RELATORIAS DE LAS III JORNADAS NACIONALES DE DERECHO Y CIBERSEGURIDAD

Evento académico celebrado los días 25 y 26 de octubre de 2017 en el Auditorio Ciudad de León (día 25) y en el Salón de Grados de la Facultad de Derecho de la Universidad de León (día 26). 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 de Instituto Nacional de Ciberseguridad de España

PRIMERA PONENCIA: «El impacto del RGPD en la abogacía»
Ponente: Prof. Dr. D. José Luis Piñar Mañas, Catedrático de Derecho Administrativo en la Universidad Centro de Estudios Universitarios San Pablo, Director de la Cátedra *Google* de Privacidad, Sociedad e Innovación
Moderadora: Prof.ª Dra. Dña. Mercedes Fuertes López, Catedrática de Derecho Administrativo de la Universidad de León
Relatora: Dña. Marta González Aparicio, Personal Investigador en Formación de la Universidad de León (Área de Derecho Financiero y Tributario del Departamento de Derecho Público)

La primera conferencia de las III Jornadas Nacionales de Derecho y Ciberseguridad comenzó con la intervención de la Prof.ª Fuertes López, quien agradeció al INCIBE y a al equipo decanal de la Facultad de Derecho de la Universidad de León la labor realizada en la organización de las referidas Jornadas, para posteriormente pasar a presentar al primer ponente, el Prof. Piñar Mañas, destacando algunos logros de su amplia trayectoria académica.

El Prof. Piñar Mañas comenzó su intervención señalando que, tal y como previamente indicó la Prof.ª Fuertes López, estamos ante un nuevo modelo de protección de datos, cuyos caracteres expuso detalladamente a lo largo de su ponencia.

La protección de datos es un derecho «nuevo», basado en los datos de carácter personal de personas físicas (no personas jurídicas), sujetos a tratamiento, si bien no

todo tratamiento de datos viola su protección. Su origen se encuentra en la II Guerra Mundial, a fin de evitar las prácticas realizadas por nazis y comunistas en este periodo derivadas del tratamiento informático de los datos personales de la población.

La generalización del uso de la informática condujo al legislador a proteger los datos personales frente al uso de la informática. Señala el ponente que precisamente este fin protector es lo que aparece en la base del art. 18.4 de la CE[1], que refleja una posición de recelo ante la informática y sus usos. A su vez, este fin protector fundamenta el derecho a la protección de todo tipo de datos de carácter personal. Las SSTC 290 y 292/2000 señalan que todos tenemos derecho a saber quién tiene nuestros datos, por qué y para qué, pudiéndonos oponer al tratamiento de esos datos, si bien con ciertos límites (p. ej. datos tributarios). La protección de datos supone la «autodeterminación informativa» sobre los propios datos, entendida como control sobre tales datos. Otra cuestión esencial en torno a este derecho es que su violación pasa desapercibida hasta que se producen las consecuencias derivadas del robo de identidad.

Los abogados y los despachos de abogados, como sujetos pasivos del derecho a la protección de datos, tienen la obligación de cumplir las previsiones sobre protección de datos en calidad de responsables o encargados del tratamiento. Tal protección va a estar regulada en un Reglamento que entrará en vigor el 25 de mayo de 2018 y que va a modificar el actual modelo de protección de datos de carácter personal. Se trata del 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[2].

Indica el Prof. Piñar Mañas que es la primera vez que se regula un derecho fundamental por medio de un Reglamento Europeo. Como todos los Reglamento de la Unión Europea, tiene alcance general y es obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro, de modo que no es necesaria su trasposición, lo que supone que, tras su entrada en vigor, los operadores jurídicos deberán conjugar el texto del Reglamento con la nueva Ley Orgánica de Protección de Datos.

A continuación se detalla la estructura sistemática del Reglamento, formado por 99 artículos y 173 considerandos. La clave de esta nueva norma es que establece un nuevo modelo, ya que, a partir de ahora, vamos a pasar de un modelo de gestión casi «administrativa» de los datos, a un modelo de gobierno responsable de la información en la que el responsable deberá hacer lo que considere conveniente para cumplir con el Reglamento y demostrar a la autoridad competente tal cumplimiento, en base al principio de responsabilidad proactiva del art. 24 y en la aproximación basada en el riesgo, lo que implica una mayor incertidumbre pero también la posibilidad de ajustar mejor el tratamiento de datos a la realidad (p. ej. implantando las medidas de seguridad que se consideren más adecuadas en función de los datos a proteger).

[1] El mencionado precepto 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».

[2] DOUE I, 119, de 4 de mayo de 2016.

En este nuevo modelo la evaluación de impacto de la protección de datos va a tener un protagonismo esencial, así como la figura del Delegado de Protección de Datos, prediciendo diversos estudios nacionales e internacionales el incremento exponencial en el número de estos profesionales. También se fortalecen los derechos de los afectados, (p. ej. en relación a consentimiento), las autoridades en materia de protección de datos y se fija un modelo sancionador más estricto.

Es muy importante el carácter global del modelo y así lo indica en el art. 3, que señala que el Reglamento se aplica a todas las entidades que ofrezcan productos y servicios a quienes estén en la UE, independientemente de su tamaño, de modo que el alcance de este texto normativo es mundial.

Los principios del Reglamento son similares a los de la Directiva actual. Los Principios relativos al tratamiento, recogidos en el art. 5 del Reglamento son los principios de licitud, lealtad, transparencia, limitación de finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva. En opinión del ponente, los principios de seguridad y finalidad son los más importantes en materia de protección de datos de carácter personal.

Las condiciones para el consentimiento aparecen en el art. 7, y en relación al mismo es destacable que en la actualidad el consentimiento puede ser tácito (y así ocurre en muchas ocasiones). Este consentimiento tácito es correcto conforme a la Ley actual, pero va a dejar de serlo conforme al Reglamento, lo cual va a requerir la transformación de esos consentimientos tácitos en expresos.

El art. 6 se refiere a la licitud del tratamiento, y dentro de este precepto el Prof. Piñar Mañas destaca el apartado f, que señala «el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño», señalando la dificultad para definir qué deben considerarse intereses legítimos.

Los derechos del interesado se amplían; hasta ahora eran los derechos ARCO (acceso, rectificación, cancelación y oposición), a los que se añaden otros derechos. Destaca el derecho de supresión o derecho al olvido del art. 17, con especial referencia a la sentencia del TJUE de 13 de mayo de 2014, caso Mario Costeja. Otro de los derechos nuevos es el derecho a la portabilidad de los datos, recogido en el art. 20 del Reglamento, que supone un primer paso para que el particular reciba los datos que le incumban en un formato estructurado, de uso común y de lectura mecánica, y pueda transmitirlos. Si bien el Prof. Piñar Mañas considera que el precepto no logra totalmente su objetivo, sí supone un primer paso en su consecución.

El modelo también cambia debido a dos principios que a su vez son obligaciones: el principio de responsabilidad, establecido en el art. 24 del Reglamento, conforme al cual el responsable aplicará las medidas que considere adecuadas en función del riesgo; y el principio de privacidad desde el diseño por defecto, del art. 25.2 del Reglamento, que supone que el responsable del tratamiento aplicará, tanto en el

momento de determinar los medios de tratamiento como en el del propio tratamiento, las medidas técnicas y organizativas apropiadas concebidas para aplicar de forma efectiva los principios de protección de datos.

A continuación, el Prof. Piñar Mañas trata la cuestión de la seguridad de los datos, recogida en los arts. 32 a 34 del Reglamento, cuya consecuencia es que el responsable deberá determinar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en función de los criterios dados en el propio art. 32 (p. ej. seudonimización y cifrado de datos personales, capacidad para garantizar la confidencialidad, integridad, disponibilidad, etc.). Estas medidas deben ser notificadas con carácter obligatorio a la autoridad de control de datos según el art. 33 (lo que supone una gran novedad respecto al modelo actual), y las violaciones de seguridad deben ser notificadas al interesado, tal y como indica el art. 34.

Se pone de manifiesto también la importancia de la evaluación de impacto relativa a la protección de datos (art. 35 del Reglamento), la necesidad de consulta previa (art. 36), así como la figura del Delegado de Protección de Datos, que debe ser una persona con formación jurídica, cuya presencia es obligatoria en todas las entidades públicas y en las entidades privadas que traten datos a gran escala, si bien el Reglamento no precisa qué es tratar datos a gran escala. La Agencia Estatal de Protección de Datos (AEPD), junto con la Entidad Nacional de Acreditación (ENAC), ha aprobado un esquema de acreditación para certificar a los sujetos que deseen ejercer como Delegados de Protección de Datos. Está acreditación no es obligatoria en la actualidad pero es recomendable.

El nuevo Reglamento potencia la autorregulación, regula las transferencias internacionales de datos (arts. 44 a 50) y las autoridades de control independientes. En el modelo europeo la existencia de estas autoridades es esencial, siendo el primer derecho fundamental con la exigencia de una autoridad de este tipo para su salvaguarda. El TJUE ha dictado varias sentencias indicando cuáles son las notas que deben garantizar la independencia de la autoridad de control. Esta autoridad tiene un papel fundamental en el modelo y también en el ámbito de cooperación y coherencia (arts. 60 a 67) entre los países de la Unión Europea. En este punto destaca la situación que tiene lugar cuando un ciudadano de un país de la Unión sufre una violación en sus datos personales por una entidad residente en otro Estado de la Unión. En estos casos, la reclamación se presenta en el Estado de residencia del particular, pero resuelve la Agencia de Protección de Datos del Estado de residencia de la entidad. Si tal Agencia desestima o inadmite, la Agencia del tercer Estado traslada la resolución al Estado de residencia del particular para que sea esta la que adopte la decisión y notifique directamente al reclamante.

Por otro lado, se fortalece mucho el derecho a indemnización y el régimen sancionador, con sanciones de hasta 20.000.000€ o, tratándose de empresas, el 4% del volumen de negocios total anual global.

Para concluir, el Prof. Piñar Mañas destacó que está en marcha la adaptación de la legislación española al Reglamento por vía de la nueva Ley Orgánica de Protección de Datos, actualmente en fase de anteproyecto, constando de 8 Títulos. El núcleo

esencial de esta Ley serán las directrices dadas por el Reglamento. Todo ello cambia la gestión y el enfoque de la protección de datos con una gran importancia de la figura del responsable, lo que nos sitúa ante una situación poco conocida, en especial para los juristas, que deben afrontar este reto en el ejercicio de su actividad.

Comentarios de la relatora

De la exposición del Prof. Piñar Mañas destaca el papel protagonista del Reglamento 2016/679 en el cambio del modelo de protección de datos de carácter personal vigente en la actualidad. Este cambio de modelo en el Reglamento, de directa aplicación en toda Europa, instaura «la cultura de la privacidad de las organizaciones», de modo que los tratamientos de datos deben respetar los derechos de los interesados y, para ello, ese respeto debe formar parte de la cultura de la organización.

Además, se amplía el número de derechos reconocidos, pues a los ya clásicos derechos ARCO (acceso, rectificación, cancelación y oposición) se añaden dos nuevos derechos, el denominado «derecho al olvido», como efectivo derecho de supresión, y el derecho a la portabilidad de datos.

Por otro lado, se introduce la figura del Delegado de Protección de Datos, cuyo nombramiento es obligatorio para todos los organismos públicos (con la excepción de tribunales en aplicación de la función judicial) y las entidades privadas, sean estas consideradas responsables o encargados del tratamiento, cuyas actividades principales supongan la «observación habitual y sistemática de interesados a gran escala» o el «tratamiento a gran escala de categorías especiales de datos».

Este nuevo marco en la protección de datos y el previsible incremento en la demanda de Delegados de Protección de Datos con formación jurídica, que se configuran como una de las piedras angulares sobre las que pivota el sistema, supone una oportunidad para los juristas y a la vez un desafío con amplias posibilidades de ser aprovechado.

