación

[3] En resumen, con la blockchain nos encontramos ante el internet del valor, pudiendo gestionar nuestro dinero desde nuestro terminal móvil a través del uso de criptomonedas, sin necesidad de contar con ningún intermediario y de una forma totalmente confidencial, traspasando las fronteras internacionales en menos de un segundo.

[4] En adelante TICs.

[5] En adelante, IBM.

de unos ordenadores bajo la marca Apple, Windows y Microsoft: la gran revolución del siglo XX. Diez años más tarde aparecería la revolución de internet con el descubrimiento de *google*. La cuarta y última gran revolución la encontramos en los teléfonos inteligentes, el S*martphone* y con ello llega la revolución de la confianza, del intermediario que crea la confianza necesaria para que funcionen las TICs de hoy en día[6].

El ponente sigue apuntando en la misma línea y alude a la creación de riqueza generada por la citada práctica, pero afirma que la misma se está produciendo de una forma totalmente asimétrica. De tal manera que el dinero gestionado no se reparte de forma equitativa pues los creadores obtienen cuantiosos beneficios pero los trabajadores ejecutan su trabajo en condiciones cada vez más precarias. Ante esta problemática actúa, de nuevo, la blockchain. Esta forma de revolución de la confianza surge de dos formas:

- Por medio de la existencia de una persona o autoridad que sirve de mediador/intermediario y que da validez a lo acordado. Ejemplos de ello pueden ser un notario o un cura.
- Por medio del consenso. Ejemplos de protocolos de consenso, el ponente destaca los Yap de Micronesia y la Pow.

A continuación, y como consecuencia de todo cuanto antecede, el ponente pone especial énfasis en la digitalización del mundo exterior, lo que genera inevitables problemas como los derivados de la propiedad intelectual, por ejemplo, las fotos, las obras de arte o el propio dinero de curso legal. La consecuencia de todo ello es que son ilimitablemente reproducibles. En relación con el dinero encontramos el problema del doble gasto, si bien, el ponente refleja la posibilidad de solventarlo con las formulas derivadas de la blockchain, es decir, por medio de la existencia de una autoridad externa o mediante el consenso[7].

Asimismo, el ponente refleja nueve características de la blockchain o cadena de bloques:

1. Es un libro contable, distribuido en múltiples ordenadores y público pues cualquiera tiene acceso al mismo. Sitúa su comienzo en el bloque génesis.
2. Todas las transacciones pueden ser vistas por todos los usuarios del sistema. Se logra, por tanto, que todos los ordenadores puedan mostrar los cambios que se producen mediante la compra y venta de bitcoin usando la tecnología del consenso.

[6] Ejemplos de terceros de confianza son Uber, Wallapop, Airbnb, Facebook, PayPal, Instagram.

[7] Se comprueba que las transacciones efectuadas por PayPal o con una determinada compañía bancaria están centralizadas, impidiendo, con ello, el problema del doble gasto al comprobar que todas las transacciones realizadas son de carácter único. Por el contrario, en la blockchain no existe una entidad centralizada, siendo todos los usuarios del sistema los garantes de que las transacciones realizadas sean válidas, disponiendo cada uno de los usuarios del sistema de una copia de la base de datos.

3. Los estados del sistema se determinan y se cambian a través de un protocolo de consenso.
4. Es un protocolo de red P2P o punto a punto. Caracterizada por ser una red de ordenadores interconectados a fin de facilitar transacciones entre los usuarios del sistema.
5. Es una plataforma distribuida resistente a la censura. Los primeros creadores de la blockchain pretendían reforzar la estructura a fin de que fuera resistente a la censura e impedir la alteración y borrado de datos. Proporciona también el día y la hora exacta en el que se produce cada registro.
6. Proporciona almacenamiento redundante a prueba de puntos de fallos. De tal manera que puede eliminarse el 20, el 30, el 40 o el 90% de la información pero la misma seguirá en los nodos a disposición del que quiera consultarla.
7. Criptografía asimétrica, claves públicas y privadas. Lo que garantiza que actúe con un régimen de confianza y consenso.
8. Transacciones a prueba de manipulación.
9. El origen de las transacciones, la cadena de bloques puede ser verificada.

A tal fin, hace suyas las palabras de Eric Hughes, en el "Manifiesto Cipherpunk", cuando señala «la privacidad es necesaria para una sociedad abierta en la era electrónica», a lo que el ponente añadiría el derecho a la intimidad es el fundamento de una sociedad democrática. La privacidad en una sociedad abierta requiere de un sistema de transacciones anónimas. En este sentido, cita a Hal Finney, desarrollador en PGP Corporation, creador del cifrado asimétrico y primer desarrollador de bitcoin, tras su creador conocido bajo el alias de Satoshi Nakamoto[8].

