RELATORIAS DE LAS II JORNADAS NACIONALES DE DERECHO Y CIBERSEGURIDAD

Evento académico desarrollado los días 19 y 20 de octubre de 2016, en el Salón de Grados de la Escuela de Ingenierías Industrial e Informática de la Universidad de León, coordinado por D. Francisco Pérez Bes (Secretario General de INCIBE, Abogado, Especialista en Derecho TIC) y por Dña. Isabel Durán Seco (Profesora Contratada Doctora, Acreditada Profesora Titular, de Derecho Penal de la Universidad de León)

PRIMERA PONENCIA: "Escenario legislativo y tendencias regulatorias en el ámbito de la ciberseguridad"
Ponente: D. Francisco Pérez Bes, Secretario General de INCIBE, Abogado, Especialista en Derecho TIC
Modera: Dña. María José Santos, Abogada, Coordinadora Departamento Jurídico de INCIBE
Relatoría: Dña. Natalia Torres Cadavid, Investigadora predoctoral del Área de Derecho penal de la Universidad de León

Una vez concluida la Inauguración de las II Jornadas Nacionales de Derecho y Ciberseguridad, la moderadora de la primera ponencia, Dña. María José Santos González, presenta al ponente, D. Francisco Pérez Bes, y sin dilaciones le concede la palabra. El ponente comienza su intervención con una introducción sobre el momento histórico que estamos viviendo, en el que no estamos presenciando una serie de cambios sino, en sí mismo, un cambio de época. Explica cómo en la última década han surgido servicios que han cambiado el mundo, la manera de comunicarnos y la forma de hacer negocios, tales como Facebook, Twitter, YouTube, Uber, Airbnb, Snapchat, Instagram, Fitbit, Spotify, Dropbox, Whatsapp, Nest, Box, Hulu o Jet. Los cuales plantean serios e importantes retos sociales pero también retos regulatorios. El ponente explica que los retos regulatorios a los que en la actualidad se enfrentan los diferentes países están relacionados con la determinación de los límites que deben tener los avances cibernéticos y tecnológicos que cada día van aumentado en número. En particular se refiere a los siguientes avances y a los riesgos que llevan aparejados: a) el big data y los problemas de privacidad relacionados con su análisis; b) los drones y los problemas relacionados con la privacidad (en grabaciones por ejemplo), con los usos militares y riesgos de usos criminales y terroristas, y la incidencia en vuelos cercanos a infraestructuras críticas; c) los coches sin conductor y las dudas que plantea la posibilidad de su regulación, por ejemplo la moral de los algoritmos que se diseñan

para tomar decisiones, ¿cómo tomar la decisión entre atropellar tres peatones o colisionar con otro coche en el que viajan cuatro personas?; d) el llamado internet de las cosas y los riesgos relacionados con la privacidad, al tener toda clase de aparatos conectados a Internet, e incluso la seguridad de los usuarios; e) el *cloud computing* y las herramientas de cifrado para garantizar la ciberseguridad; f) los avances tecnológicos en salud y las dudas relacionadas con la ética de estas modificaciones en los cuerpos de las personas, además de ciertas preguntas que surgen en este contexto, por ejemplo, cuándo una máquina podrá tener estatus de ser humano. A continuación Pérez Bes se refiere al estado actual de la legislación señalando los diferentes cuerpos normativos, entre ellos el Código de Derecho de la Ciberseguridad que se trata de una compilación de normas que existen en España y que regulan la materia de la Ciberseguridad. La normativa sectorial, representada por la Ley General de Telecomunicaciones y la Ley de Servicios de Seguridad de la Información. La Directiva NIS para la seguridad de redes y sistemas de información, la cual le plantea a España importantes retos en materia de liderazgo en la elaboración de normativas europeas y en el proceso de trasposición a la legislación nacional. Y finalmente, el Reglamento General de Protección de Datos y el Reglamento de Identidad Electrónica y Servicios de confianza, que completan el marco regulatorio. Ahora bien, el ponente puntualiza que todos estos retos y esfuerzos regulatorios se encuadran en el marco estratégico de la ciberseguridad en España, el cual fue diseñado en el año 2013 y que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la estrategia de seguridad nacional en materia de protección del ciberespacio. Este documento se creó con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas. No obstante, precisa que más allá del ámbito de los ciberdelitos, que parece ser el contexto en el que se concentra toda la atención actual, la ciberseguridad también está relacionada con la prevención y con la reacción oportunas. Para terminar, Pérez Bes presenta los retos y oportunidades que plantea la ciberseguridad para el mundo de la abogacía: a) capacitación, formación y especialización para la gestión de oportunidades de negocio en asesoramiento jurídico en las empresas (en particular IICC); b) acciones de concienciación y difusión, como BYOD (Conan, Servicio antibotnet), herramientas gratuitas de INCIBE para identificar problemas de ciberseguridad en las terminales electrónicas; c) planes de *compliance*, lo que trasciende el campo del *compliance officer* en materia penal a otros ámbitos también (DPO – protección de datos); d) nuevas tendencias de investigación, por ejemplo en el Derecho de seguros, en los ciberdelitos y en el manejo de la privacidad; e) responsabilidad legal relacionada con la implementación de mecanismos de ciberseguridad (contractual, extracontractual, de los administradores); f) en el contexto de la responsabilidad social empresarial todas las buenas prácticas que se desarrollen en materia de ciberseguridad pueden transformarse en responsabilidad social empresarial; g) deontología profesional, en la protección del secreto profesional; y finalmente, e) en la Universidad como centro capacitador en demanda sofisticada "investigación", el ponente precisa que considera que la Universidad es el ámbito en el que deben abrirse espacios para formar a los futuros profesionales e investigadores que puedan satisfacer las necesidades del mercado en el ámbito de la ciberseguridad. Para discutir y establecer un marco de trabajo mutuo en este contexto, menciona el ponente, en el 2015 el INCIBE y el Consejo General de la Abogacía suscriben un acuerdo de colaboración, para la concienciación y preparación de los

abogados, en el que se trabaje en la difusión de las obligaciones, pero también de las oportunidades que da la ciberseguridad.

Comentarios de la relatora

En la actualidad nos encontramos ante todo un nuevo escenario de avances tecnológicos y cibernéticos que plantea serias dudas en materia de privacidad, seguridad y ética, el cual demanda un marco regulatorio que vaya al mismo ritmo y pueda dar respuesta a la incorporación de estos cambios a la vida cotidiana de las personas, al intercambio empresarial, a las actividades de los organismos no gubernamentales y a la acción de los gobiernos. La ciberseguridad es el mecanismo que permite hacer ese tránsito de manera razonable y segura, con medidas eficaces en materia de prevención y reacción ante ataques de la ciberdelincuencia, que cada vez es más sofisticada y potencialmente más dañina. El marco regulatorio se encuentra aún en ciernes, requerirá el esfuerzo común de todos los actores involucrados en el tránsito cibernético y, por ahora, plantea toda una serie de retos sobre los que hay que discutir intensamente desde diferentes perspectivas y ámbitos del conocimiento.

SEGUNDA PONENCIA: "Estado de la Ciberseguridad en España"

Ponente: D. Marcos Gómez Hidalgo, Subdirector de Servicios de Seguridad de INCIBE
Modera: Dña. Marisol Aldonza, Abogada, Departamento Jurídico de INCIBE
Relatoría: Dña. Nieves Alonso García, Personal Investigador en Formación, Área de Derecho Constitucional de la Universidad de León

La moderadora inicia su intervención señalando que la conferencia de D. Marcos Gómez Hidalgo es fruto del desarrollo de las tendencias en Ciberseguridad en torno a los incidentes surgidos en la Red. Asimismo, destaca el perfil profesional del ponente, que, entre otros, es miembro del Grupo de Expertos de Seguridad que asesoran a la ENISA (Agencia Europea de Seguridad de las Redes y de la Información de la Comisión Europea), Subdirector de Servicios de Ciberseguridad del INCIBE y profesor en los masters de Seguridad de la Información en diversas Universidades y responsable de Bases de Datos del ESNIC. Gómez Hidalgo comienza su exposición mencionando que es necesario conceptualizar la «Ciberseguridad» ante el establecimiento de la Estrategia General de Ciberseguridad, pudiéndose afirmar que su principal objetivo se centra en resolver la articulación de métodos de prevención y protección de la información en el Ciberespacio. Prosiguiendo en su ponencia, y conforme al título de la misma, se centra en dar respuesta a quiénes son los miembros del INCIBE, destacando que está compuesto por ochenta y cinco personas aproximadamente. El perfil más destacado en los trabajadores son ingenieros informáticos, de telecomunicaciones y de todas las ramas afines al ámbito cibernético, entre ellos, algunos alumnos de la Universidad de León. El marco jurídico sobre el que se asienta INCIBE es de Instituto Tecnológico financiado por los Presupuestos Generales del Estado. En España actualmente existen tres grandes entidades relacionadas de manera directa con el ámbito de la Ciberseguridad: el INCIBE; el