SEGUNDA PONENCIA: «Ciberseguridad y derechos fundamentales: tensiones y conexiones»
Ponente: Prof. Dr. D. Juan Antonio García Amado, Catedrático de Filosofía del Derecho de la Universidad de León
Moderadora: Prof.ª Dra. Dña. Isabel Durán Seco, Profesora Contratada Doctora (acreditada Profesora Titular) de Derecho Penal de la Universidad de León
Relatora: Dña. Dhyana Stephanía Serrano Suárez, doctoranda de la Universidad de Salamanca (Área de Derecho Penal del Departamento de Derecho Público General), Colaboradora Honorífica de la Universidad de León

Esta ponencia se enmarca dentro de la mesa de trabajo titulada «Derechos fundamentales y minoría de edad». La moderadora de la mesa, la Prof.ª Dra. Dña. Isabel Durán Seco, Profesora Contratada Doctora (acreditada Profesora Titular) de Derecho Penal de la Universidad de León, después de presentar al Prof. García Amado, le cede la palabra. El ponente inicia señalando que hay una enorme vulnerabilidad de la información que se almacena en los ordenadores y que circula por la red. De igual modo, alude al hecho de que los profesores de Derecho saben muy poco de cuestiones de ciberseguridad y tampoco hay una materia que verse sobre los

problemas jurídicos de las nuevas tecnologías. Las cifras denotan la relevancia del tema: en el año 2010, al parecer, se colgaron en *Facebook* 30.000 millones de fotos y los datos del año 2015 señalan que eran 10.500 millones de fotos las que se colgaban mensualmente, lo cual suma casi 127.000 millones de fotos al año. Si a esto se suma las fotos que circulan por *WhatsApp* resultarían cifras verdaderamente impresionantes.

Menciona el ponente que uno de los principales expertos en cuestiones que tienen que ver con la ciberseguridad, especialmente con el derecho a la privacidad o a la intimidad: el Prof. Dr. Alessandro Acquisti, italiano, de la Universidad de Carnegie Mellon. Este autor revela algunos experimentos que se realizaron hace 5 o 6 años, uno de los cuales consistía en tomarles una foto a algunos sujetos experimentales (estudiantes) para posteriormente someterla a una aplicación de tratamiento o reconocimiento de imágenes y en cuestión de segundos en el ciberespacio aparecieron imágenes de ese sujeto con muy poco margen de error. Y no solo eso, sino que a partir de esas imágenes y con la utilización de otros programas conseguían hallar datos de la vida privada de esos sujetos.

Seguidamente, el ponente se cuestiona sobre cuántas son las preocupaciones que las personas serían capaces de asumir si no solo fueran celosos de su derecho a la intimidad, sino que además estuvieran preocupados por sus relaciones cotidianas, familiares y sentimentales. Es el caso del registro de datos que se espera mantener en el anonimato como pago de moteles.

Asimismo refiere que en la película *Minority Report* de Tom Cruise, se ve como cuando el actor pasa por cierto pasillo se va proyectando publicidad personalizada para él. Y de hecho ya empiezan en algunas ciudades a utilizar unos sistemas de publicidad personalizada en razón del coche; es decir que en las vallas publicitarias se va a proyectar una cosa u otra en razón al vehículo que esté circulando en un determinado momento.

El Prof. García Amado se cuestiona si somos completamente transparentes, plantea que para dejar de serlo posiblemente tendríamos que desconectarnos de muchas cosas, debido a que en los últimos tiempos se habla de computación ubicua, que implica que las nuevas tecnologías se integran en el entorno de la persona, lo cual implica que los dispositivos se encuentran todos interconectados entre sí y conectados con el mundo. Además, las aplicaciones que se utilizan para el cuidado de la salud, como las que llevan los deportistas, están transmitiendo constantemente datos sobre todo: por donde se mueve la persona, cuales son sus pulsaciones, síntomas, etc. Algunos datos señalan que normalmente, los usuarios de estas aplicaciones no leen las condiciones de privacidad, de hacerlo les tomaría unos 25 días al año.

Siendo este contexto al que nos sometemos, una conclusión elemental es que tal vez no existe una plena consciencia o no se educa para asumir responsablemente las consecuencias de lo que hacemos cuando damos nuestros datos, cuando enchufamos nuestros aparatos o cuando llevamos encendida la ubicación de nuestro móvil.

Por otra parte, el Prof. García Amado señala que en una ocasión uno de los habituales comentaristas de su *blog* le pidió borrar todos los comentarios que había hecho, pues le estaban haciendo una prueba en una empresa y quizás había dicho cosas que no le convenía que se supieran. Ante lo cual refiere que es completamente conocido que lo primero que hacen los departamentos de personal de las empresas es ir a hacer rastreos en las redes y el ciberespacio de la persona que desean contratar. Si esa empresa o departamento administrativo tiene suficiente habilidad, recursos, destrezas y competencias, se puede encontrar en la red con un completo perfil de la persona que incluya: su estado de salud, sus hábitos, sus gustos, etc.

Es evidente que hay un conocimiento nuestro que nos expone a cualesquier uso y ahí está lo que el ponente llama «la paradoja de la privacidad». La bibliografía sobre ciberseguridad y derecho a la intimidad subraya que, en las encuestas, las personas señalan que les importa en gran medida el derecho a la intimidad, pero simultáneamente no son conscientes de que se están desnudando de múltiples maneras, y a veces literalmente.

El ponente refiere que, para organizar una asignatura sobre problemas de ciberseguridad y derechos fundamentales, habría que hacer toda una clasificación o una casuística que pondría a los juristas en la tesitura de poner a prueba gran parte de teorías y conceptos que se creen muy consolidados. La ciencia y la tecnología avanza en su capacidad para plantear retos o para atacar ciertos bienes o derechos como la intimidad; pero no solo, también el honor o la propiedad, entre otros.

Hoy en día los sujetos pasivos y activos de los ciberataques pueden ser los Estados, las personas jurídicas (básicamente las empresas) y los propios sujetos particulares. Hay acuerdo entre los expertos en señalar que el escenario de las próximas guerras (sino ya las actuales) será el ciberespacio. Durante la última década no en vano los Estados desarrollados han puesto en marcha políticas o estrategias de ciberseguridad nacional. Hay estudios que señalan cómo los Estados organizan estas cuestiones, por ejemplo: en que manos se pone la coordinación del mando supremo cuando hay un ataque muy grave contra instalaciones básicas de un Estado; cómo se lleva a cabo la coordinación entre los distintos organismos estatales; o cómo la coordinación entre los aparatos públicos y las empresas privadas.

De hecho, las guerras antaño transcurrían mediante el enfrentamiento físico de quienes integraban los ejércitos. El desarrollo tecnológico trajo la posibilidad de matar al enemigo sin el encuentro físico con él, por ejemplo bombardeando, pero en la actualidad los bombardeos se hacen con drones y a través de la utilización de programas en sustitución de armas. Ahora vemos que los Estados ya no se están armando con bombas ni buques de guerra sino con *hackers*. Por ejemplo, Corea del Norte tiene un autentico ejercito de *hackers* dispuestos a atacar a sus enemigos reales o imaginarios. Ese Estado que puede ser víctima de ataques, al mismo tiempo se tiene que armar convirtiéndose en un riesgo para los derechos personales y para el derecho a la intimidad.

El ponente relata que el hoy Rey de España, entonces Príncipe de Asturias, acudió en una ocasión a una universidad. Ya que era grande la preocupación en cuanto a su seguridad, el comisario de Policía mencionaba que estarían «haciendo barridos en el

ciberespacio» y la máquina estaría monitoreando las conversaciones para asegurarse de que no hubiera peligro. Lo cual evidencia que los Estados sufren ataques que tienen que prevenir y aumenta su capacidad para intervenir en nuestras comunicaciones, lo cual podría poner en riesgo nuestra intimidad.

Por otra parte, las empresas también sufren ataques; por ejemplo, los realizados contra *JP Morgan*, *eBay* y *Adobe*. Los piratas pueden obtener nombres, datos, claves, números de tarjetas, etc.; estas empresas, a su vez, entran en el contraataque y ponen en peligro la intimidad. No obstante, el derecho a la intimidad también puede ser puesto en peligro cuando una persona accede al móvil de otra para establecer su ubicación. También sucede que un Guardia Civil de cierto ámbito de seguridad, solo con el número de matrícula de un vehículo puede verificar en su ordenador donde fue captado por un radar o si tiene alguna multa.

Desde el punto de vista jurídico a esas intromisiones en nuestra información le podemos dar todo tipo de calificación. La fácil es la penal, pues hay conductas que son delito. Hay toda una casuística de comisión mediante instrumentos informáticos; y de está manera estamos protegiendo los bienes jurídico penales tradicionales frente a modos de acceso actuales. Pero existen algunos casos en que nos movemos un poco en el limbo. Por ejemplo, los casos en que las empresas de telefonía, de seguros, o de energía (los tres grandes tipos de empresas delincuentes contra el derecho a la intimidad y la salud) se hacen con números de teléfono y llaman para ofrecer un cambio de compañía o descuentos.

El ponente cuestiona cuál es el tratamiento jurídico que merece o se puede dar a quien nos envía sistemáticamente *spam* o correo electrónico no solicitado con fines publicitarios. En esta materia se presenta una especie de limbo por el hecho de que el servidor en cuestión estará en un lugar inaccesible para el común de las personas. Posteriormente se pregunta: ¿qué pasa con los llamados *big data*?, y además se cuestiona sobre la legalidad o ilegalidad de la construcción de perfiles de las personas a partir del procesamiento de datos de cientos y miles de personas.

Otro experimento al que hace mención el ponente es aquel en el que a partir del nombre de una persona, los experimentadores acceden a la lista de sus amigos en internet y consiguen establecer quienes son sus dos mejores amigos; generalmente un programa lo hace con alto grado certidumbre. Fundiendo las imágenes de los dos amigos construyen una imagen única. El experimento consiste en establecer que si a una persona le llega un mensaje con la imagen de un vendedor ofreciéndole un producto comercial, esta reacciona con frialdad y distancia porque se lo está vendiendo alguien que no conoce. Pero es diferente si es esa imagen familiar la que le llega, a pesar de que la persona es incapaz de reconocerla y no llega siquiera a sospechar que la foto es la fusión de los dos mejores amigos. Al existir una familiaridad inconsciente se siente una proximidad que aumenta enormemente la probabilidad de realizar un trato. A partir de lo cual se generan interrogantes respecto a cómo se gestiona el derecho a la intimidad.

El ponente indica que la literatura menciona dos paradojas. La más importante es la «paradoja de la privacidad», que consiste en lo siguiente: a menudo el descuido al

manejar datos nuestros es exactamente proporcional a nuestra preocupación por la intimidad; es decir, muchas veces las personas que se proclaman más celosas de su privacidad, acaban siendo las más inclinadas a ofrecer todo tipo de datos. Esto se suma a la llamada «paradoja del control», que señala que es muy fácil engañar a las personas también. Hay investigaciones muy interesantes relacionadas con el último premio nobel de economía el Dr. Richard H. Thaler, uno de los fundadores de la llamada economía conductual, teoría que plantea que las personas no son sujetos racionales como señalaba el pensamiento económico clásico, sino que actúan y razonan determinados por sesgos, lo que tradicionalmente se conoce como prejuicios, y por heurística. La manera de engañar es hacerle pensar a las personas que tienen el control, por ejemplo, cuando les piden una serie de datos y posteriormente les preguntan si quieren que esos datos se hagan públicos o no. Si bien la persona marca «No», procede a proporcionar gran cantidad de información personal. Lo que ha ocurrido es que la persona ha afirmado que no desea que la información la hagan pública, mas no que no la traten de determinada manera.