Define, también el ponente la criptografía como la capacidad de difuminar el mensaje y, por ende, impedir el acceso al mismo hasta que no se disponga de la clave privada. De ahí surge la técnica del cifrado asimétrico que cuenta con dos claves. La primera, de carácter público, que sirve para cifrar el mensaje y la segunda, de carácter privado, que sirve para descifrarlo[9]. Al extrapolar la citada técnica de cifrado asimétrico a la blockchain, el bitcoin contaría con una clave privada como elemento esencial para el uso de las criptomonedas, y la clave pública, que es la que autoriza el envío y recibo de bitcoin, sin posibilidad de autorizar retirada de bitcoin, para lo cual será requisito *sine qua non* disponer de la clave privada.

Categoriza a continuación dos clases de blockchain:

- Públicas: lo que autoriza a cualquier persona, con identidad desconocida, a la formación de un nodo y su uso ilimitado por cualquier persona. Ejemplo de blockchain pública la encontramos en el bitcoin.

[8] Reflexionando sobre la tradición, el ponente refleja que ya los egipcios, los griegos y los espartanos usaban técnicas de cifrado, siendo crucial en la II Guerra Mundial cuando los americanos descubren la clave de los japoneses para comunicarse. En aquel tiempo las técnicas de cifrado no se permitían entre la población civil, si bien, es en los ochenta de este siglo cuando se comprueba que es necesario contar con métodos de cifrado para comunicarse.

[9] Ejemplo de ello es el número de cuenta bancario que se corresponde con la clave pública (solo permite ingresar dinero) y el pin de la cuenta con la clave privada (que nos permite operar con la cuenta para la retirada de efectivo).

- Permisionadas: condicionadas a la oportuna autorización de permiso. Encontramos ejemplos de blockchain permisionadas principalmente en el sector de la banca, como quorum, hyperledger fabric o IBM.

Afirma el ponente que algunos de los problemas más graves son los planteados en relación con el derecho a la protección de datos de carácter personal que es un apéndice de los derechos a la intimidad y a la privacidad. El ponente, refleja la importancia del tema, por cuanto nuestra personalidad viene determinada por nuestros propios datos. Nos enfrentamos, en consecuencia, a nuevos ataques a la privacidad. Es por ello que surge un nuevo derecho, esto es, el derecho a la protección de datos personales, desarrollado sentencia tras sentencia del Tribunal Constitucional, marcado por la influencia europea en la materia[10]; la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos que toma como base el artículo 18.4 de la Constitución Española cuando señala «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos» y, en fin, la reciente aprobación del proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Seguidamente, el ponente pone de manifiesto que la blockchain desarrollada por técnicos genera las siguientes problemáticas en relación con el derecho a la protección de datos personales:

- Las blockchain están deslocalizadas. Destaca la ausencia de domicilio social, al disponer de diferentes nodos de los registros en todos los países.
- Carecen de personalidad jurídica. Se trata, por tanto, de una serie de procesos realizados que carecen de autor conocido. Así sucedió con el creador de los bitcoin, que desarrolló el proceso de la blockchain de bitcoin en software libre y años más tarde desapareció, conocido bajo el seudónimo de Satoshi Nakamoto. En la actualidad se desconoce su identidad.
- No existe un responsable del fichero ni un encargado del tratamiento. Ello es debido a que existen determinadas personas que tratan con partes concretas de los datos protegidos por encriptación, pero que desconocen el origen y el fin de la citada información.
- Carácter indeleble de los registros de la blockchain. Los bitcoin tienen un espacio para incorporar un determinado texto escrito, pero surge la duda de qué ocurre con ese texto si presuntamente la blockchain tiene un marcado carácter indeleble.

Posteriormente el ponente refleja las aportaciones que la blockchain ha supuesto en materia de ciberseguridad:

- Confidencialidad. Los datos están protegidos por criptografía fuerte y ninguna autoridad externa tiene acceso a los mismos. Ahora bien, la blockchain de

[10] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE.

bitcoin no es totalmente anónima, se trata de un seudonimato, caracterizado por ser una persona desconocida, pero de la que se puede trazar y esbozar un perfil a partir de las transacciones que ha realizado. Ahora bien, existen otras monedas en las que resulta imposible. Por ejemplo, monero o z-cash.

- Integridad. En la blockchain no se puede falsear los datos, pues reúnen dos características claves, la inmutabilidad y la transparencia. Datos, por tanto, a prueba de manipulaciones cuyo origen puede ser verificado. Todas las áreas de negocio que utilicen datos sensibles pueden beneficiarse de esta tecnología, ya se trate de datos financieros, personales, médicos o de cualquier otra índole.
- Disponibilidad. Los datos están disponibles en miles de nodos, por tanto, el servidor nunca fallará, siempre será accesible, dado que el almacenamiento está distribuido y es redundante a prueba de caídas del sistema.