Mando Conjunto de Ciberdefensa, adscrito al Ministerio de Defensa y que da servicio a los tres ejércitos, cuyo cometido fundamental gira en torno a toda protección frente a cualquier amenaza ("ciberguerra") y el Centro Nacional de Excelencia en Ciberseguridad. En este contexto, las Administraciones Públicas poseen la obligación de cumplir con una base de protección de seguridad e información al amparo del Ministerio de Hacienda y Administraciones Públicas. De manera específica, el INCIBE trabaja en la protección de la privacidad de los usuarios, fomenta el establecimiento de mecanismos para la prevención y reacción a incidentes de seguridad de la información, minimizando su impacto en el caso de que se produzcan y promueve el avance de la cultura de la seguridad de la información a través de la concienciación, la sensibilización y la formación. Del cien por cien de los incidentes detectados por el INCIBE, aproximadamente el noventa por ciento es localizado por el Instituto, es decir, no es preciso que el usuario, una empresa o cualquier institución académica comuniquen tal suceso. Además, el INCIBE promueve en gran medida la formación a profesionales, así como la concienciación en la población; más en concreto, desde hace cuatro años, con la aparición de la Agenda Digital para España se fomentó la promoción e impulso de talento en ciberseguridad.

PRIMERA MESA DE TRABAJO:
"La protección del consumidor en la adquisición de productos y servicios en línea", Dña. Helena Díez García, Profesora Titular de Derecho Civil (Acreditada Catedrática) de la Universidad de León
"Derecho al olvido", Dña. Anabelén Casares Marcos, Profesora Titular de Derecho Administrativo de la Universidad de León
"Retos de la ciberseguridad en los nuevos mercados financieros (información privilegiada)", Dña. Elena Fátima Pérez Carrillo, Profesora Ayudante Doctora de Derecho Mercantil de la Universidad de León
"Tratamiento tributario de los nuevos medios de pago virtuales: las bitcoins", Dña. Marta González Aparicio, Becaria de Investigación FPU de la Universidad de León
Modera: Dña. Isabel Durán Seco, Profesora Contratada Doctora (Acreditada Profesora Titular) de Derecho Penal de la Universidad de León
Relatoría: Alfredo Alpaca Pérez, Investigador Contratado Predoctoral de la Universidad de León

La moderadora de la primera mesa de trabajo, Profesora Dra. Isabel Durán Seco, cede la palabra a la Profesora Dra. Helena Díez García, quien inicia su intervención señalando que en la actualidad existe una revolución jurídica en el marco de la regulación de la compraventa y de la prestación de servicios a distancia. Comenta la ponente que el 6 de mayo de 2015 la Comisión Europea presentó unas líneas de estrategia para el mercado único digital a nivel europeo. En ese marco, se calcula que creando un mercado único digital se puede incrementar el producto interior bruto de Europa en 250000 millones de euros (hay que tomar en cuenta que se cifran en 415000 millones de euros el coste de no existir ese mercado único digital). La ponente señala que para crear ese mercado único digital la estrategia que se plantea desde la Comisión consiste en incrementar los mecanismos que refuercen la confianza de los consumidores en el mercado digital y que también se favorezca la seguridad jurídica

de las empresas en ese mercado único digital. La Comisión Europea, ya a principios de diciembre de 2015, presentó dos iniciativas legislativas como son la propuesta directiva que regula determinados aspectos de los contratos de compraventa en línea y otras ventas a distancia de bienes y la propuesta directiva específica sobre la contratación de suministros digitales en línea. De momento, estamos en fase de propuesta y no existen otras iniciativas al respecto (que se hayan cristalizado en una directiva comunitaria). Con las directivas se buscan incrementar las transacciones electrónicas. Por otra parte se observa que los consumidores podrían operar en línea y podrían ahorrarse hasta 11000 millones de euros. Por tanto, según Díez García, es necesario favorecer la confianza de los consumidores en estos mercados, sobre todo para que los consumidores y las empresas se abran al mercado transfronterizo. La ponente se refiere seguidamente a los instrumentos que se utilizan o se van a utilizar para potenciar ese mercado único digital. Estos son los instrumentos legales que colmen los vacíos existentes en estos momentos en la legislación europea y en la de los Estados miembros. Al respecto, según Díez García, se observa una gran disparidad en materia de remedios frente a la falta de conformidad y se observa también un absoluto vacío legal en la regulación de la compra venta de contenidos digitales. Con respecto a la regulación actual, la ponente señala que, sin perjuicio de que exista una regulación sectorial (por ejemplo en materia de contratación a distancia de servicios financieros), existen en el marco europeo la Directiva de 2000 sobre comercio electrónico (que fue transpuesta a través de la Ley 34/2002) y la Directiva 2011/83 que se refiere a los derechos de los consumidores (que fue transpuesta a través de la Ley 3/2014 que vino a reformar la regulación de la contratación a distancia en el seno del texto refundido de la Ley General para la defensa de consumidores y usuarios). Díez García incide en que la normativa de la Ley 3/2014 del texto refundido se aplica a contratos a distancia (únicamente contratos que se formalizan sin la presencia simultánea de las partes contratantes), siempre y cuando una de las partes sea consumidor (es decir, que actúe al margen de una actividad profesional o comercial) y un empresario. Quedan al margen de esta normativa los contratos a distancia que se perfeccionen, por ejemplo, entre profesionales que se rigen exclusivamente por la Ley 34/2002. Díez García ahora se concentra en el texto refundido de la Ley General para la defensa de consumidores y usuarios. Hay determinados aspectos que se regulan en la directiva y por lo tanto en la legislación interna de transposición que han permitido alcanzar una cierta uniformidad a nivel europeo en estos ámbitos. Y estos ámbitos son los que precisamente no se van a tocar en las proposiciones de directiva antes señaladas. Estos aspectos son: los referidos a la información precontractual, a los requisitos formales del contrato, al derecho de desistimiento que le asiste al consumidor, a la ejecución del contrato en relación con los periodos de entrega, los pagos adicionales, la transmisión del riesgo. El artículo 97, acogiendo lo que dice el artículo 7 de la directiva, obliga a todo empresario que actúe a distancia u ofrezca servicios o productos a distancia. Conforme a esto, le impone el deber de ofrecer una información precontractual antes de que el consumidor quede vinculado. Por tanto, la información debe ofrecerse, precisamente, antes de que se perfeccione cualquier contrato. ¿Cómo se debe informar? La ponente señala que el texto refundido dice que debe informarse "de forma clara y comprensible". ¿Cuál es el contenido de la información? Díez García señala que se trata de un contenido excesivamente (a veces) detallado. En primer lugar debe identificarse qué es lo que se contrata (características del bien o del servicio, por ejemplo). Se tiene que identificar la persona con la que se