Afirma el Prof. García Amado, que está bien que en algún lugar se procesen esos datos que piden las aplicaciones que se utilizan para salir a correr, en razón a que tiene utilidad científica, pero muchas personas son enormemente celosas de su intimidad. Por lo que el ponente expone su tesis: Tal vez se deba cambiar el concepto sobre ciertos derechos fundamentales. Muchas veces se pretende acceder a ciertos beneficios como la pensión sin tener los requisitos de trabajo requeridos. Queremos disfrutar al máximo de todo, pero al mismo tiempo que se nos respete todo enormemente y nos sentimos «titularísimos» de unos derechos que no solo son inalienables, sino incuestionables.

En otras palabras, la tesis del ponente es que primero: en cuestiones de derecho a la intimidad, quizás deberíamos relajarnos un poco. Debido a que vamos siendo transparentes hay que aprender a vivir en esa situación y en esa tesitura. Si queremos beneficiarnos de la información tenemos que asumir que nos convertimos en información. Y tal vez más que utilizar el instrumento jurídico con un ánimo inútilmente represor, lo que convendría es que desde las escuelas hasta las universidades se enseñara a manejar responsablemente la información. Segundo: si publicamos nuestra información tenemos que asumir la responsabilidad. Tercero: precisamente estos autores de la economía conductual se han inventado el concepto de *nudge*, que significa «empujón» o «empujoncito», que trata de cómo no es útil el paternalismo de la prohibición. Lo que hay que hacer es enseñar e impulsar, incentivar a la gente a un uso responsable de su información, así como incentivar a las empresas, en particular a las empresas tecnológicas, para que lleven a cabo los desarrollos de los programas y las aplicaciones que permitirían, sin mucho coste adicional, una mejor protección de nuestra intimidad.

El Prof. García Amado finaliza su exposición aclarando que su tesis de fondo es que en estas materias debemos llegar a una cierta combinación de más responsabilidad y menos histeria. Debemos reservar el Derecho y la represión, la *ultima ratio*, para atentados verdaderamente graves contra bienes auténticamente básicos, cuyo daño no se deba a una irresponsable y deliberada exposición por nuestra parte.

Comentarios de la relatora

La exposición del Prof. García Amado combina varios temas de relevancia en la nueva era digital relacionadas con la paradoja seguridad *vs.* privacidad, la utilización de información personal por parte de Estados y empresas, así como la ciberguerra y el ciberespionaje. En cuanto al ciberespionaje que pueda ser realizado por parte de los Estados, considero, tal como lo expone Hanni Fakhoury, que existe un marco legal en el que se define cómo puede un Estado llevar a cabo la vigilancia y hacerlo de tal manera que respete los derechos humanos; ya sea la vigilancia al interior del Estado, para reprimir la comisión de delitos, cómo la vigilancia fuera del país. Ello se encuentra consagrado en trece principios que al respecto se deben seguir: legalidad, necesidad, transparencia y proporcionalidad, entre otros; principios que difícilmente pueden obviarse en un Estado Social de Derecho que sea garante de los derechos humanos.

No queda duda de que la exposición que actualmente decidimos hacer de nuestra información personal en las redes sociales, *blogs* y aplicaciones, conlleva asumir responsabilidad por ello. Una de las conclusiones que comparto con el ponente es la necesidad de educar a los ciudadanos en temas de ciberseguridad, logrando de esta manera una conexión entre gobiernos, empresas y el ámbito académico, especialmente lo que se refiere al manejo del *big data*, lo que quizás permitiría que la privacidad y la ciberseguridad puedan complementarse o al menos no entorpecerse.

También hay que reconocer que el análisis masivo de esta información que es subida a la red por los usuarios puede traer múltiples beneficios y tal como lo expone la ingeniera en computación Dña. Érika Azabache, puede ayudar a revelar tendencias y estadísticas que facilitan la toma de decisiones para optimizar procesos, reducir costos o encontrar soluciones para los problemas de la vida cotidiana. Asimismo, en el sector bancario, a través de este procedimiento se puede reducir el riesgo de los fraudes, mejorar el conocimiento de los clientes para optimizar las ofertas y desarrollar nuevos productos, alentar la puntualidad de los pagos por parte de los consumidores e impulsar la rentabilidad. Azabache apunta que incluso a través de la aplicación del análisis de *big data,* es factible aliviar el problema del tráfico en las ciudades, permitiendo crear conocimientos que propician la aparición de nuevos emprendimientos, modelos de negocios y *startups* innovadoras.

Finalmente, con el Prof. Dr. Alessandro Acquisti, considero que una de las peleas decisivas de nuestro tiempo será la pelea por el control de la información personal. La pelea por que el *big data* se vuelva una fuerza de libertad en lugar de una fuerza que nos manipule desde las sombras.

TERCERA PONENCIA: «Límites de la Ley en la protección de menores en internet»
Ponente: D. José Fernández Díaz, Jefe de la Sección de Informática del Servicio de Asistencia a Municipios de la Diputación de León
Moderadora: Prof.ª Dra. Dña. Isabel Durán Seco, Profesora Contratada Doctora (acreditada Profesora Titular) de Derecho Penal de la Universidad de León
Relatora: Dña. María Nieves Alonso García, Personal Investigador en Formación de la Universidad de León (Área de Derecho Constitucional del Departamento de Derecho Público)

El ponente, D. José Fernández Díaz, inicia su intervención destacando el crecimiento que ha experimentado el uso de las tecnologías de la información y comunicación en los últimos años, siendo especialmente significativo este incremento entre los más jóvenes. La proporción de uso de tecnologías de información por la población infantil (de 10 a 15 años) es, en general, muy elevada.

La evolución de los resultados según la edad sugiere que el uso de internet es una práctica mayoritaria en edades anteriores a los 10 años. Por su parte, la disposición de teléfono móvil se incrementa significativamente a partir de los 10 años hasta alcanzar el 90,9% en la población de 15 años.

En cuanto a las motivaciones en el uso de las tecnologías, el 15'8% afirma que les proporciona bienestar y casi un 10% señala que es útil para evadirse de los problemas.

El uso de estas tecnologías por los menores genera dificultades para el control parental. A fin de ejemplificar la extrema facilidad y la falta de controles para el acceso a las nuevas tecnologías por parte de los menores, puede tenerse en consideración la creación por parte de un menor de 12 años de Torrevieja de un canal de *Youtube* con el objetivo de obtener ganancias por su actividad como *youtuber*. Para ello, dicho menor, con la ayuda de un amigo, creó en agosto de 2016 su canal y cuenta de *Google Adwords* para empezar a cobrar por cada vídeo que publicara gracias a la publicidad. *Google Ireland* le solicita al menos 100.000 euros en concepto de publicidad de su espacio. La multinacional empezó a cargar cantidades de 50 a 150 euros en la cuenta del menor. El gasto creció de forma exponencial, llegando en septiembre de ese mismo año a superar los 78.000 euros. La entidad bancaria asociada a la cuenta se puso en contacto con los padres como titulares para informarles de los extraños movimientos, momento en el cual el menor desactiva su cuenta.

En la última década han proliferado los delitos relacionados con las nuevas tecnologías tales como el ciberacoso, el *cyberstalking*, *happy slapping* o sextorsión, que tienen entre los menores en muchas ocasiones a sus víctimas, por su rango de conocimiento en el acceso a las nuevas tecnologías y su especial vulnerabilidad.

Es especialmente significativo destacar la inexistencia de control de acceso para la creación de cuentas en las redes sociales. Conforme a la normativa española, el art. 13.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, establece que «Podrá procederse al

tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores». Por consiguiente, el consentimiento para el tratamiento de los datos personales solamente puede ser otorgado por el interesado, salvo en el caso en que el afectado sea menor de 14 años o incapaz, en cuyo caso deberá ser otorgado por sus padres o tutores, sin perjuicio de que estos deban completar la capacidad del menor, aunque sea mayor de 14 años, en aquellos supuestos en que una ley así lo establezca.

Una de las medidas encaminadas a proteger a los menores por parte de sus padres y tutores es la no disposición de tarifa de datos en sus teléfonos móviles. Llevado a la práctica, ha supuesto en ocasiones el acceso de los menores a través de las redes wifi. Su acceso libre supone la utilización indiscriminada desde sus dispositivos móviles de aplicaciones, redes sociales y demás herramientas de acceso a internet.

Asimismo, ha sido objeto de cuestionamiento la responsabilidad de la red social en tanto en cuanto no ejerce ningún control de acceso para su utilización por parte de los menores. A tenor de esta situación, se plantea la aplicación del art. 1.263 del Código Civil conforme al cual «No pueden prestar consentimiento: 1.º Los menores no emancipados, salvo en aquellos contratos que las leyes les permitan realizar por sí mismos o con asistencia de sus representantes, y los relativos a bienes y servicios de la vida corriente propios de su edad de conformidad con los usos sociales. 2.º Los que tienen su capacidad modificada judicialmente, en los términos señalados por la resolución judicial».

En cuanto a la responsabilidad que pudiera ostentar la red social, el art. 98.9 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias establece que «Corresponde al empresario probar el cumplimiento de las obligaciones a que este artículo se refiere. El empresario deberá adoptar las medidas adecuadas y eficaces que le permitan identificar inequívocamente al consumidor y usuario con el que celebra el contrato».

Por lo que respecta al control parental de los menores, cabe tener en consideración los arts. 4 y 5 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación del Código Civil y de la Ley de Enjuiciamiento Civil, modificados por la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, conforme a los cuales los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones.

La brecha digital supone otra de las dificultades a la que se enfrentan los progenitores de cara al sometimiento de control a sus hijos.

Es significativa al respecto la entrevista realizada al Magistrado-Juez de Menores de Granada, el Ilmo. Sr. D. Emilio Juan Ildefonso Calatayud Pérez, quien sostiene que

es preciso tener en cuenta el art. 155 del Código Civil, en virtud del cual «Los hijos deben: 1.º Obedecer a sus padres mientras permanezcan bajo su potestad, respetarles siempre. 2.º Contribuir según sus posibilidades al mantenimiento de la familia». Calatayud Pérez recurre a los supuestos prácticos que han sido objeto de su enjuiciamiento, haciendo referencia a niñas que fueron castigadas sin móvil y como respuesta maltrataron a sus madres con lesiones graves o intentaron suicidarse por no disponer de aquel. El Magistrado-Juez justifica la violación de la intimidad de los hijos a fin de evitar consecuencias gravemente dañosas para el menor.

Comentarios de la relatora

Las nuevas tecnologías avanzan a una velocidad vertiginosa que dificulta la adaptación de la normativa a unas circunstancias en constante cambio. Ello implica en algunos supuestos situaciones de desprotección. En los menores se enlazan dos características que dificultan su total protección: por un lado, son el sector de la población que adquiere con mayor rapidez el dominio de estas nuevas tecnologías y, por otro, su especial vulnerabilidad supone que sean objeto de los riesgos de la red. La Ley en algunos casos limita la protección de los menores en internet. Es preciso, a fin de adaptar la normativa a la nueva era digital y evitar situaciones de desprotección, regular aspectos como el consentimiento otorgado por los menores, introducir controles de acceso con límites de rangos de edad, así como facilitar el control parental del uso de las nuevas tecnologías.