Aventura el ponente en líneas generales el futuro de los pagos. En este sentido, el dinero de curso legal desaparecerá y quedará exclusivamente el dinero bancario[11]. Pero no solo debe tenerse en cuenta ese control bancario, sino que también todas las transferencias de dinero operadas a través de bancos no manejan dinero físico, sino que simplemente se trata de un apunte contable, a lo que se añade la necesidad constante de contar con un intermediario toda vez que se pretende llevar a cabo una transacción comercial. El bitcoin y, por ende, las criptomonedas, pretenden convertirse en el efectivo digital con el que se pague, pues reúnen las siguientes características:

- Carácter anónimo.
- Carácter descentralizado, lo que elimina la necesidad de contar con una autoridad externa que haga efectiva la transacción.

Con su uso se pretende proteger los derechos a la privacidad e intimidad de las personas. Afirma Cuadrado Malasaña que las criptomonedas serán la única forma de manejar efectivo digital cuando ya no existan monedas y billetes. Si bien, pone de relieve las debilidades que puede afrontar la blockchain:

- Vulnerabilidades de la plataforma. La integridad de la blockchain está determinada por la plataforma de software sobre la cual se ejecuta. En este sentido, refleja el ponente que si la plataforma es poco fiable, ello afecta a la blockchain.
- Malware. La infraestructura que admite la blockchain está sujeta a toda clase de amenazas y vulnerabilidades comunes. Ningún software, resulta, por tanto, exento a la posibilidad de ataques.
- Pérdida de control. Caracterizado por un abuso del privilegio de la condición de administrador y la consecuente realización de cambios no autorizados en la infraestructura. Destaca, el ataque del 51%, cuando alguien controla el 51% de los nodos de la blockchain, y el ataque Sybil, una persona adopta diferentes identidades en internet para atacar la blockchain y tomar el control.

[11] En el momento en el que pretendamos realizar una transacción económica tendremos que operar con nuestros bancos, estando sometidos con ello al control de bancos y gobiernos, pese a la apariencia de que el dinero es circular.

Sella el ponente su intervención reseñando las promesas a las que aspira convertirse la blockchain, tras lo cual procede a responder a las preguntas formuladas por los asistentes, reflexionando acerca de las tres preguntas suscitadas con su intervención. Cierra la sexta intervención, el moderador D. Collado de la Guerra, agradeciendo a D. Cuadrado Malasaña la magistral ponencia efectuada sobre el tema, tras lo cual se dan por concluidas las IV Jornadas Nacionales de Derecho y Ciberseguridad y se procede por parte de los organizadores a la clausura de las mismas.

Comentarios de la relatora

No cabe duda de que nos encontramos en un constante avance tecnológico. Primero llegó la evolución y revolución de la información con la creación de los primeros ordenadores y el posterior lanzamiento de los *smartphones* y, ahora, esta modernización pionera da paso a la revolución del pago creando el internet del valor. Nos da recelo adentrarnos en ese mundo desconocido que supone la blockchain, pero al igual que ocurrió tiempo atrás con el internet de la información, aunque, *a priori* asusten los cambios, es inequívoco los beneficios que ha supuesto en nuestra calidad de vida el desarrollo del internet de la información. Lo mismo puede suceder, por tanto, ahora, con el internet del valor. Se comprueba que la blockchain, devuelve el poder del dinero al propio pueblo, eliminando la mediatización de bancos y demás autoridades; permite realizar diferentes transacciones de forma completamente anónima por medio de un código encriptado, preservando el derecho a la privacidad de nuestros datos de carácter más personal, salvaguardando, en consecuencia, nuestra razón de ser, la personalidad de todos nosotros. Pero no todo lo aventurado por la blockchain es halagüeño, también, afronta dificultades a solventar si quieren convertir la criptomoneda en el pago del futuro. Se comprueba el uso de la blockchain para la compra de armas, drogas, y, en general, como medio para defraudar; se ha demostrado que no es un sistema inmutable, pues es posible su hackeo o toma de control, lo que se traduce en una inevitable quiebra del sistema. Ahora bien, no podemos permanecer ajenos a la sociedad en la que vivimos, somos parte de esta era tecnológica, las Administraciones cada vez apuestan más por la electrónica en su proceder diario, extrapolándolo hasta sus relaciones para con los ciudadanos y, en fin, todo se vuelve cada vez más digital, hasta que llegue un día en el que ya no quede nada realizado a papel, ni siquiera, el propio dinero.