contrata. Se tiene que determinar cuánto debe pagarse por el producto o servicio (el precio y todos los costes adicionales). Se tiene que determinar cómo se va a ejecutar el contrato (en qué plazos, el lugar de la realización de la entrega, por ejemplo). En qué lengua se va a contratar. Se señala también si asiste o no al consumidor un derecho de desistimiento y como se puede ejercitar. Asimismo, se debe establecer si existen códigos de conducta por parte del empresario, la duración del contrato, las condiciones de resolución del contrato, si hay garantías financieras y cuáles son los mecanismos de resolución extrajudicial de controversias. ¿Cuál es el valor de la información? La ponente señala que todo este deber de información es lo que formará parte del contenido del contrato. Por tanto, la virtualidad de esa información es determinar cuáles son los derechos y obligaciones de las partes, lo cual es conforme con lo que dispone el artículo 65 del texto refundido. Por otro lado, el artículo 98 señala que el empresario tiene el deber de facilitar al consumidor o de poner a su disposición esta información obligatoria, lo cual se realiza conforme a las técnicas a distancia utilizadas en la contratación. Según Díez García, cuando la ley habla del "deber de facilitar" indica que el empresario tiene el deber de colocar a la información (¿apta?) para que el consumidor pueda acceder a la información. En ese sentido, según la ponente, los términos utilizados en la ley deben ser entendidos como "accesibilidad a la información". No es importante que luego el consumidor acceda a la información, pues una vez que se suministra diligentemente por el empresario el hecho de que el consumidor no consulte esa información es irrelevante: él asume el riesgo de no acceder a la información. Es evidente que la información se debe proporcionar al consumidor antes de que este quede vinculado, esto es, antes de que el contrato se perfeccione. Esa antelación vendrá marcada por el medio a distancia que se utilice para la contratación (no es lo mismo vía internet que SMS, por ejemplo). De esta forma, según Diez García, la Ley nos habla de que para el comerciante tampoco tiene que suponer una carga excesiva facilitar esa información al consumidor. Aquí se emplea, para medir la diligencia del profesional, los criterios de razonabilidad y en términos de buena fe. La buena fue impone a las partes en la contratación un deber de lealtad recíproco, por lo que si bien el empresario tiene que suministrar la información pertinente, lo debe hacer en forma de lo que razonablemente él debe confiar en lo que debe conocer un consumidor. En esa línea, la información ha de resultar comprensible para el consumidor. Esto supone que se realice en términos de lo que razonablemente puede esperar un comerciante que actúa de buena fe en el mercado en relación con la diligencia que puede esperarse de un consumidor medio. El comerciante debe adaptar las condiciones de la información. Tiene que tener en cuenta cuáles pueden ser las circunstancias personales del grupo o del consumidor medio al que pertenece el grupo al que destina la oferta comercial o la oferta de contratación. Pero también tiene que tener en cuenta que puedan existir colectivos que por sus circunstancias no tengan tan fácil acceder a esa información. Al respecto, el Parlamento Europeo, en resolución de 22 de mayo de 2012, sostiene que se ha de atender a las condiciones del consumidor vulnerable en la contratación. La vulnerabilidad puede venir dada la dificultad de acceder a la información, de comprenderla o de la imposibilidad de acceder a internet de ese consumidor. Con respecto a la lengua, la ponente señala que si bien en el marco europeo se da absoluta libertad a los Estados miembros al respecto, el legislador español ha considerado que cualquiera sea la lengua que se utilice en la oferta o en la información precontractual o la contratación, tiene que ser siempre comprensible para el consumidor, además de que siempre se requiere la utilización del idioma castellano.

Aquí, sin embargo, debe destacarse que lo importante no es que se utilice el castellano, sino que se comprenda el contenido de la información que se entiende como obligatoria. Por otro lado, la Ley, siguiendo a la directiva, trata de adaptar el cumplimiento de sus presupuestos normales de los contratos a distancia a las herramientas que se utilizan en la contratación. Por ejemplo, se tiene en cuenta la posibilidad de que se utilice una herramienta a distancia que limite el espacio y el tiempo para facilitar la información (ofertas contractuales vía televisión, vía SMS). En este supuesto, lo que determina el texto refundido en su artículo 98, es que el empresario puede facilitar una mínima información y remitirse a otra fuente de información donde serán facilitados al consumidor todos los datos que conforman el contenido obligatorio de la información según el artículo correspondiente. Pero en esta nueva fuente de información esta debe ser accesible y comprensible para el consumidor. Por otra parte, en los contratos electrónicos a través de sitios web, en principio el legislador comunicatorio comenzó diciendo que no había ninguna dificultad para que a través de las páginas se web se suministre toda la información considerada como obligatoria. Sin embargo, sí se preocupa en el hecho de que, cuando se utiliza la web para contratar, al realizarse el procedimiento de manera rápida, el consumidor puede alegar luego un desconocimiento de algún aspecto de la contratación (por ejemplo, algo que el consumidor debía pagar pero que no sabía que tenía que hacerlo). Por ello, lo que exige la ley, siguiendo el criterio de la directiva, es que, antes de contratar, el comerciante tiene la carga de determinar en su propia página web que aquello que pide el consumidor supone una obligación de pago. Por otro lado, se tiene que informar al consumidor si se aplican o no restricciones a la entrega del producto (por ejemplo, que el producto esté condicionado a la disponibilidad de existencias, por ejemplo). Por esto, si no se produce la entrega, habrá lógicamente un incumplimiento de contrato, con lo cual el consumidor podrá resolver ese contrato y en su caso solicitar la indemnización por daños y perjuicios correspondiente. Con respecto a las formas de pago, según la ponente, pasa lo mismo: el comerciante debe informar al consumidor los medios de pago admitidos. En ese sentido, si no dice nada, el consumidor será libre para determinar la forma de pago sin que el comerciante pueda rechazarlo. Díez García señala seguidamente que en relación con los contratos electrónicos, aunque no se dice nada en el texto refundido, ni tampoco en la Directiva, parece obvio que el comerciante tiene que facilitar al consumidor cuáles son las condiciones generales que van a regir el contrato. Eso queda más claro, según la ponente, en el artículo 27 de la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico. Se señala que antes de contratar, el comerciante tendría que facilitar al consumidor o al adherente una copia de las condiciones generales de contratación que lo van a vincular. Por otro lado, las condiciones generales forman parte de la información obligatoria, con lo cual no es suficiente con que estén en la página web, sino que tienen que estar accesibles, es decir, no pueden estar ocultas o mostrarse de forma equívoca (en el apartado de "ayuda", por ejemplo). Si esto se produce, no se cumplirían las exigencias del artículo 5 de la Ley 7/1998, sobre Condiciones Generales de la Contratación. Díez García señala que es una cuestión clave el hecho de que el empresario tenga la carga de confirmar el contrato con el consumidor mediante un soporte duradero. El contenido de esa confirmación depende de si previamente le ha facilitado la información obligatoria exigida por la ley, el soporte duradero o no. En todo caso, la confirmación debe proporcionarse en un soporte duradero. Un "soporte duradero" se define en el 59

bis del texto refundido. Un soporte duradero es todo aquel elemento que permite almacenar o guardar la información, que no se pueda manipular, que se pueda reproducir y que permita la conservación de los datos durante el tiempo del contrato. No se considera un soporte duradero, según el Tribunal de Justicia de la Unión Europea, la propia web del comerciante, pues en este no hay garantías que la información no se pueda manipular por parte del comerciante. Las páginas web normales no constituyen ningún soporte duradero, aunque sí lo pueden ser, según la ponente, los correos electrónicos o los mensajes de texto (SMS).

Posteriormente, toma la palabra la Profesora Dra. Anabelén Casares Marcos, quien comienza su intervención señalando que el denominado "derecho al olvido" es un derecho de nuevo cuño, fundamentalmente jurisprudencial pero que ya ha tenido cierto reconocimiento normativo. La evolución constante e imparable de las nuevas tecnologías (y su prácticamente ilimitado potencial para el tratamiento de información o datos personales), supone una amenaza o por lo menos pone en serios aprietos la capacidad de los ciudadanos de controlar toda la información personal que se refiera a ellos o que les afecte. Junto a las dificultades reconocidas por el desarrollo tecnológico, se suma la ausencia de respuestas para la solución de posibles controversias de trascendencia jurídica (del derecho comparado o del derecho internacional). Los ataques que tienen como objeto la información o los datos personales no sabe de fronteras: son agresiones esperables y explicables en el contexto socio-económico actualmente vigente en el que la información se erige, cada vez más, en instrumento de poder y en valor de cambio, desatando un voluminoso y difícilmente controlable tráfico de información. En este contexto el debate sobre el derecho al olvido brota a partir del denominado "efecto eterno" de la información en internet, fruto de la memoria total de la red. Casares Marcos señala que el derecho a la intimidad en su vertiente de derecho de "ser dejado en paz", ha evolucionado como un nuevo "derecho al olvido". Así, las diferentes instancias de protección de derechos se han enfrentado en los últimos tiempos a múltiples solicitudes de personas que exigen que sus datos sean retirados de páginas web, de directorios, de hemerotecas o de listas de resultados de búsquedas en internet. La ponente señala que las respuestas jurídicas sobre estos asuntos no son en absoluto simples. La normativa, aunque joven, ha supuesto muchos problemas para los tribunales en los que ha sido aplicada, pues los problemas que pretenden ser solucionados poseen una gran dinámica que les permite evolucionar con gran rapidez, en buena cuenta debido a que emergen en el marco de herramientas tecnológicas que a su vez suponen una importante complejidad. Casares Marcos señala que el derecho al olvido digital, de creación jurisprudencial, podría definirse como el derecho que tienen las personas físicas, cuyos datos han accedido a los buscadores de páginas web en internet, a que tales datos desaparezcan de los buscadores, de tal modo que no resulte viable seguir encontrando informaciones antiguas y/o desactualizadas que tras un periodo de existencia en la red, resulta justificado que el sujeto afectado solicite su desaparición. En este marco, muchas personas aparecen como involucradas en el posible conflicto (editor, el motor de búsqueda, el internauta, el propio protagonista, afectado o interesado). Esta diversidad de protagonistas se traduce, a su vez, en una gran diversidad de derechos afectados (protección de datos personales; honor, intimidad y propia imagen; integridad física o psíquica; dignidad humana y libre desarrollo de la personalidad). No existe ningún derecho absoluto, por lo que un posible conflicto