CUARTA PONENCIA: «El enésimo capítulo de tensión entre privacidad y seguridad: la obligación de conservación y cesión de los metadatos relativos a las comunicaciones electrónicas»

Ponente: **Prof. Dr. D. Luis Ángel Ballesteros Moffa**, Profesor Titular (acreditado Catedrático) de Derecho Administrativo de la Universidad de León
Moderador: **Prof. Dr. D. Salvador Tarodo Soria**, Profesor Titular de Derecho Eclesiástico del Estado de la Universidad de León
Relatora: **Dña. Tamara Álvarez Robles**, Personal Investigador en Formación de la Universidad de León (Área de Derecho Constitucional del Departamento de Derecho Público)

El moderador, Prof. Dr. D. Salvador Tarodo Soria, comienza con la presentación del Prof. Dr. D. Luis Ángel Ballesteros Moffa y de su ponencia «El enésimo capítulo de tensión entre privacidad y seguridad: la obligación de conservación y cesión de los metadatos relativos a las comunicaciones electrónicas». En particular, la ponencia se fundamenta en su reciente investigación: «La difícil situación de la Ley 25/2007 de conservación y cesión de datos de tráfico y localización en las comunicaciones electrónicas: la "tala" de su base comunitaria y los desfavorables vientos desde sus homólogas europeas», publicada en la Revista Aranzadi de Derecho y Nuevas Tecnologías, núm. 44, mayo/agosto 2017, p. 42 y ss.

El moderador cede la palabra al ponente, no sin antes advertir que nos encontramos ante un profesor de la Facultad con un reconocido prestigio en la investigación del Derecho Administrativo y con varios artículos publicados en relación al tema que se nos presenta.

Comienza D. Luis Ángel Ballesteros indicando que el problema a tratar representa un capítulo específico pero importante en la tensión privacidad-seguridad, junto con otros, como la nueva Directiva de policía en materia de protección de datos, Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo; o la también novedosa Directiva de transferencia de datos PNR en la lucha contra el terrorismo y delincuencia grave, la Directiva (UE) 2016/681, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

Si bien, la intervención se centra en el problema, también actual, de la obligación de conservación preventiva de los datos de tráfico de las comunicaciones electrónicas. Un tema que atañe a varias normas europeas e internas, como las siguientes: el Reglamento europeo de protección de datos, la Directiva 2002/58/CE de privacidad electrónica y la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Ante este marco normativo complejo, seis apartados exponen los puntos más importantes que derivan del estudio del mismo:

1) Adaptación del instituto de protección de datos a los distintos ciclos tecnológicos; en particular, a las comunicaciones electrónicas, servicios de la sociedad de la información y nuevos servicios basados en internet. Nos permitirá concretar el régimen jurídico.
2) Riesgos especiales de la privacidad electrónica, aparte de los generales también en el ámbito de las comunicaciones electrónicas (internet).
3) El riesgo de los datos de conexión o metadatos relativos a las comunicaciones electrónicas: régimen jurídico de protección (haz de protección).
4) Privacidad como un derecho que no es absoluto; en particular, la tensión al enfrentar la privacidad con seguridad.
5) Ejemplo paradigmático de esta tensión afecta a datos de conexión: la obligación de conservación preventiva y cesión con fines de seguridad/penales (envés de protección): dos fases temporales de su régimen jurídico.
6) La incidencia del Tribunal de Justicia de la Unión Europea sobre esta obligación legal de conservación: actúa como «guardián» de la privacidad en detrimento de la seguridad, debiendo destacar dos sentencias: *Digital Rights Ireland* de 2014 (invalidez de Directiva específica), y *Tele2 Sverige* AB de 2016 (no conforme a Derecho europeo); que traen como consecuencia la afección de la Ley 25/2007 de conservación de datos de comunicaciones electrónicas, aún vigente y no modificada a este respecto.

De este modo, y una vez expuestos los apartados anteriormente reseñados, el Prof. Ballesteros Moffa, infiere de su estudio anterior las siguientes conclusiones.

Las normas de los Estados miembros de la Unión Europea sobre conservación preventiva y generalizada de datos generados o tratados en las comunicaciones electrónicas, al menos en su tenor literal, han recibido dos sacudidas de alcance por parte del Tribunal de Luxemburgo: primero, la declaración de invalidez de su Directiva 2006/24/CE de origen que, tras los atentados de Madrid y Londres, pretendía la obligatoriedad y armonización de esta valiosa técnica de lucha contra la delincuencia (STJUE *Digital Rights Ireland* de 2014); después, su propia disconformidad en cuanto resulten contrarias a las exigencias de proporcionalidad anticipadas en la primera Sentencia, pero a la luz del art. 15.1 de la Directiva 2002/58/CE, donde se reconocía ya con carácter general tal posibilidad en el marco de sus posibles excepciones (STJUE Tele2 Sverige AB de 2016).

Estamos ante el enésimo capítulo de tensión entre seguridad y privacidad, bajo el árbitro de la doctrina de limitación de los derechos fundamentales, sancionada por la Carta Comunitaria de Derechos Fundamentales.

Por cuanto la conservación y eventual cesión a las autoridades competentes de los metadatos son, en efecto, un claro exponente de limitación de los derechos y obligaciones de privacidad, traducidos para las comunicaciones electrónicas en forma de confidencialidad y supresión de los mismos tras el cumplimiento de sus funciones técnicas o exigencia de consentimiento para los tratamientos comerciales.

Todo ello en un momento de ambiciosa renovación (europea e interna) del régimen jurídico de los datos personales, a la vez que se hace más exigente desde esta perspectiva la lucha común contra la delincuencia organizada y el terrorismo, según evidencian la Directiva (UE) 2016/680 de policía y la Directiva (UE) 2016/681 de transferencia de datos PNR.

Ahora bien, más allá de la inaplicación o desplazamiento de las disposiciones de la LCD en virtud de la jurisprudencia analizada por el principio de primacía del Derecho europeo, lejos de considerarse fallida, no debe renunciarse a esta moderna herramienta de investigación, detección y enjuiciamiento de delitos graves. Recae en el legislador la importante misión de perseverar en ella, aunque ajustada a los requerimientos jurisprudenciales: sí conservación preventiva pero selectiva, pese a que la Propuesta de Reglamento sobre privacidad y comunicaciones electrónicas, en el contexto de las limitaciones por fines de seguridad, no recoge ya la previsión general de la posible conservación de los metadatos. Su retención y cesión han de seguir ilustrando la subordinación justificada de la privacidad a las exigencias de seguridad en un escenario internacional de creciente preocupación por la misma.

En suma, como ha reconocido la Corte Europea, el Derecho de la Unión «no se opone a que un Estado miembro adopte una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave» (apartado 108), asumiendo así la principal tesis de las conclusiones del Abogado General de que «una obligación general de conservar datos

es compatible con el régimen establecido por la Directiva 2002/58 y, por lo tanto, que un Estado miembro puede hacer uso de la facultad ofrecida por el art. 15, apartado 1, de dicha Directiva con el fin de imponer una obligación de esta índole. El recurso a esa facultad está, no obstante, supeditado a que se cumplan estrictamente los requisitos establecidos no solo en dicha disposición, sino también de las disposiciones pertinentes de la Carta leídas a la luz de la Sentencia *Digital Rights Ireland* […]» (apartado 116).

Hay que recordar que el art. 6 de la Carta no solo reconoce el derecho de toda persona a la libertad, sino también a la seguridad.

Lamentablemente, la amenaza del terrorismo y la delincuencia organizada a escala global no permite prescindir de ello, aun cuando haya que cohonestarlo con el menor impacto para los derechos afectados: el imprescindible para los objetivos perseguidos, en la permanente búsqueda de este delicado equilibrio.

Concluye el ponente, el Prof. Ballesteros Moffa, con la siguiente reflexión: El camino no pasa por arrumbar esta herramienta sino ajustarla a los requerimientos de equilibrio entre seguridad y privacidad, según la doctrina marcada por el Tribunal de Luxemburgo. Si a Jueces y Tribunales puede corresponderles la inaplicación total o parcial del régimen actual por su contradicción con el Derecho europeo, en el legislador recae la importante misión de mantener esta estrategia de seguridad, modificándola o renovándola según los requerimientos comunitarios.

Comentario de la relatora

Atendemos a la confrontación entre dos principios vertebradores, cuales son: la conservación de datos en pro de la seguridad y la propia privacidad de los ciudadanos. Principios que se articulan en un complejo marco normativo que afecta no solo a la Unión Europea y los Estados miembros, sino que podría alcanzar a los prestadores de servicios externos a la propia Unión.

A ello, hemos de unir los pronunciamientos del Tribunal de Justicia de la Unión Europea y el equilibrio que van a tener que realizar nuestros Tribunales domésticos para no contravenir al primero, pues nuestra normativa podría ser reclamada ante las instituciones europeas por entenderse contraria al derecho de la Unión.

Por último, la necesidad de trabajar por la armonización normativa en un momento de alerta máxima al observar un crecimiento en la delincuencia terrorista, en crimen organizado, etc., que a su vez merecen que sea constante la revisión de los principios de seguridad y de protección de datos de carácter personal.

QUINTA PONENCIA: «Aspectos legales de la robótica»
Ponente: Dña. María José Santos González, Coordinadora del Departamento Jurídico del Instituto Nacional de Ciberseguridad de España
Moderador: Prof. Dr. D. Pedro Álvarez Sánchez de Movellán, Profesor Titular de Derecho Procesal de la Universidad de León
Relatora: Dña. Cristina Llamas Bao, Abogada del Ilustre Colegio de Abogados de León, doctoranda de la Universidad de León (Área de Derecho Procesal del Departamento de Derecho Público)

Realizada la presentación del tema que va a exponerse por el Prof. Dr. D. Pedro Álvarez Sánchez de Movellán, cede la palabra a Dña. María José Santos González, quien se dispone a comenzar su ponencia señalando que la robótica es una materia que todavía está por construir y que tenemos que elaborar entre todos, no solo por parte de la ciencia, sino también por parte de los juristas, quienes tenemos que introducirnos en ella y empezar a plantearnos cuestiones para regularla.

Santos González explica que la ciencia de la robótica ha avanzado tanto que los robots, en ciertas tareas, ya son capaces de superar al ser humano, pues las realizan con mayor eficiencia y sin ningún tipo de error, pronosticando los científicos que, en un plazo de 20 años, los robots, la denominada «inteligencia artificial», va a superar a la inteligencia humana.

Quiere esto decir que los robots convivirán y colaborarán con nosotros con el objetivo de ayudarnos y mejorar nuestra vida, nuestro bienestar social. Tenemos bastantes dificultades, a nivel demográfico incluso, pues tenemos una pirámide invertida en la que nuestros mayores no van a tener quién les atienda en un futuro y, para eso, estaría la tecnología, para dar soluciones; y los robots podrían ser la solución.

Uno de los inconvenientes con el que nos encontramos es que ha existido un cierto recelo a la hora de regular la robótica. La ciencia entendía que regulándola se iba a limitar la investigación y con ello su desarrollo, pero se ha llegado a un punto en que este último es inevitable. Los juristas tenemos que abrir el debate de los derechos y la regulación de la robótica. No se trata de fabricar máquinas por fabricar máquinas, sino fabricar máquinas para que los humanos seamos más felices. En definitiva, lo que tenemos que regular es la sociedad de los humanos en la que se incluyan los robots con el objetivo de que nos ayuden a vivir mejor.

Santos González expone una fotografía de la película «El hombre bicentenario», inspirada en un libro de Isaac Asimov, genio y visionario de la robótica. Esta película muestra los diferentes interrogantes que pueden suscitarse en relación con los robots: sus derechos, cuestiones éticas, etc.; y algo que parece tan alejado y ficticio, no lo es tanto. Un informe del Reino Unido señala que en 50 años es posible que los robots estén reclamando derechos. Todavía no se ha llegado a ese paso, pero tenemos que ver qué sociedad queremos construir, alineando los diferentes intereses, esto es, los de los robots, los de las personas, los de la sociedad; en definitiva, buscar el bienestar común. Es cierto que tendremos que delimitar la ciencia, pero también definir qué

principios y qué derechos queremos que se recojan en nuestra sociedad y que la robótica tenga que respetar.