conlleva necesariamente a una ponderación de derechos para determinar cuál de ellos debe prevalecer en el caso concreto. Desde una perspectiva material, el ejercicio del derecho al olvido puede proyectarse sobre dos tipos de contenidos: ilegales o legales. Casares Marcos dice que sobre los primeros se referirá muy poco, pues se encuentra suficientemente garantizado el ejercicio del derecho al olvido (de supresión o cancelación). Su materialización pasaría por acudir a la Agencia Española de Protección de Datos o a la vía judicial oportuna para ver protegido el correspondiente derecho (normalmente el derecho al honor, a la intimidad o a la propia imagen). La legislación española establece que si los contenidos son manifiestamente ilegales, no es precisa una sentencia judicial o una resolución administrativa para solicitar al buscador la retirada del contenido en su lista de resultados. Mucha más compleja es la situación con los contenidos legales: aquellos contenidos cuya publicación en principio resulta inocua, cuando no incluso exigida por una norma jurídica. Pero el interesado, pasado el tiempo, desearía haber eliminado de internet. Según la ponente, el contenido que uno desea eliminar de internet es normalmente información pretérita, cuya publicación estuvo justificada en un momento dado, pero que ya ha perdido actualidad, interés y cuya inmediata disponibilidad es considerada por el perjudicado como gravosa, máxime cuando es extemporánea y aparece como uno de los primeros resultados de un buscador en la web, al ingresar el nombre y los apellidos de una persona en dicho buscador. En España, las publicaciones que con mayor frecuencia han sido objeto de petición de olvido son de dos tipos: 1) noticias de periódicos ubicadas en hemerotecas (cuya digitalización las mantiene siempre accesibles); y 2) resoluciones judiciales y administrativas cuya publicación en los boletines oficiales muchas veces es preceptiva, a tenor de la normativa aplicable. Casares Marcos señala que el Tribunal Supremo ha tenido la oportunidad de perfilar los límites del derecho al olvido. Así, procede apreciar el derecho el olvido aunque el tratamiento de los datos pueda ser veraz, siempre que, no obstante, haya transcurrido tiempo, no tenga actualidad, no tenga interés, o inclusive pueda tener un efecto estigmatizador sobre el sujeto en la sociedad (sobre su inserción en la sociedad). El Tribunal Supremo llama la atención sobre que el derecho al olvido no significa un derecho del sujeto a "construir" un pasado a su medida, de tal manera, que no consiste en un derecho a impedir la difusión de cualquier información sobre hechos que no consideremos positivos ni tampoco justifica que se pueda solicitar la construcción de un currículum a la medida. El derecho en cuestión solamente justificaría la petición de los afectados de que los responsables de las hemerotecas digitales adoptaran medidas tecnológicas para que la página web de la hemeroteca digital en la que aparece esta información obsoleta y gravemente perjudicial no pueda ser indexada por los buscadores. Sin embargo, sí continuaría estando presente en la hemeroteca digital e incluso podría ser indexada por un buscador interno de la propia publicación, ya que entiende el Tribunal Supremo que en caso contrario se estaría restringiendo de manera excesiva la libertad de información. Casares Marcos hace referencia a continuación a la aprobación del nuevo reglamento de la Unión Europea 2016-679 de 7 de abril, relativo a la Protección de las Personas Físicas frente al Tratamiento de sus Datos Personales. El derecho al olvido se encuentra en el artículo 17, que se define como el derecho del interesado "a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales" al concurrir las circunstancias que el propio artículo señala. En todo caso, señala la ponente, el ejercicio del derecho de supresión por parte del

interesado recae sobre el editor del contenido, quien posee la obligación de informar sobre el particular a los buscadores, para que dejen de indexar y esos enlaces dejen de estar disponibles. Ha de facilitar, para ello, todos los medios que sean tecnológicamente razonables y las técnicas que puedan resultar oportunas, a fin de eliminar todos los enlaces a esos datos o cualquier copia o réplica de los mismos. Se refuerza con ello claramente (ahora ya en el plano normativo), el derecho al olvido en línea que ha venido sancionando y reconociendo la jurisprudencia tanto comunitaria como interna. El propio artículo 17 reconoce excepciones y admite que la normativa comunitaria como la de los Estados miembros recojan limitaciones acerca de los contenidos que puedan exigirse que sean borrados o suprimidos de internet. Interesante es al respecto lo señalado en el artículo 82 del reglamento, que establece un derecho de indemnización y responsabilidad por la infracción del mismo, y dentro de este, del precepto referido al derecho al olvido. Finalmente, Casares Marcos señala que, a la luz de los recientes pronunciamientos normativos y jurisprudenciales, europeos y nacionales, se ha llegado a cuestionar, incluso, la propia conveniencia de mantener la expresión de "derecho al olvido". Primero, porque garantizar realmente el "olvido" es prácticamente una tarea imposible. Segundo, porque la denominación "derecho al olvido" ha sido utilizada para hacer referencia a pretensiones muy diferentes y casi siempre mucho más amplias de lo que los propios tribunales han reconocido, suscitando así una gran confusión. El derecho al olvido no supone un derecho de cada usuario a borrar toda la información que considere pertinente y que ha ido dejando con el tiempo en la propia red, sino que solo consiste en la capacidad de exigir la eliminación de uno o varios resultados de una lista ofrecida por un motor de búsqueda a partir del propio nombre, cuando tal sujeto desea que no sea mostrado, siempre que consiga demostrar que no existe un interés público prevalente en que se mantenga disponible y accesible para los internautas. En la doctrina han surgido algunos esfuerzos por intentar renombrar esta variante concreta del derecho de supresión, por ejemplo, "derecho a la oscuridad digital", que pondría un mayor énfasis en los efectos reales del mal llamado "derecho al olvido".

A continuación inicia su ponencia la Profesora Dra. Elena Fátima Pérez Carrillo, quien anuncia que abordará el tema de la ciberseguridad y mercados financieros, para lo que señala que, si bien su ponencia posee algunos aspectos comunes con las ponencias precedentes, se diferencia de las mismas en que abordará la relación con contratos o contrataciones en los que intervienen profesionales (y no tanto consumidores). También señala, con respecto a la posibilidad del denominado "derecho al olvido", que estamos en un ámbito en el que hay que evitar el olvido o, en todo caso, a permitir registros de bastante duración. También en este aspecto, en relación con los mercados financieros, es necesario subrayar, según la ponente, que nos movemos en el límite entre la regulación administrativa y la regulación civil o mercantil. Los sectores financieros que destaca la ponente son tradicionalmente banca (mercado de valores, mercado de commodities y seguros). Todos ellos tienen planteado como uno de sus grandes retos, precisamente, el de la ciberseguridad. En materia de banca (la banca móvil, el mercado de divisas Forex, las transferencias digitales) prácticamente se está cambiando el modelo o el negocio y de hecho se ven los cambios que conducen a todos, precisamente, a una nueva banca. En materia de mercados, la cuestión de las anotaciones en cuenta de las acciones es ya muy antigua, aunque es relativamente nuevo el tema de los algoritmos (que las órdenes se procesan

mediante fórmulas matemáticas). Bastante más novedoso son los *traders*, los algoritmos de alta velocidad, donde las órdenes se transmiten de una manera prácticamente automática y que responden a sistemas programados por adelantado. Las plataformas de financiación (sobre la que existe regulación en España, la Ley 15 de 2015), pero sobre todo (responderían a mercados regulados de bolsas de valores) mecanismos de negociación y sistemas organizados de contratación (SOC), que son sistemas donde se negocian commodities. Estos últimos están evolucionando de forma muy rápida y configurándose en buena medida todavía hoy en día. Junto a lo señalado, Pérez Carrillo señala que en los seguros también tenemos muchos ejemplos (contratación, comparadores, contrataciones on line, seguros ad hoc). Dentro de lo que serían los mercados, dentro de los servicios financieros el aspecto de mercados, los bursátiles, mercados no bursátiles, mercados alternativos, mercados secundarios, mercados de commodities. Dentro de estos mercados hay dos tipos de sujeto o dos tipos de riesgos, todos ellos sometidos a ciberataques de formas diferentes. Por un lado, las infraestructuras, por otro, los intervinientes. En los intervinientes están los gestores, los emisores, los intermediarios (directos o indirectos) y los inversores. Todos estos intervinientes están sometidos a una fuerte regulación española y europea. Esta regulación, debido a la crisis económica de 2007, se está actualizando. En estas reformas (después de 2007) se están introduciendo algunas medidas que tienen que ver con la ciberseguridad. Por el otro lado la ponente destaca la existencia de las infraestructuras: las sociedades gestoras, las plataformas y las conexiones. Seguidamente, Pérez Carrillo comenta que detrás del conocido "*Flash Crash*" de 2010, parece haber existido un ciberataque muy peculiar: originado por operadores internos o *insiders* (de alguno de los agentes mencionados anteriormente). Esto conduce a pensar que además de las medidas técnicas, hace falta reflexiones y medidas estratégicas para conocer las vulnerabilidades o las amenazas y para establecer con más nitidez lo que se puede y no se puede hacer. En ese sentido, la ponente comenta las posibilidades de ampliar algunas instituciones clásicas, bien conocidas, a las necesidades de los mercados actuales, teniendo en cuenta, sobre todo, que la realidad ha cambiado debido a las nuevas tecnologías. En este contexto, es que en Estados Unidos y en Europa se ha comenzado con la redefinición o reforma de definiciones legales. En el europeo, Pérez Carrillo destaca la Directiva de 2014 que afecta la Ley de mercados y valores españoles sobre abusos de mercado. Este ámbito es importante pues uno de los abusos que puede suceder en el mercado tiene que ver con la información privilegiada, esto es, información de carácter concreto que se refiere a un instrumento financiero que no se ha hecho pública y que podría influir, de haberse conocido, en las cotizaciones. La ponente destaca que la tradicional idea del abuso de mercado por la cual uno conoce una información por alguien que la brinda de primera mano, está absolutamente superada con las nuevas formas que permite la tecnología de la información (que hace posible la comunicación de información en cuestión de segundos). Pérez Carrillo señala que, en estos casos, la rapidez es tal que no se sabe muy bien cómo reaccionar. En el plano internacional, a pesar de existir informes y guías que permiten flexibilidad para los reguladores de cada país, no hay aún un consenso sobre la materia. Al respecto, sostiene la ponente, que acaba de aprobarse una directiva de 2016 de ciberseguridad que es general, que afecta a las infraestructuras de mercado pero no afecta ni a los agentes ni a los intermediarios o emisores aludidos con anterioridad. La directiva 2016/1148, sobre ciberseguridad, establece la imposición de sistemas para controlar las órdenes (vigente desde 2018),

para facilitar los análisis así como generación de alertas. Esta directiva de ciberseguridad afecta bastante poco a emisores o intermediarios, pero sí afecta a los operadores de mercados. Así, les obliga a establecer medidas de mantenimiento de redes y sistemas de información y a controlar (o mejor, registrar) incidentes en el mercado. Finalmente, Pérez Carrillo señala que en España, en materia de ciberseguridad sobre servicios financieros, por un lado, va a tener que haber una adaptación al sistema comunitario que Europa impone. Las sugerencias de las organizaciones internacionales son: más gobernanza esto es, establecimiento de sistemas, mecanismos o protocolos por los cuales los ataques se comuniquen o se identifiquen; protección, detección, de recuperación (lo que significa difusión pero sin más daños al mercado); posibilidad de suspender cotización cuando se verifican órdenes extrañas (incluso si no llegan a ser un ciberataque). Se mencionan, además, otras medidas: Registros PAAE, retención de datos personales, ajuste de seguridad de cada mercado y emisor, mecanismos específicos administrativos procesales para la exigencia de responsabilidades (de internos y de terceros).

Seguidamente inicia su ponencia la Investigadora Marta González Aparicio, quien aborda lo relacionado a la fiscalidad de las bitcoins partiendo de algunas ideas básicas sobre estas monedas virtuales. La ponente destaca que este es un tema que engloba asuntos diversos como criptografía, ingeniería de software, economía y derecho. Un bitcoin es una moneda virtual o, dicho de manera más técnica, una criptomoneda, que se ha obtenido a partir de un procedimiento informático y que (y esta es la primera diferencia con el dinero tradicional) carece de soporte físico tal y como lo entendemos, así como tampoco es emitido por organismo o banco central alguno (segunda diferencia). Se trata de una moneda creada siguiendo una serie de protocolos informáticos y que, al poseer un valor, es susceptible de ser utilizada en el tráfico comercial y mercantil. El protocolo de las bitcoins proviene del año 2009, momento a partir del cual su uso se ha incrementado de manera exponencial. Las monedas poseen un valor, pero no es un valor fijo, sino que fluctúa según la oferta y la demanda. Este valor es único para todos los bitcoins en circulación. La ponente señala que la cotización del bitcoin se caracteriza también por su gran volatilidad. Así, en el año 2016, el valor de cotización de estas monedas ha fluctuado entre los 400 y 700 dólares. Por lo tanto, nos encontramos ante un activo con una volatilidad muy alta. Por otro lado, los bitcoins se pueden partir, esto es, se puede comprar un bitcoin o se puede comprar una parte de un bitcoin. Lo mismo sucede para pagar (con un bitcoin o con una parte del mismo). González Aparicio formula las preguntas: ¿Cómo funcionan las transacciones realizadas con bitcoins? ¿Qué pasa cuando un sujeto paga con bitcoins? La cadena de operaciones es como sigue: Cuando un sujeto A envía un pago con bitcoins a un sujeto B, la transacción pasa a la red, donde se convierte en un bloque de datos cifrados. Los "mineros" son los que descifran esos datos, esto es, desbloquean los datos, verifican la transacción y la aprueban. El primer "minero" que descifra el bloque de datos cifrados, a cambio de su actividad, obtiene una recompensa, también en bitcoins. Verificada la transacción por el sistema, el bloque se añade a una "cadena de bloques" ("*blockchain*") que es el fundamento del funcionamiento del bitcoin, que no es otra cosa que un libro contable público, replicado en todos los ordenadores de los usuarios del sistema y que reflejan todas las transacciones que se realizan con estas criptomonedas. Todo este proceso permite que el sujeto B reciba los bitcoins. A primera vista, González Aparicio destaca la participación de varios sujetos en este

proceso. Esto es muy importante desde el punto de vista tributario, pues no todos ellos van a tributar igual. Los "mineros" son los creadores de las criptomonedas y obtienen su remuneración en bitcoins. Otra figura es la conocida como "*excharger*" que son las personas físicas o jurídicas cuya actuación consiste en la compraventa e intermediación en la transmisión de bitcoins, percibiendo a cambio de sus servicios una comisión. Por otro lado, los particulares o personas físicas que utilizan los bitcoins como medio de pago o bien para mantenerlos como una suerte de activos de inversión y proceder a una posterior venta. Finalmente, están las empresas que, al igual que los particulares, pueden adquirir monedas o bien admitirlas como forma de pago por servicios para mantenerlas en su activo y revenderlas posteriormente o bien para pagar con ellas los productos y servicios necesarios para su actividad. Por tanto, González Aparicio señala que el bitcoin es una moneda virtual, con valor económico, que se emplea en el tráfico comercial y que (y esto es lo más importante desde el punto de vista tributario) las operaciones realizadas con bitcoins denotan capacidad económica. El principio de capacidad económica es un principio básico en materia tributaria para someter las rentas obtenidas a tributación. Ante este panorama, la ponente considera que Hacienda no puede permanecer al margen y, de hecho, no lo hace. Esto conduce directamente a preguntar cómo deben tributar en la práctica las operaciones y los sujetos que emplean y crean bitcoins. En primer lugar, hay que clasificar o determinar la naturaleza jurídica de los negocios que emplean bitcoins, tal como exige el artículo 13 de la Ley General Tributaria. Ante esto hay dos posibilidades. Por un lado, considerar los bitcoins como bienes (de modo que los negocios jurídicos llevados a cabo con estas criptomonedas, deberán ser calificados como permutas, en los términos establecidos en el Derecho civil) o aproximar los bitcoins al concepto de dinero, tal y como comúnmente lo entendemos (lo que equipara estas monedas a los medios de pago de general aceptación establecidos en la normativa iusprivatista). La ponente señala que argumentos a favor y en contra de cada una de las opciones hay varias. Al respecto, González Aparicio es partidaria de considerar a los bitcoins como bienes o commodities, entre otras cosas, porque para poder ser empleados, necesitan el previo acuerdo entre comprador y vendedor. En contra de esta postura se ha manifestado tanto la Dirección General de Tributación Española (en diversas consultas vinculantes) como el Tribunal de Justicia de la Unión Europea (en sentencia de 22 octubre de 2015), aproximando los bitcoins a las monedas de curso legal. ¿Qué implicaciones de esta postura se verifican en el ámbito tributario? La ponente señala que hay que comenzar diferenciando entre la imposición directa y la imposición indirecta y dentro de ella analizar qué figuras impositivas resultan aplicables a qué operaciones y cómo se deben aplicar. Tomando en cuenta la relación de sujetos intervinientes (particulares, "mineros", "*excharger*", empresas), en materia de imposición directa son varias las figuras impositivas que pueden gravar estas operaciones. Las dos principales son: el impuesto sobre la renta de las personas físicas y el impuesto sobre sociedades. También se pueden encontrar supuestos de aplicación del impuesto sobre actividades económicas, impuesto sobre el patrimonio y el impuesto sobre sucesiones y donaciones. González Aparicio se encarga de relacionar cada uno de los intervinientes con el impuesto sobre la renta de las personas físicas y el impuesto sobre sociedades. Con respecto a la imposición indirecta, la ponente señala que son dos las figuras tributarias que pueden recaer en estas operaciones: el impuesto sobre el valor añadido y el impuesto sobre transmisiones patrimoniales y actos jurídicos documentados. Esta sería la tributación, de manera rápida y resumida,