La robótica ha sido posible gracias al desarrollo de la tecnología, las matemáticas, la informática, la cibernética, el *machine-learning*, el *deep-learning* y, sobre todo, por el desarrollo de la inteligencia artificial. Esta última, fue señalada por Alan Turing en 1940 y en 1950. Este mismo matemático creó el llamado «test de Turing». Si una máquina superaba este test, se consideraba que podía pensar. Hoy en día las máquinas superan este test.

Continuamente recibimos nuevos hitos en relación con la inteligencia artificial. Podemos citar como ejemplos: el «*Deep-blue»* de *IBM*, máquina que ganó a Garri Kaspárov en un campeonato de ajedrez; «*Siri»*, de *Apple*, que es capaz de reconocer la voz y las palabras que manifestamos las personas sin conocernos; *«Watson»* de *IBM* que ganó a dos seres humanos en el concurso estadounidense *Jeopardy!*; o «Erica», un humanoide que es capaz de comunicarse y de mantener una conversación completa con una persona. También existen multitud de robots en nuestro mercado, como «HRP-4C», que es una modelo que es capaz de gesticular, «Atlas», que realiza tareas de búsqueda y rescate, *«Robocop»*, que puede poner multas, o *«Tom & Jerry»*, que preparan la mediación para pacientes en Gran Bretaña.

El avance tecnológico conlleva de manera irremediable una nueva regulación, siendo dos los aspectos que merecen ser objeto de estudio: por un lado, aclarar la confusión que pueda existir entre lo real y lo virtual y, por otro lado, la manipulación de la sociedad a través de la robótica, porque en el momento en que un robot tome una decisión e interactúe en el mundo puede condicionar al ser humano.

A día de hoy, hace falta determinar las normas a que debe ajustarse la robótica y la inteligencia artificial, ya que lo que hay regulado son normas técnicas. El objetivo es garantizar el control del hombre sobre estas máquinas, evitar su uso clandestino y asegurar el respeto de los derechos humanos. Las zonas geográficas más pioneras en esta materia son Corea del Sur, Japón, China, Estados Unidos y Europa.

Japón ha elaborado un informe para regular la sana conducta de la próxima generación de robots. En este informe, se plantea la creación de un Registro en el que se recoja cuál ha sido la conducta incorrecta de un robot, cuál ha sido el daño causado y cómo se debería reaccionar ante una situación así. Este Registro ha de ser público y transparente con el fin de se vayan conociendo los riesgos a los que nos estamos enfrentando a medida que la tecnología va avanzando.

En Corea, que es el país más robotizado del mundo (de cada 10.000 empleados 400 son robots y se espera que en el año 2020 haya un robot por cada hogar), se ha elaborado una Carta Ética que pretende regular la conducta de los robots.

En China, uno de los mayores fabricantes de robots, se está invirtiendo en materia armamentística y están interesados en los llamados robots asistenciales existiendo proyectos pilotos en escuelas y hospitales.

En Estados Unidos, en octubre de 2016 se crea un informe llamado «Preparando el futuro de la inteligencia artificial». También hay un Plan Nacional de Investigación en materia de Inteligencia Artificial, con grandes fondos de inversión económica para la integración de la robótica en todas las áreas de la vida, no sólo la industrial, sino la social y la doméstica.

De Europa se podría decir que estamos en la vanguardia en la implementación de normas sobre robótica y hay un gran interés en el desarrollo de la robótica. Esta apuesta de la UE se muestra con la formalización de un contrato de colaboración público-privada con una asociación en materia de robótica de 700 millones de euros para instalar robots en materia de construcción, ortopedia robótica, investigación en la operación conjunta robots y humanos en el trabajo y cómo el robot puede comprender el entorno e interactuar con él.

En relación con la normativa europea, la Estrategia Global de Política Exterior y Seguridad de la Unión Europea del año 2016 establece que tenemos que regular la biotecnología, la inteligencia artificial, la robótica y los aparatos pilotados a distancia con el fin de evitar riesgos de seguridad y aprovechar los beneficios económicos.

Ya en el año 2015 se crearon grupos de trabajo como el Grupo de Evaluación de las Opciones Científicas y Tecnológicas (STOA), que servirá de apoyo al legislador Europeo. En mayo de 2016 se elaboró un informe que contiene recomendaciones a la UE sobre normas de derecho civil de la robótica con el fin de «asegurar que los robots estén y sigan estando al servicio de los seres humanos». Estas recomendaciones fueron aprobadas por el Parlamento Europeo el 16 de febrero de 2017 y recogen las principales líneas de trabajo que deben afrontarse actualmente por el legislador al respecto, entre las que destacamos, por un lado, la creación de una Agencia Europea de Robótica e Inteligencia Artificial, es decir, un organismo que asesore a las autoridades públicas con sus conocimientos técnicos, éticos y reglamentarios en esta materia; por otro lado, la necesidad de un Código de Conducta Ético Voluntario, es decir, que los principios y derechos que queramos que rijan en nuestra sociedad sean llevados a la ciencia por los desarrolladores, fabricantes de los robots, etc., y lo implanten en sus programaciones, de tal manera que la robótica no pueda contradecir nuestro modelo de sociedad y asegurar que operen de acuerdo con las normas legales, de seguridad y éticas.

Otro aspecto importante es la responsabilidad de los robots, los *drones* y los automóviles no pilotados. Se necesita saber cuál va a ser la responsabilidad si se causa algún daño ya sea social, ambiental o de salud humana, porque estamos hablando de máquinas que se pueden desplazar por la vía pública, actuar de manera autónoma y sin supervisión del ser humano, incluso tomando sus propias decisiones una vez la inteligencia artificial avanzada sea una realidad.

También es necesario regular el régimen jurídico de los robots, pues se ha llegado a utilizar el concepto de «persona electrónica», para referirse a ellos; revisar el modelo de empleo y educación existente en la UE y ver si éste es compatible; y contemplar cuestiones de seguridad, pero no sólo desde un punto de vista técnico sino ético.

Con respecto a esta última materia, es decir, la seguridad, es necesario determinar qué pueden y qué no pueden hacer los robots. De la misma forma que los seres humanos tenemos reguladas determinas conductas que no podemos realizar (como vender droga, robar…) hay que dejar por escrito qué acciones son ilícitas y no pueden ser llevadas a cabo por los robots.

Recalca Santos González que la configuración legal actual de la responsabilidad civil no sirve para los robots a partir del momento en que estos actúan de manera independiente en el mundo, siendo muy difícil culpar al ser humano, titular de ese robot, de un daño causado por este. Será complicado probar el nexo causal entre la acción humana y el daño por actuaciones autónomas de los robots. Para estos casos, se están planteando diferentes posibilidades: o bien, que la responsabilidad sea del propio robot, o bien, que la responsabilidad atribuible al ser humano sea inherente a la gestión del riesgo, esto es, lo que pudo hacer un humano para controlar y evitar el daño. Se está hablando del establecimiento de un régimen de seguro obligatorio y un fondo común para cubrir los riesgos.

En el ámbito penal, también existen múltiples interrogantes, entre otros, si existe intencionalidad o dolo, qué impacto tendría para un robot una sanción, cuál ha de ser la sanción a imponer, si esta podría ser una desconexión, quién la puede realizar y en qué condiciones. La UE aboga por la posibilidad de que los robots incluyan interruptores para su desconexión en caso de emergencia.

En relación con las categorías jurídicas de los robots, hay que tener en cuenta lo siguiente: no se podrían identificar como personas físicas ya que los robots están al servicio y para ayudar al hombre y no pueden equiparse a este pues el art. 30 CC dispone que para ser persona has de desprenderte del seno materno. Tampoco pueden ser personas jurídicas porque cualquier acto de estas es adoptado por una persona física que la representa. Los robots inteligentes en cuanto que tienen autonomía y capacidad para tomar decisiones e interactuar con su entorno son algo más que simples cosas. Además, se prevé que se les dotará de ciertos derechos y obligaciones, facultades de las que carecen las cosas.

Para solventar esta dificultad, se prevé la creación de un nuevo estatus jurídico para estos robots denominado «persona electrónica», términos con los que no está de acuerdo Santos González por dos razones: primero porque no estamos ante una «persona» y, segundo, porque no estamos ante algo electrónico; la electrónica ya la hemos superado y ahora de lo que lo que toca hablar es la de inteligencia artificial. Considera que un concepto más adecuado podría ser el de «robot inteligente artificialmente».

Un elemento esencial para facilitar la implementación de las recomendaciones es la creación del Registro Europeo de los Robots Inteligentes.

Para Santos González el robot inteligente es un elemento esencial en materia de regulación de la robótica y tenemos que construir una seguridad jurídica en la que tendrían que colaborar tres niveles de juristas; juristas tecnológicos, juristas capacitados en materia de robótica, y científicos y técnicos con conocimientos en

Derecho. Precisamente con este marco de seguridad jurídica y seguridad técnica podríamos hablar de una innovación segura y fiable y de una revolución en materia de la robótica. Concluye su ponencia, a modo de reflexión final, con la siguiente cita de Isaac Asimov: «Es el cambio, el cambio continuo, el cambio inevitable, el factor dominante de la sociedad actual. Ninguna decisión sensata se puede hacer por más tiempo sin tener en cuenta no sólo el mundo tal como es, sino el mundo como será».

Comentarios de la relatora

A colación con lo anteriormente expuesto, en mi opinión, el empleo de los robots no deja de ser un tema que despierta interés y curiosidad, pero a la vez resulta inquietante. Se ha comprobado que los robots pueden llegar a ser más efectivos que el propio ser humano y se está investigando su incorporación en todas las áreas de nuestra vida. La duda que me surge es su integración en las Administraciones Públicas y más concretamente en la Administración de la Justicia. La rapidez y precisión de los robots podría acabar con la saturación de estas Administraciones, pero no deja de ser preocupante que expedientes administrativos y judiciales, queden en manos de estos seres. Antes de que esta situación se materialice, es necesaria una regulación no sólo europea, sino nacional, que fuera clara y detallada en lo que respecta al empleo de los robots.

Desde un punto de vista procesal, su empleo podría resultar útil en los procesos (tanto penales como civiles) y más concretamente como medio de prueba, incorporándose así al art. 299 LEC. La duda que me surge es si este robot se utilizaría como instrumento para probar un determinado suceso o si él mismo podría actuar en calidad de testigo o perito. Pero demos un paso más allá. Si los robots se diseñan para tomar decisiones ¿cabría la posibilidad de que existiese un juez robot?, ¿podría éste dictar una sentencia?, ¿no sería paradójico que un robot decidiese sobre la conducta de un ser humano? El tiempo nos dará la respuesta.

SEXTA PONENCIA: «Recogida, almacenamiento y tratamiento de evidencias digitales»

Ponente: D. César Lorenzana, Comandante Jefe de Tecnología y Apoyo Táctico del Departamento de Delito Telemáticos de la Unidad Central Operativa de la Guardia Civil

Moderadora: Dña. Marisol Aldonza Vivanco, Técnica del Departamento Jurídico del Instituto Nacional de Ciberseguridad de España

Relator: D. Francisco Xabiere Gómez García, Personal Investigador en Formación de la Universidad de León (Área de Derecho del Trabajo y de la Seguridad Social del Departamento de Derecho Privado)

La moderadora, Dña. Marisol Aldonza Vivanco, presenta a los participantes en la segunda mesa de trabajo, la cual va a versar sobre «La prueba electrónica», tras lo que cede la palabra al primer ponente, D. César Lorenzana, Comandante de la UCO, quien comienza su exposición afirmando que el Derecho se basa en certidumbres, mientras que el mundo de la tecnología lo hace sobre incertidumbres; pese a lo cual ambas materias están condenadas a entenderse.

Comparte la opinión de que internet no es una revolución tecnológica en sí misma, sino una revolución de revoluciones, pasando el reto actual por la gran cantidad de información a extraer. De este modo, urge repensar los modelos y los procedimientos de funcionamiento de la vida diaria, incluidos los jurídicos. El ejemplo sería la empresa *Kodak*, con una posición dominante en el mundo de la fotografía durante el siglo XX, pero que no supo adaptarse al mundo digital y acabó entrando en quiebra. Por ello, si el Derecho sigue como hasta ahora, corre el riesgo de desaparecer por no ser útil para las personas.

Entrando ya en la forma de adquirir las evidencias digitales, se plantea el problema de amoldar lo digital al plano físico, debiendo siempre tener muy presentes dos criterios, como son la incertidumbre y la gestión de riesgos. Es necesario comprender que muchas veces la información no está en el lugar físico de los registros policiales y se debe obtener en remoto. Hasta ahora la información estaba tras una puerta, en un lugar concreto al que, de una forma u otra, se podía acceder, pero el empleo de la fuerza en la actualidad ya no consigue derribar esa puerta; una puerta digital no depende de la fuerza, estando subordinado el acceso a los límites de seguridad que tenga la propia evidencia. Esto plantea el dilema de qué técnicas se pueden usar desde la legalidad para eludir esas barreras, como el uso de troyanos, por poner un ejemplo.

El siguiente problema es que si se puede acceder a través de una puerta digital, significa que se tiene privilegios de administrador, lo que permitiría crear o modificar las evidencias, por lo que será necesario auditar todo el proceso.

Otro interrogante que se va a plantear es quién tiene la jurisdicción sobre esa información o prueba, la cual puede estar segmentada, replicada desde varios lugares, recombinada o encontrarse en itinerancia. Sobre esta cuestión, la Comisión Europea está en camino de validar la pauta legal de que si se tiene acceso desde cualquier lugar de la Unión Europea a la evidencia digital (*e-evidence*) de un asunto criminal, también se tendría jurisdicción sobre la misma.

Por otra parte, continúa señalando D. César Lorenzana, es necesario normalizar la información para presentarla en una vista, dado que deberá ser comprensible para personas que no tienen la obligación de tener conocimientos informáticos. El tratamiento de la información plantea entonces diferentes retos, siendo el principal que se puedan duplicar las estructuras y sistemas en los que se manifestó la evidencia; de lo contrario, se corre el riesgo de visualizar e interpretar algo diferente a lo que realmente existe.

Un segundo desafío radica en conservar la evidencia sin manipular. Hasta ahora, la evidencia física se precintaba en una bolsa, en un procedimiento el cual garantizaba en un alto porcentaje su conservación, pero dicho recipiente no funciona con las evidencias digitales, pues un dispositivo electrónico puede seguir recibiendo reacciones electromagnéticas de no ser custodiado en las condiciones adecuadas. El Comandante Lorenzana pone el ejemplo de que cualquier teléfono se modifica a sí mismo al estar conectado a la red, sin necesidad de que ninguna persona lo manipule, lo que podría alterar el estado de la prueba original. En consecuencia, demanda una

norma que especifique el procedimiento a seguir, por ahora inexistente, ya que las evidencias físicas no lo precisaban.

El último de los problemas al que alude el ponente es que, en la actualidad, la pericial de un dispositivo cualquiera supone unos 30 terabytes de datos, lo que es inviable si consideramos que 4 terabytes equivaldrían a unas 1.700 lecturas de la Constitución. Por esto, el ponente propone definir primero qué se debe buscar en concreto y escrutar solo el tipo de información que sea relevante en el proceso específico (datos contables, comunicaciones, etc.), aplicando la gestión de riesgos en relación a una posible pérdida de la carga de la prueba.

Para concluir, el Sr. Lorenzana solicita la implicación de todos los actores responsables en la materia, desde el trabajo de las unidades de investigación hasta el esfuerzo del legislador, pasando por la necesaria dotación presupuestaria del ejecutivo, con vistas a modernizar el sistema de seguridad, para que no se siga regulando respecto de un mundo que ya no es la única realidad, mientras los delincuentes campan a sus anchas.

Comentarios del relator

Cuanto más se populariza el uso de instrumentos y aplicaciones basados en la informática, más comunes son las evidencias digitales y menos las físicas. Por ello, el ámbito del Derecho, en especial lo relacionado con el Poder Judicial, debe dar un paso adelante hacia una nueva concepción de la protección jurídica de las personas que, por otra parte, precisará de las aportaciones relevantes de distintas ramas del conocimiento. Ahora bien, concebir un nuevo marco ideológico y procedimental, en lugar de intentar adaptar a las nuevas realidades el utilizado hasta ahora, no debe desarraigar el Derecho de sus sólidos cimientos construidos de antiguo. Mantener las garantías legales en la era digital va a suponer más esfuerzo económico y en materia de personal de lo que venía siendo necesario hasta esta época. El reto está planteado, a la par que el tiempo vuela de forma inexorable. De la permeabilidad y pericia que demuestren poderes públicos y operadores jurídicos, dependerá que consigamos tener sociedades futuras más seguras y cohesionadas.

SÉPTIMA PONENCIA: «Recogida y presentación en juicio de pruebas digitales»

Ponente: Ilmo. Sr. D. Francisco Javier Gutiérrez Hernández, Fiscal de León
Moderadora: Dña. Marisol Aldonza Vivanco, Técnica del Departamento Jurídico del Instituto Nacional de Ciberseguridad de España
Relator: D. Luis Miguel Ramos Martínez, Personal Investigador en Formación de la Universidad de León (Área de Derecho Penal del Departamento de Derecho Público)

Para la séptima ponencia, segunda de las encuadradas en la segunda mesa de trabajo titulada «Recogida, almacenamiento y tratamiento de las evidencias digitales», los coordinadores del evento eligieron acertadamente al Ilmo. Sr. D. Francisco Javier Gutiérrez Hernández, Fiscal de León. La moderadora de esta segunda mesa, Dña. Marisol Aldonza Vivanco, del Departamento Jurídico del Instituto Nacional de

Ciberseguridad de España (INCIBE), tras hacer una breve presentación del ponente cede la palabra al mismo, quien comienza su intervención mostrando su agradecimiento a la Universidad de León por haber sido invitado a las Jornadas para hablar sobre la «Recogida y presentación en juicio de pruebas digitales». Anuncia también su intención de ser breve ya que, dada la activa participación del auditorio en los turnos de preguntas de ponencias anteriores, motivada por los interesantes temas tratados, su exposición comienza algo más tarde de la hora prevista.

Haciendo uso de una esquemática presentación de diapositivas proyectada para facilitar el seguimiento y compresión de su discurso, se introduce en la materia partiendo del concepto de prueba digital o electrónica, a saber: toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio, que pueda tener cierta eficacia en un procedimiento judicial abierto o susceptible de ser abierto. La susceptibilidad de apertura del procedimiento se refiere a la obligación de incorporar junto con la demanda, en el orden civil, estas pruebas (que no han de encajar necesariamente en la definición de documento electrónico) siempre que ya se disponga de las mismas en el momento de iniciación del procedimiento.

Tras definir el concepto de prueba digital, surge la necesidad de diferenciar entre otros dos conceptos básicos: la fuente y el medio de prueba. La fuente, la cual se identifica con la prueba en sí, es la información contenida o transmitida por medios electrónicos (una fotografía, un mensaje *SMS* o la grabación de un sonido); el medio, la forma de introducir dicha información en el proceso.

Ya haciendo referencia exclusiva al medio, el conferenciante recuerda la necesidad de atenerse a las reglas impuestas por la ley procesal civil extensivas a los procedimientos penales, contencioso-administrativos y sociales a causa de su supletoriedad reconocida en el art. 4 de la Ley de Enjuiciamiento Civil (en adelante LEC); concretamente al art. 299.2 LEC. Opina que en este precepto ya queda patente la conciencia del legislador del cambio que se estaba produciendo en las formas de comunicación y en general de interacción sociales[3] (ahora nos amenazamos por *WhatsApp* y no por carta o trabajamos con facturas electrónicas y no en papel). Este artículo es un llamamiento a la prueba digital: «También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso».

La exposición continúa con la enumeración de las características distintivas de las pruebas digitales: en primer lugar, son intangibles, pues se pueden reproducir o copiar con facilidad, diluyéndose las posibilidades de distinguir los originales de las copias (extremo este al que siempre se le ha dado mucha importancia en sede judicial debido a que el Juez ha de valerse de documentos auténticos a la hora de dictar una

[3] Este artículo ya formaba parte del texto original de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, por lo que el legislador no solo adaptó la normativa al contexto de entonces, sino que, en parte, previó la importancia de la incidencia de las nuevas tecnologías en los procesos judiciales.

resolución); en segundo lugar, son volátiles por mudables, inconstantes o, en definitiva, manipulables si se tienen los conocimientos suficientes; en tercer lugar, son delebles o destruibles, ya que pueden ser borradas o pueden destruirse los soportes que las almacenan; en cuarto lugar, son parciales, y ello porque, aunque no siempre, normalmente se encuentran en soportes físicos que están en poder de quien las presenta al procedimiento para respaldar sus pretensiones (pudiendo presentar solo lo que le interesa y obviar el resto); y el quinto y último lugar, son intrusivas, pues la recogida de las evidencias digitales, la mayoría de las veces, afecta a los derechos fundamentales plasmados en el art. 18 de la Constitución (en adelante CE), en especial a la intimidad personal, a la inviolabilidad del domicilio, al secreto de las comunicaciones y a la autodeterminación informativa en el ámbito de protección de datos de carácter personal[4]. En referencia a la última de las características enunciadas advierte que, en algunos casos, no se podrá valorar la prueba digital por lo dispuesto en el art. 11.1 de la Ley Orgánica del Poder Judicial (en adelante LOPJ) en materia de proscripción de la prueba ilícita; lo cual enlazará con aspectos que se tratarán más adelante.

Definidos y caracterizados los conceptos básicos, el ponente menciona ahora las dos modalidades de prueba digital ya adelantadas al hablar sobre la fuente probatoria: los datos o informaciones almacenados en un dispositivo electrónico (en los que la prueba digital es el propio dispositivo que se ha de poner a disposición judicial) y los datos transmitidos por cualquier red de comunicación abierta o restringida (como internet, una red de telefonía móvil, o en general por cualquier medio en un proceso de comunicación entre particulares o la información transmitida y almacenada por las redes sociales).

Su exposición se centra después en las fases de la prueba digital: obtención, incorporación y valoración.

La licitud de la obtención, primera de las fases, es, como ya dijo anteriormente, un requisito esencial para que la prueba sea válida. Por ello, si la parte procesal no tiene acceso a la prueba en cuestión deberá solicitar al Juez (al que está pidiendo que la valore y resuelva conforme a Derecho y, si es posible, conforme a lo solicitado), que supla la falta de disponibilidad y de voluntad de llevar la prueba al proceso, evitando así incurrir en supuestos de falta de consentimiento del sujeto afectado o falta de autorización judicial. Esto es común cuando los datos que se quieren incorporar al procedimiento no son los que se contienen en un dispositivo del solicitante sino en uno ajeno. La solución: una resolución judicial en la que se autorice la aprehensión de ese dispositivo. Esto puede realizarse mediante una autorización de entrada y registro (siendo ya habituales las imágenes en prensa de la Policía Judicial incautándose de los ordenadores de una entidad determinada), a través de la intervención de las

[4] Bastante antes que en el art. 299.2 LEC, el legislador constituyente plasmó ya la importancia de las nuevas tecnologías en lo que luego se llamó protección de datos de carácter personal (en consonancia con la tendencia internacional iniciada tras la Segunda Guerra Mundial), disponiendo en el art. 18.4 CE: «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».

comunicaciones (habitual en investigaciones de delitos contra la salud pública), por medio de los denominados controles remotos o aprehendiendo los datos de una página *web* que ha vulnerado derechos de las presuntas víctimas (o que simplemente son interesantes para un procedimiento penal o incluso civil).