la tributación de los bitcoins. Para finalizar, González Aparicio comenta que si bien en sus inicios esta moneda estaba ligada a actividades fraudulentas (que estaban al margen de la administración tributaria), en la actualidad, debido al incremento de las operaciones que se realizan con las criptomonedas, se ha tomado cartas en el asunto y se han asumido actuaciones de cara a controlar cómo se utilizan aquellas. Por ejemplo, desde la Agencia Tributaria se están enviando requerimientos a aquellas empresas que admiten el pago con bitcoins para que justifiquen las cuantías recibidas. La ponente considera que el propio funcionamiento de la "*blockchain*" favorecería el control por parte de la administración, la que deberá esforzarse pues el control de tal libro contable no es nada sencillo.

Comentarios del relator

Las intervenciones de las ponentes en la Primera Mesa de Trabajo han dejado muy claro la trascendencia de las nuevas tecnologías y de la informática en el ámbito jurídico: en el ámbito del Derecho civil (contrataciones entre empresas y particulares, de cara a la prestación de servicios a distancia); en el ámbito del Derecho constitucional (el llamado "Derecho al olvido" y la determinación de qué información personal uno puede decidir o no que se muestre en las redes); en el ámbito del Derecho mercantil (la contratación de profesionales y la necesaria seguridad de la información relevante en el ámbito bursátil) y en el ámbito del Derecho tributario (reflexiones desde el ámbito fiscal sobre las bitcoins, así como el tratamiento jurídico-tributario de los intervinientes en todo el proceso que implica la utilización de las mencionadas criptomonedas). Las reflexiones planteadas por las intervinientes, a mi modo de ver, dejan dos asuntos que resulta necesario destacar. Primero, el incontestable enfoque interdisciplinar que supone el abordaje de diversos aspectos en los que, como medio para configurar relaciones de trascendencia jurídica, aparecen la tecnología y la informática. En la actualidad se ha vuelto algo común realizar compras por internet, llevar a cabo pagos de servicios por medio de tarjetas de crédito o elaborar contratos de las más diversas formas con una contraparte que se encuentra inclusive en otro país, con la que posiblemente el único elemento común sea el acceso a un dispositivo electrónico con acceso a internet. Estos escenarios deben ser amparados por el Derecho, el que debe ser configurado a partir de las propias características de los recursos y elementos que provee la tecnología y la informática. Segundo, el referido a la ciberseguridad, esto es, a los mecanismos de control de entrada y salida de información, así como de protección de las bases de datos en los que pueden contenerse importantísima información mercantil, civil o tributaria (relacionada a empresas, a las relaciones entre estas y sus proveedores, a los contratos entre estas y su personal, a sus informes o balances tributarios y financieros, etc.). Pero el tema no parece limitarse a estos ámbitos, sino que también se extiende al espacio de la información personal, esto es, a todos aquellos datos de una persona que pueden aparecer en la red. La virtualmente incontrolable fuerza que posee internet, en el que se acumula información de lo más variada, sin discriminación cronológica o de origen, debe corresponderse con la necesidad de que los ciudadanos gocen de una protección jurídica relativa a la supresión de la información personal irrelevante o que pueda resultar perjudicial para su desarrollo individual. Los esfuerzos del Derecho comunitario y nacional parecen haber reconocido este asunto, por lo que es de esperar un mayor desarrollo legislativo y jurisprudencial en los próximos años.

TERCERA PONENCIA: "Prevención y concienciación en ciberseguridad"
Ponente: D. Jorge Chinea López, Técnico de ciberseguridad INCIBE
Modera: D. Francisco Pérez Bes, Secretario General de INCIBE, Abogado, Especialista en Derecho TIC
Relatoría: Tamara Álvarez Robles, Personal Docente Investigador en Formación, Contratada Predoctoral en el Área de Derecho Constitucional de la Universidad de León

D. Jorge Chinea López comienza su exposición planteando la siguiente pregunta ¿qué es la ciberseguridad? Para dar respuesta a tal cuestión parte del concepto de información. La información que se almacena en los diferentes dispositivos tecnológicos, tanto a nivel personal como por las distintas entidades, y que es confidencial, es susceptible de ser protegida mediante la aplicación de las distintas medidas de seguridad existentes. Protegiendo esos dispositivos, que almacenan la información, de manera adecuada estaremos protegiendo debidamente nuestro principal activo, la información. La información ha de ser protegida frente a los ciberdelincuentes, quienes intentan acceder a la información para proceder a su venta en el mercado negro de la ciberdelincuencia. Si bien, la ciberseguridad no sólo se traduce en posibles ataques a esos medios que contienen información por parte de los ciberdelincuentes sino que afecta a la pérdida de información a consecuencia de incendios, de picos de tensión, etc. El ponente explica cuáles son las motivaciones de los ciberdelincuentes debiendo destacar las siguientes: primero, motivaciones de tipo económico, debido a la venta de información en el mercado negro; segundo, publicidad y notoriedad: fundamentalmente asociada al terrorismo; y, tercero, dañar la imagen de un tercero: mediante ataque dirigidos a la competencia o a un tercero. El ponente señala seguidamente con la explicación de la técnica del "*phishing*" (técnica utilizada para la consecución de datos de carácter personal como nombres de usuarios y contraseñas, detalles de tarjetas financieras, etc.). Luego, explica la necesidad de implantar medidas de seguridad en las empresas, en el día a día, para de ese modo generar la confianza necesaria. Chinea López resume en tres las medidas fundamentales a implantar para garantizar unos niveles mínimos de seguridad: el uso de contraseñas, la realización de copias de seguridad y la actualización de equipos. Respecto de la primera medida, el uso de contraseñas, reseña la importancia de utilizar distintos caracteres, mayúsculas y números; junto a ello el uso de distintas contraseñas para los diversos servicios y su cambio periódico. En cuanto a la realización de copias de seguridad, el ponente facilita varias pautas que han de seguirse: la selección de información crítica, la actualización de los antivirus, comprobación de las copias creadas y mantener copias fuera de la red interna o del dispositivo copiado. En este punto el ponente hace partícipe a los asistentes del virus "*Randsomware*" también conocido como "virus de la policía", cuya proliferación ha causado numerosos problemas a distintas empresas y personas. Se trata, dice, de un virus que accede a nuestro sistema y nos roba información, tras lo cual se contacta al usuario y se pide un rescate para devolver la información sustraída. Para combatir este virus es importante tener una copia de seguridad dado que mediante la restauración de la misma no causaría en el medio plazo y en un primer momento, tantos daños. Por último, el ponente destaca la importancia de mantener los equipos y aplicaciones actualizadas a fin de evitar dejar expuestos los mismos a hackers. Se trata, en

definitiva, de corregir las deficiencias de seguridad advertidas mediante la actualización de sistemas operativos, aplicaciones o antivirus. Para concluir este apartado el ponente resalta que estas medidas han de ser completadas con dos acciones igualmente importantes, cuales son la formación y la concienciación de aquellas personas que tienen en su poder información sensible, personal y confidencial. Es por ello que debemos conocer la Ley Orgánica de Protección de Datos, esto es, la parte legislativa de la ciberseguridad, dice el ponente, para de ese modo proteger de una manera más adecuada la información que se gestiona en el día a día. Concluye Chinea López su intervención con la reiteración de la necesidad de implementar las pautas o medidas de seguridad aludidas en su intervención para conseguir proteger la información.

Comentarios de la relatora

En estrecha relación con la intervención de D. Jorge Chinea López, considero necesario profundizar el conocimiento de la Ley Orgánica de Protección de Datos, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal, para de ese modo poder ejercitar los derechos que asisten a las distintas personas, derechos relacionados con la posesión y divulgación de los distintos datos que obran en posesión de terceros, debiendo resaltar los derechos de acceso, rectificación, cancelación y oposición, y consecuencia de estos el derecho al olvido. Esta norma fundamental unida al conocimiento y uso de los mecanismos de seguridad expuestos por el ponente son imprescindibles de cara a proteger nuestra información de prácticas abusivas, de malos usos, etc. La importancia de la seguridad de los datos es tal que la citada norma la incorpora como uno de los principios, junto a la calidad de los datos y al consentimiento, dedicándole su artículo 9 y desarrollado reglamentariamente en Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

CUARTA PONENCIA: "Aspectos sustantivos de la ciberdelincuencia"
Ponente: D. Fernando Javier Muñiz Tejerina, Magistrado del Juzgado de Instrucción N° 1 de León
Modera: D. Miguel Díaz y García Conlledo, Catedrático de Derecho Penal de la Universidad de León
Relatoría: Alfredo Alpaca Pérez, Investigador Contratado Predoctoral de la Universidad de León

El moderador, Profesor Dr. D. Miguel Díaz y García Conlledo, agradece a los organizadores del seminario y seguidamente presenta al ponente, D. Javier Muñiz Tejerina, Magistrado del Juzgado de Instrucción Número 1 de León, quien toma la palabra y comienza su ponencia señalando que el tema que se encargará de abordar es un tema muy vasto. El ponente afirma que lo primero que uno se pregunta cuando aborda lo referido a la ciberdelincuencia, específicamente, los delitos informáticos, es, precisamente, si esta clase de delitos existe. Esta inquietud preliminar tiene sentido pues, señala el ponente, hay muchos autores en la doctrina que afirman que la

mencionada clase de delitos no existe, sino que en realidad se tratan de modalidades especiales de comisión de delitos tradicionales que afectan a bienes jurídicos individuales (patrimonio, intimidad, etc.). Por el contrario, existen opiniones que señalan que los delitos informáticos son todos aquellos delitos que no se podrían cometer si no existiera la informática ni el internet (concepción más sociológica). Muñiz Tejerina señala que el concepto de delito informático no es novedoso: desde hace treinta años ya se viene hablando de esta categoría de delitos. En ese sentido, se ha venido definiendo al delito informático como todas aquellas conductas punibles o dignas de punición en las cuales el ordenador es el instrumento o el objeto del delito. Debido a que este concepto es aún bastante amplio, Muñiz Tejerina se refiere a otro un poco más delimitado: delitos informáticos serían aquellos en los que se tipifican conductas consistentes en atacar sistemas o datos informáticos o determinados contenidos, especialmente aptos para ser vulnerados por las nuevas tecnologías. Muñiz Tejerina señala que con la aparición de las nuevas tecnologías se habla, más que de delitos informáticos, de delitos tecnológicos. Asimismo, teniendo en cuenta el carácter transnacional de la delincuencia informática o ciberdelincuencia, se habla en la actualidad de "ciberdelitos", los cuales adquirieron una carta de naturaleza en el Convenio sobre ciberdelincuencia (conocido también como "Convenio de Budapest sobre ciberdelincuencia") de 2001, que constituyó el primer tratado internacional orientado, entre otras cosas, a hacer frente a los delitos informáticos y los delitos cometidos mediante internet. ¿Cómo se enfrenta el legislador a esta clase de delincuencia? Dos serían las vías, según el ponente: castigar mediante "tipos de equivalencia" o mediante la creación de nuevos tipos penales. La primera vía supone la creación de cláusulas complementarias a tipos penales que ya existen (el delito de estafa, por ejemplo). La ventaja más clara de esta primera alternativa es que desde el punto de vista del principio de seguridad jurídica, se delimitarían bien las conductas que se quieren sancionar penalmente. Como contrapartida, su desventaja radicaría en que se impide que se puedan sancionar nuevas formas de criminalidad como la que aquí se aborda, que es dinámica y que va mucho más rápido que los cambios legislativos. Con respecto a la segunda vía (el establecimiento de nuevos tipos penales), el ponente sostiene que mediante la creación de nuevas figuras delictivas orientadas a hacer frente a los ciberdelitos no solo se protegen los bienes jurídicos tradicionales, sino otros, como la integridad de las redes o los sistemas informáticos de los programas que sirven para el almacenamiento de datos. Si se llega a la conclusión que intereses como estos pueden ser entendidos como bien jurídico, el ponente afirma que se justificaría el tratamiento de figuras delictivas de carácter independiente a otras de carácter más tradicional. Muñiz Tejerina reitera que el concepto de ciberdelitos adquiere carta de naturaleza a partir del convenio sobre ciberdelincuencia, que fue ratificado por España el 20 de mayo de 2010 y que entró en vigor el 01 de octubre de 2010. Este convenio se complementa con el Protocolo Adicional al Convenio sobre ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, que entró fue ratificado por España el 11 de noviembre de 2014 y que entró en vigor el 01 de abril de 2015. El convenio, según el ponente, contiene una serie de definiciones muy importantes de cara a la interpretación de los tipos delictivos. Así, se propone definiciones para importantes categorías como "sistema informático", "datos informáticos", "proveedor de servicios" o "datos sobre el tráfico". Asimismo, en el Protocolo se propone una definición auténtica de "material racista y xenófobo".

Asimismo, en el Convenio, hay un apartado denominado "Derecho penal sustantivo". Aquí se establece una lista de categoría delictivas que el ponente caracteriza como "ciberdelitos": acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema y abuso de los dispositivos. Estos delitos son denominados en el Convenio como "delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos". En el propio Convenio se reconoce también como "delitos informáticos" a la falsificación informática y al fraude informático. Como "delito relacionado con el contenido", según el Convenio, está el delito relacionado con la pornografía infantil. Finalmente, en el Convenio se reconocen también a los "delitos relacionados con infracciones de la propiedad intelectual y derechos afines". Sobre esta tipificación, España no ha formulado reserva alguna, según señala el ponente. Por otro lado, el Protocolo contempla una serie de categorías delictivas denominadas por el ponente como "delitos de odio", entre las que están: la difusión de material racista y xenófobo mediante sistemas informáticos; amenazas con motivación racista y xenófoba; los insultos con motivación racista y xenófoba; y la negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad. Ahora bien, refiriéndose en concreto al Derecho español, el ponente hace referencia a las disposiciones pertinentes: el artículo 18 de la Constitución Española en el que se reconoce el derecho a la intimidad, el Convenio de Budapest, el Protocolo, la Directiva 2013/40/UE de 12 de agosto de 2013, sobre ciberdelincuencia (que sustituye la Decisión Marco 2005/222/JAI de 24 de febrero de 2005) y el Código Penal (modificado por Ley Orgánica 5/2010 de 22 de junio y por Ley Orgánica 1/2015 de 30 de marzo). Seguidamente, el ponente reconoce algunos de los delitos establecidos en el Código Penal que son relevantes para la materia. Por ejemplo, la estafa informática (artículo 248, 2. b)), las defraudaciones de fluido eléctrico y análogos (artículos 255 y 256); los daños informáticos (artículo 264); la denegación de servicio o sabotaje informático (artículo 264 bis) y el abuso de dispositivos (artículo 264 ter). Asimismo, los delitos relativos a la propiedad intelectual (artículo 270); delitos relativos a los secretos de empresa (artículo 279); los delitos relativos al acceso a servicios cerrados de radiodifusión (artículo 286); la falsedad de documentos electrónicos (artículos 390 a 399); el blanqueo de capitales (artículo 301); el sabotaje de redes de telecomunicaciones (artículo 560). Por otro lado también reconoce a los delitos de descubrimiento y revelación de secretos (artículo 197 ter), el *cyberbulling* (artículos 169, 171, 173, 197, 205, 206, 208 y 209); los delitos informáticos intrusivos y de daños con finalidad terrorista (artículo 573.2); el delito de distribución o difusión de mensajes o consignas que incitan a cometer los delitos de terrorismo (artículo 579).