Ya dentro de la fase de incorporación al proceso, el conferenciante repasa los requisitos que ha de cumplir una prueba (digital o no) para ser admitida y valorada por el Juez. Ha de tratarse de una prueba pertinente, es decir, vinculada directamente con los hechos que se trata de acreditar; pero también necesaria, sin que esa cuestión concreta haya sido ya debidamente probada a través de otros medios. Asimismo, la entrada de esa prueba (que debe de ser lícita) al procedimiento ha de llevarse a cabo a través de los medios probatorios establecidos en las leyes procesales, teniendo en cuenta las peculiaridades de cada uno de ellos y cumpliendo todos los requisitos procesales.

Acto seguido se refiere a las posibles formas de incorporación de las pruebas: mediante documentos en papel, documentos digitales o electrónicos, o a través de otros medios.

Para el primero de los casos cita la Sentencia del Tribunal Supremo (en adelante TS) 300/2015, de 19 de mayo, de la Sala Segunda de lo Penal, que fija los criterios para que el Juez tenga en cuenta la fuerza probatoria de las capturas de pantalla presentadas en papel. Esta resolución señala la necesidad de acreditar, por la parte que presente la prueba y mediante una pericial, la autenticidad (origen de los datos) e integridad (ausencia de modificaciones) de la misma, en caso de que estas características sean cuestionadas[5] por impugnación expresa de los documentos privados efectuada por la parte a la que perjudiquen; no obstante, la no aportación de una pericial instrumental no impide que el juzgador valore dicha prueba conforme a las reglas de la sana crítica y teniendo en cuenta el conjunto de pruebas presentadas.

Muy importante también es el uso de las actas notariales (documento público) que dan fe del contenido de un dispositivo digital o electrónico.

El apartado relativo a los documentos electrónicos lo inicia haciendo referencia a la definición del art. 3.5 de la Ley 59/2003[6]: «Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y

[5] Exigencias derivadas principalmente de los arts. 230.2 LOPJ y 217, 326 y 382.2 LEC; sin embargo, en la resolución mencionada (de la que fue ponente el Excmo. Sr. D. Manuel Jesús Marchena Gómez), en la que se recuerda la postura del TS respecto a que las conversaciones registradas no son pruebas documentales en sentido estricto a efectos casacionales, no se accedió a la casación solicitada aunque no se presentó una prueba pericial que avalase la autenticidad de la conversación, y ello porque la parte que la aportó puso a disposición del Tribunal *a quo* las claves para acceder a su cuenta de la red social *Tuenti* por la que se mantuvo la conversación, evidenciándose así que no tenía nada que ocultar y, además, la misma fue confirmada por los sujetos de la comunicación (emisor y receptor) mediante otras pruebas colaterales.

[6] De 19 de diciembre, de la Firma Electrónica.

tratamiento diferenciado […]» (regulación en la línea de las directrices dadas en su día por el Derecho comunitario[7]); pero señala también la existencia de otros conceptos relevantes a estos efectos como los recogidos en el art. 26 del Código Penal (que define documento para el orden penal englobando «todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica»), en el art. 24.2 CE (que eleva a constitucional el derecho «a utilizar los medios de prueba pertinentes para su defensa»), en el ya transcrito art. 299.2 LEC y teniendo en cuenta el mandato del primer párrafo del art. 230.1 LOPJ[8]. Además, hace mención a las copias de documentos electrónicos oficiales regulados en la Ley 39/2015[9], al concepto de información pública que recoge el art. 13 de la Ley 19/2013[10] y a la eficacia de las facturas electrónicas reconocida por el Real Decreto 1619/2012[11].

Para finalizar las formas de incorporación al proceso de la prueba, el ponente hace una breve mención a otros medios probatorios distintos de los documentos ya vistos, centrando la atención en el reconocimiento judicial y la idoneidad probatoria de poner a disposición del Juez los dispositivos electrónicos. Este podrá tener un mayor o menor conocimiento informático para saber si ha sido o no modificado, pero siempre puede acudir a pruebas periciales, tal y como dispone para el orden penal el art. 588 *sexies* c.1 de la Ley de Enjuiciamiento Criminal (en adelante LECr). Asimismo, alude a otras pruebas interesantes como la pericial mencionada, los interrogatorios (de parte o de testigos) colaterales y las técnicas de preconstitución extraprocesal (por medio de las actas notariales), de prueba preconstituida en el ámbito penal (a la que la LECr recurre en varios supuestos) o anticipada en el civil (arts. 293 a 296 LEC).

Sintiendo no poder terminar su exposición dedicando unas palabras a la valoración de la prueba (de la que, no obstante, hablará la última de las ponentes de la tarde), el conferenciante se despide agradeciendo la atención del auditorio entre los aplausos de los presentes y las palabras de gratitud de la moderadora en nombre de la organización. Más tarde, junto al resto de profesionales con los que comparte mesa de trabajo, responderá a las preguntas formuladas por los asistentes.

---

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

8 «Los Juzgados y Tribunales y las Fiscalías están obligados a utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establecen el Capítulo I bis de este Título, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y las demás leyes que resulten de aplicación».

9 De 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

10 De 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

11 De 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.

Comentarios del relator

El enorme cambio que los avances tecnológicos han supuesto en las formas de interacción humana, en especial en la comunicación, tiene ya su necesario reflejo en la legislación. La consideración de los nuevos medios de prueba digitales o electrónicos que hacen las leyes procesales y el enorme aumento del uso de este recurso en los procedimientos han transformado las actuaciones judiciales. Basta con reflexionar sobre el hecho de que, ahora, una gran parte de nuestras conversaciones son documentadas, pudiendo acudir a los archivos de los dispositivos de emisor y receptor o del servidor del canal de transmisión si necesitamos hacer uso de su valor probatorio.

Pero estos medios de prueba son resultado de la transducción a un lenguaje digital de otro tipo de señal analógica (por ejemplo eléctrica) que, en su origen, procede de fuentes reales: imágenes, sonidos o palabras escritas. Y este proceso de transformación caracteriza los medios de prueba digitales (intangibilidad y, sobre todo, mutabilidad), provocando que la información contenida en un medio electrónico o transmitida por dicho medio haya de ser tratada con mayores reservas, asegurando su autenticidad e integridad de la misma, bien mediante periciales o reconocimientos judiciales, bien mediante el uso de otras pruebas «clásicas» colaterales. Además, la incidencia en derechos fundamentales de los contenidos en el art. 18 CE añade a las anteriores garantías otras necesarias en su fase de obtención.

La irrupción de las nuevas tecnologías en la Justicia supone una modificación total del funcionamiento de las estructuras estatales de resolución de conflictos, tal y como evidencian, entre otros, el mandato del art. 230.1 LOPJ, la documentación de las actuaciones mediante sistemas de grabación y reproducción de la imagen y el sonido del art. 147 LEC o la obligatoriedad del sistema LexNET plasmada en el art. 273 LEC; requiriendo que se continúe con la adaptación del personal de la Administración y, en general, de los operadores jurídicos, quienes ya no podrán depender exclusivamente de técnicos especialistas externos para la obtención, incorporación y valoración de pruebas digitales.

Esto debería provocar (y ello sin hacer predicciones sobre las nuevas formas de almacenar o transmitir información que surgirán en un futuro) profundas revisiones legislativas que trasciendan de las operadas hasta ahora; «parches» que en ocasiones añaden aún más complejidad a las a veces decimonónicas normas que modifican (piénsese en la engorrosa técnica legislativa de adverbios numerales latinos utilizada en la LECr).

OCTAVA PONENCIA: «Aspectos procesales de la ciberseguridad: la prueba digital»
Ponente: Dña. Laura Fra Rodríguez, Abogada del Ilustre Colegio de Abogados de León
Moderadora: Dña. Marisol Aldonza Vivanco, Técnica del Departamento Jurídico del Instituto Nacional de Ciberseguridad de España
Relatora: Dña. Gracia Fernández Caballero, Abogada del Ilustre Colegio de Abogados de León, doctoranda de la Universidad de León (Área de Derecho Procesal del Departamento de Derecho Público), Colaboradora Honorífica de la Universidad de León

Tras la ponencia de D. Francisco Javier Gutiérrez Fernández, Fiscal de León, sobre «Recogida y presentación en juicio de pruebas digitales», la moderadora presenta a Dña. Laura Fra Rodríguez, abogada y miembro de la Junta de Gobierno del Ilustre Colegio de Abogados de León, dando paso a la misma para que nos introduzca en su conferencia, la última de las Jornadas, titulada «Aspectos procesales de la ciberseguridad: la prueba digital».

Esta ponencia se centra en la forma de aportación de la prueba digital al procedimiento judicial y la problemática que engendra en cuanto a la acreditación de su autenticidad y su posterior valoración por el juzgador.

Comienza Fra Rodríguez agradeciendo a la organización de las Jornadas su coordinación y el haber contado con ella para participar como ponente, agradeciendo asimismo a los Decanos, tanto de la Facultad de Derecho como del Ilustre Colegio de Abogados de León, ser partícipes en estas ponencias y fomentar la unión entre la Facultad y el Colegio Profesional. Tras los agradecimientos, la ponente hace alusión al escaso tiempo que le resta para desarrollar su ponencia, bromeando con la común expresión en Sala hacia los abogados «letrado vaya concluyendo su exposición, le quedan un par de minutos», y aduciendo que es consciente de que ella parte ya de ese par de minutos.

Inicia así la ponencia hablando sobre las cuestiones generales prácticas de la prueba digital; y que la conferenciante enmarca en, por un lado, los datos almacenados en un dispositivo electrónico y, por otro, en los datos e informaciones transmitidas a través de redes de comunicación como internet, telefonía fija o móvil, u otras.

La ponente aborda su conferencia haciendo hincapié en la problemática de la prueba digital desde el punto de vista de los abogados, que cuentan con lo que sus clientes les aportan, y ellos deben plantearse cómo pueden incorporar esos elementos probatorios en el procedimiento para que sean admitidos y valorados como prueba; a lo que se añade la problemática derivada de aportar esa prueba digital vía LexNET (plataforma que solo permite la aportación de ficheros en formato pdf, y tan solo texto e imágenes; y con un tamaño limitado). Ello supone que cuando la prueba no sea ni un documento de texto ni una imagen, deba anunciarse cómo se va a probar el hecho en cuestión, anunciar la aportación del documento digital de que se trate (vídeo,

sonido, metadatos, etc.) y, posteriormente, aportarlo debidamente en un CD o dispositivo válido que se llevará al Juzgado para su reproducción.

Pues bien, centra Fra Rodríguez las cuestiones prácticas de la prueba digital en tres aspectos: su obtención, su incorporación al proceso y su valoración.

Se hace hincapié en su incorporación al proceso bien en formato papel[12] mediante «pantallazos», bien como documento electrónico[13] a través de la incorporación de los datos obrantes en un soporte electrónico, resultando aplicable entonces lo previsto en los arts. 299.2 en relación con los arts. 382 a 384 LEC.

La aportación al Juzgado de esta prueba digital, ya sea vídeo, sonido o metadatos, como ejemplo, deberá poder ser reproducida en sala, lo que lleva al siguiente problema que plantea la prueba digital en la práctica, y es que la Ley procesal no establece en qué medios electrónicos o soporte concreto deben aportarse esas pruebas, siempre que se cumplan unos requisitos: que los mismos puedan ser examinados por el órgano jurisdiccional y las partes con pleno respeto a las garantías del debido proceso y que el Juzgado o Tribunal disponga de los medios técnicos necesarios para su práctica.

Destaca la ponente que los letrados deben anunciar en qué soportes van a aportarse dichas pruebas para que la Sala pueda reproducirlos; lo que en ocasiones lleva a situaciones en que el propio Juzgado manifiesta que no cuenta con medios técnicos adecuados para reproducir las pruebas en cuestión en Sala, y será el letrado interesado el que se encargue de poner a disposición de la Sala los medios idóneos para el visionado o reproducción de la prueba.

La ponente a continuación habla de la prueba digital referida a hechos sucedidos a través de diversas aplicaciones y redes sociales: *Twitter*, *Facebook*, *WhatsApp*, entre otros; y para cuya acreditación ante el juzgador deben aportarse las conversaciones, audio o imágenes enviadas a través de dichas aplicaciones de comunicación.

---

[12] Alude la ponente a la STS, Sala Segunda, 3300/2015, de 19 de mayo, que establece a este respecto: «Las conversaciones mantenidas, incorporadas a la causa mediante "pantallazos" […] no son propiamente documentos a efectos casacionales. Se trata de una prueba personal que ha sido documentada a posteriori para su incorporación a la causa. Y aquéllas no adquieren de forma sobrevenida el carácter de documento para respaldar una impugnación casacional. Así lo ha declarado de forma reiterada esta Sala […]».
«La impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido»

[13] El concepto de documento electrónico lo encontramos fuera de las leyes procesales, en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, en cuyo art. 3.5 se identifica estos documentos 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».

Estos medios de comunicación resultan sumamente polémicos a la hora de su aportación como prueba en un proceso judicial, toda vez que muchas de estas aplicaciones garantizan una privacidad que supone que, en teoría, no se archiven datos de comunicaciones entre usuarios, lo que redunda en un problema a la hora de acreditar la veracidad en integridad de la prueba. A esto se suma la facilidad en su manipulación; si bien existe ya jurisprudencia referente a la aportación de esta clase de comunicaciones al procedimiento, que refiere que deberá valorarse en conjunto con el resto de pruebas practicadas[14].

Hay que conocer cómo probar esta clase de hechos, que se suelen aportar siempre como prueba documental. Ahora bien, deben presentarse de modo que pueda comprobarse su veracidad. Hace alusión Fra Rodríguez a que aportar un «pantallazo» de una conversación no constituye una prueba digital en sí, sino una mera documental. Habrá que obtener copia de la comunicación según permita la aplicación en cuestión, y aportar ese archivo informático al proceso como documento; la ponente reproduce en pantalla una presentación de diapositivas en la que se explica cómo extraer de los dispositivos (*Android* e *iOS*) las conversaciones en diferentes redes sociales y aplicaciones. Destaca asimismo la importancia del acta de cotejo por el Letrado de la Administración de Justicia de los mensajes del teléfono cuya transcripción se aporte por el denunciante[15].

Conforme a las leyes procesales, quien alega el hecho debe probarlo como estime oportuno para acreditarlo; si bien puede que la prueba que se aporte sea impugnada por la parte contraria, porque entienda que no es veraz, que no es íntegra, que esté manipulada. Es entonces cuando la parte que alega el hecho debe acreditar su veracidad, reforzar su prueba, lo que en esta clase de supuestos lleva con casi toda seguridad a la elaboración de un informe pericial que analice y concluya si la prueba aportada ha sido manipulada o no, así como si incluye la comunicación completa (ya se dice por la jurisprudencia que se debe aportar de modo íntegro para su correcta valoración).

Alude la ponente a la aplicación *WhatsApp*, que con mucha frecuencia es utilizada y por ello suele ser fuente de prueba de conversaciones entre las partes que acreditan hechos objeto de un procedimiento judicial. El problema concreto de esta aplicación radica en que supuestamente no guarda las conversaciones en ningún servidor; lo que, por ejemplo, no sucede con otra similar, *Telegram*. Pregunta la ponente en este momento al auditorio, en el que se encuentran expertos y técnicos del INCIBE, si es verdad que esta aplicación no archiva las conversaciones de sus usuarios, lo que lleva a una grave problemática a la hora de acreditar hechos acaecidos a través de la misma. Responde por alusiones un técnico del INCIBE que confirma que *WhatsApp* no guarda en ningún servidor las conversaciones entre usuarios; ahora bien, puntualiza que el terminal sí las almacena. Plantea entonces la ponente si es posible que el usuario las borre y entonces no quede rastro que permita probar el hecho en cuestión,

---

14 SAP Madrid, Sección 27, de 24 de noviembre de 2015.

15 En esta ponencia se alude a la prueba digital en general, sin diferenciar una Jurisdicción concreta, por lo que existen alusiones tanto a la Jurisdicción civil, como a la penal, y a la social.

a lo que el experto del INCIBE responde que aunque se borren pueden ser recuperadas del terminal por un técnico y alude a que desde luego los técnicos del INCIBE sí lo han podido hacer. Agradece Fra Rodríguez la valiosa intervención de este experto, aludiendo a que precisamente esta participación es el espíritu de una mesa redonda como en la que se está; y la utilidad de su intervención pues, manifiesta la ponente que, en periciales privadas, se ha encontrado ante el problema de no poder acreditar fehacientemente la existencia y contenido de conversaciones mantenidas a través de esta aplicación.

Pasa la ponente seguidamente a hablar sobre la valoración de la prueba digital. A este respecto, la ponente parte de qué medios se pueden y deben utilizar para acreditar la veracidad de la prueba digital en cuestión, y más si ha sido impugnada. Alude a que el abogado debe ser consciente de ante qué clase de procedimiento está, pues si bien lo ideal es una prueba pericial informática, las mismas suponen un coste bastante elevado para los clientes, no debiendo olvidar que, a la hora de valorar esta prueba (que no deja de ser una documental privada), rige la libre valoración del juzgador, la sana crítica. Así, lo cierto es que en no pocas ocasiones, a través de testificales e interrogatorios de parte, se acaban reconociendo conversaciones que pudieran haber sido impugnadas o simplemente no reconocidas inicialmente; no debiendo perderse de vista que el juzgador hará una valoración conjunta de la prueba practicada en el procedimiento, por lo que el hecho puede quedar probado en función del resto de pruebas de las partes.

Señala la ponente otros medios de prueba, además del informe pericial, para acreditar estos hechos acaecidos a través de estos medios de comunicación modernos, como son las actas notariales, reguladas en el art. 198 y ss del Reglamento Notarial. Insiste la conferenciante en que, en este sentido, debe quedar clara la diferencia entre hecho y negocio jurídico. Una cosa es que se recoja un hecho en un acta notarial, a través de la apreciación mediante los sentidos del notario, y otra cosa es un negocio jurídico plasmado en una escritura pública, conforme al art. 17 de la Ley del Notariado.

Explica la ponente los requisitos que debe cumplir el acta notarial a efectos de una prueba digital, en cuanto al acta notarial sobre una *web*, destacando los siguientes elementos: tiene que constar el código fuente, ubicación del servidor en que se encuentra, la ruta de conexión, garantizar que el servidor hace su trabajo y que no se está sufriendo un ataque[16].

En cuanto a los medios probatorios adecuados para acreditar el contenido y autenticidad de una prueba digital, si bien se ha hecho alusión al mismo a lo largo de toda la ponencia, la conferenciante explica de manera más pormenorizada cuándo es necesario un informe pericial informático.

Así, resume Fra Rodríguez que el informe pericial informático es necesario indudablemente: cuando son necesarios conocimientos técnicos para acceder a la información; para acreditar la autenticidad o integridad del contenido de la

[16] Se hace alusión a un interesante artículo: «Bricolaje Notarial: Acta de página web para *dummies*», del Notario D. Javier González Granado.

información estableciendo de forma indudable el origen de la misma y su no alteración o manipulación; para desvirtuar la concurrencia de alteración o manipulación; para analizar el contenido de la información cuando sea necesario establecer la autenticidad de un software en delitos contra la propiedad intelectual; y para conocer fechas de modificación o creación de archivos o el origen y destino de la información enviada, entre otros.

Sobre las fases de la pericial informática, la ponente las enumera en: preservación, adquisición, análisis, documentación y presentación. Así, en cuanto a la obtención de los datos del informe pericial, se recogerán las circunstancias de la aprehensión del dispositivo, acceso al contenido o comunicación.

Es indispensable el clonado de los datos y el cálculo del *hash*. El clonado de los datos es la obtención bit a bit, de la información original en el mismo lugar en el que se encuentre el dispositivo. Es una copia física del contenido del dispositivo; siempre existirá el original y la copia del mismo, por lo que es esencial que no se borre el original, pues puede ser necesario un nuevo cotejo.

En cuanto al cálculo del *hash*: lo describe la ponente como «si fuese el DNI del documento», pidiendo permiso a los expertos informáticos presentes en la sala sobre si se puede explicar así, a lo que le dan su beneplácito; ofreciendo la ponente asimismo la definición técnica que se concreta en un algoritmo que permite afirmar que los datos que se encontraban en un dispositivo en el momento de su ocupación no han sido objeto de manipulación posterior. Debe indicarse el código *hash* del original y el de la copia.

Resalta la ponente la importancia de la cadena de custodia en la pericial informática: procedimiento oportunamente documentado que permite constatar la identidad, integridad y autenticidad de los vestigios o indicios de un hecho relevante para el asunto, desde que son encontrados hasta que se aportan al proceso como pruebas. Y que debe ser garantizada.

En conclusión, en la prueba pericial electrónica deben darse las garantías jurídicas a través de presencia de testigos y/o fedatario público (Notario o LAJ) y la utilización de un tercero de confianza para obtener un resultado positivo para nuestras pretensiones.

El interés de la intervención de Dña. Laura Fra Rodríguez quedó refrendado por el turno de preguntas posterior a su exposición y que cerró su participación en las Jornadas.

Comentarios de la relatora

La arrolladora evolución tecnológica en que la sociedad está inmersa incide en el mundo jurídico que, por tanto, debe adaptarse a ella. Destaca, como se desprende de esta ponencia, la relevancia de la evolución de los medios de comunicación: aplicaciones y redes sociales, cada vez fuentes de prueba más frecuentes.

La aportación de prueba digital, sobre la que ha versado la ponencia objeto de esta relatoría, aún es algo ciertamente novedoso; no tanto en cuanto a la frecuencia de su aportación a los procedimientos judiciales por las partes, como a su regulación legal y a su correcta presentación y valoración conforme a los requisitos que la misma necesita para que se acredite su veracidad.

Es cierto que la manipulación de esta clase de pruebas es hasta cierto punto sencilla, por lo que parece casi necesaria su impugnación por la parte contraria a quien alega los hechos que pretenden acreditarse mediante esa prueba digital. Ahora bien, tampoco debe perderse de vista que estamos ante una prueba documental y que si lo que se aporta es cierto, puede no interesar su impugnación, como ante cualquier otra documental privada.

A ello se añade la frecuente complejidad para que el propio órgano judicial valore una prueba de esta clase, pues conocer su veracidad e integridad rara vez se puede hacer sin un apoyo técnico y experto: un informe pericial.

De este modo, es destacable cómo los informes periciales informáticos se ensalzan como el medio probatorio más idóneo para confirmar la veracidad de las pruebas digitales y documentos electrónicos, si bien suelen resultar económicamente muy costosos y por ello no en todos los procedimientos judiciales son utilizados.

Con la interesante ponencia de Fra Rodríguez lo que desde luego se pone de manifiesto es que aún queda mucho por aprender en materia de prueba digital en general; y que por ello debe ser objeto de enseñanza específica a los alumnos de Derecho, así como a los propios letrados desde sus Colegios Profesionales y, desde luego, a los juzgadores. A juicio de esta relatora, debe promoverse un régimen legal más claro de estos medios de prueba que lleve a que su aportación y valoración resulte más sencilla de lo que lo es en la actualidad, pues, lo que es innegable es la relevancia y abundancia de las pruebas digitales, que necesitan una regulación más desarrollada, específica y clara, de aplicación a todas las jurisdicciones, que la que existe en la actualidad y que, hasta la fecha, se ve complementada por la jurisprudencia existente.