Comentarios del relator

El tema abordado por D. Javier Muñiz Tejerina constituye uno de actualidad y de gran relevancia si se toma en cuenta el estado actual del desarrollo tecnológico e informático. Los grandes avances que esto implica, especialmente en lo relacionado a las nuevas tecnologías de la información, han pasado a ser parte de nuestra vida diaria. Como sucede en muchos ámbitos vitales, la incorrecta utilización de los medios tecnológicos e informáticos deben reflejar un adecuado tratamiento jurídico, más aún, si tal incorrecta utilización supone la afectación grave de intereses personales importantes como la intimidad, el honor, el libre desarrollo de la personalidad y la

libertad, entre otros. Por esto, el planteamiento de D. Javier Muñiz Tejerina resulta de importancia, sobre todo, al discutir la forma en la que el Derecho penal debe abordar estos nuevos escenarios caracterizados por su complejidad: aplicación de tipos penales ya conocidos (estafa, hurto, etc.), a los que se integrarían cláusulas específicas referidas a la utilización de medios tecnológicos o recursos informáticos; o la creación de nuevas figuras penales, que reflejen con exactitud el contenido del desvalor jurídico-penalmente relevante que se pretende combatir. Parece ser que la última vía es la más adecuada: la creación de nuevos tipos penales obliga al legislador a reflexionar sobre los escenarios (y, en definitiva, entenderlos) en los que aquellos pretenden ser aplicados y, evidentemente, exige una importante concentración sobre lo que resultaría punible y lo que quedaría impune (¿Qué se castiga y qué no? ¿Por qué una conducta se castiga y otra no?), esto es, una deliberación profunda de lo que quedaría aún dentro de los márgenes de lo permitido al ciudadano (lo que representa una discusión muy importante, tomando en cuenta la masividad del uso de las tecnologías en la vida diaria de las personas). Asimismo, esta segunda vía necesita inexorablemente un abordaje interdisciplinar, en donde lo jurídico-penal puede quedar eventualmente condicionado a lo técnico, esto es, a las referencias que de la informática y la tecnología se puedan obtener de cara a la delimitación de los alcances de las nuevas figuras delictivas.

QUINTA PONENCIA: "La responsabilidad penal frente a la robótica, la inteligencia artificial y el internet de las cosas"
Ponente: D. Ignacio Martínez San Macario, Abogado, Vocal de ENATIC
Modera: D. Fernando Rodríguez Santocildes, Abogado del Ilustre Colegio de Abogados de León
Relatoría: Stephania Serrano Suárez, Doctoranda del Programa "Estado de Derecho y Gobernanza Global" de la Universidad de Salamanca, Colaboradora Honorífica del Área de Derecho Penal de la Universidad de León

D. Ignacio Martínez San Macario inicia su intervención señalando que no hay una regulación específica sobre esto, por tanto, lo único que se puede hace es filosofar sobre la implicación de la inteligencia artificial y la robótica en la vida, en el ámbito de la tecnología y en el Derecho penal. Y en este sentido, señala el ponente, la posibilidad de actos relevantes para el Derecho penal que puedan ser cometidos por androides. Asimismo, Martínez San Macario refiere que trataría la responsabilidad penal "in vigilando", esto es, la responsabilidad por el hecho de no haber instalado, por ejemplo, un antivirus. El ponente inicia formulando una pregunta amplia: ¿Qué es y para qué sirve el Derecho penal? Responde señalando que este se entiende como ese acuerdo que tenemos entre todos, esos diez mandamientos, es el acuerdo de unos mínimos para poder convivir. Destaca al respecto que el Código penal es inmenso. En ese sentido, cita a Gimbernat Ordeig y dice que se trataría inclusive del Código Penal más duro de Europa. Esto sería así pues contiene las penas de prisión privativas de libertad más duras, a las cuales últimamente se han sumado penas limitativas de la libertad, como la libertad vigilada, que en el peor de los supuestos podrían llegar a sumar una pena de 60 años, 40 años de prisión, más 20 años de libertad vigilada. En este ámbito es importante reconocer el concepto de delito, pues de este se puede

desprender si se puede aplicar la responsabilidad penal a entes humanos o no. En el Código Penal se regula la posibilidad de condenar no solamente a personas físicas, sino también a personas jurídicas, lo cual implica la condena de un ente abstracto. Esto deja la duda si se puede aplicar la responsabilidad penal a una máquina, a un androide o un ente de inteligencia artificial. El ponente también se plantea: ¿se pueden aplicar penas corporales sobre las máquinas? ¿Cuáles serían las penas para un androide si no tiene sentimiento de libertad? A su vez presenta otro cuestionamiento: ¿Podría sustituir o suprimir, al juez o a los abogados la inteligencia artificial? esta última posibilidad se está presentando con los contratos inteligentes. Y por último: ¿Comprarías un coche que elegiría matarte para salvar otras vidas?, ¿a quién quieres que atropelle tu coche? Martínez San Macario afirma que nuestra vida actualmente es diferente, hemos cambiado el bar por las redes sociales. Esto conlleva que la gente que camina por la calle mirando el móvil es peligrosa, es un arma. Se trata de cómo incrustar la tecnología en la vida real, y eso en el Derecho penal está teniendo un anclaje regular. La justicia penal lleva sus ritmos para garantizar el supremo valor de la presunción de inocencia. Se ha dicho "los juicios son lentos, si queréis algo rápido ahí tenéis los prejuicios", esto debido a que se requiere una investigación con garantías. El ponente afirma que la tecnología no es buena si se reúnen personas y no se hablan entre sí por estar utilizando un dispositivo móvil. El impacto de la tecnología también se puede ver en las redes sociales, pues al eliminar a alguien de Facebook, por ejemplo, esa persona se siente despreciada. También el desarrollo tecnológico y virtual en las relaciones familiares puede tener otras consecuencias en un futuro cierto o incierto. Otra consecuencia que se presenta es que los dispositivos se hacen más pequeños y los seres humanos se hacen más gordos. De otra parte, el ponente señala que los abogados son un colectivo digitalmente inculto. Los juristas han llegado tarde al mundo digital, entre otras cosas porque contaban con el fax que lo solucionaba todo. En el mundo jurídico esta falta de cultura digital se traduce en el desconocimiento del abogado al presentar una prueba tecnológica y el desconocimiento que tiene el juez a la hora de valorarla. Seguidamente, Martínez San Macario presenta un *tweet* con insultos y amenazas de muerte. Ante esto, pregunta: ¿Qué pasaría si ese *tweet* lo escribiera una máquina? (esto es, una máquina de inteligencia artificial que ha aprendido con su propio sistema a relacionarse con los humanos). En España es muy habitual relacionarnos con insultos tanto para mal o como para bien. La máquina entiende que no sería responsable, pero, ¿qué sucedería con quien la programó? La solución a este problema es compleja, a pesar de que pueda quedar claro que la lesión de derecho es gravísima. Martínez San Macario presenta varios cuestionamientos en el siguiente sentido: ¿Cómo se condena a una máquina o a su propietario cuando la maquina es autora? Al respecto, hace una cita de unas noticias publicada en internet: "Google creó un coche sin conductor ni pasajeros" y "El coche sin conductor de Tesla cruzará datos con Facebook para decidir a quién atropella". Tesla insiste en que el 90% de los accidentes que ocurren en carretera son fallo humano, y que con sus coches se va a reducir en un 90% los accidentes. Pero, y la decisión de ¿Cómo programamos nuestro coche para que mate a los demás o para que si el daño social es menor nos mate a nosotros mismos?, ¿quién toma esa decisión?, ¿optamos por protección interior o protección de la lesión socialmente más grave?, si yo elijo proteger a mi hija, ¿soy responsable penalmente? porque mi decisión ha sido programar una máquina para decida acabar con la vida de alguien, no la mía. ¿Tiene esto sentido? Respecto al desarrollo de los androides, el ponente expone una noticia de un androide y su creador:

"en pocos años no podremos distinguir entre robots y humanos". El creador se dedica a hacer androides que hagan lo mismo que hacen los humanos, con sus virtudes y con sus defectos. Ante eso, el ponente pregunta: ¿Conseguiremos un autor criminal? y en ese caso, ¿qué hacemos con él, con su propietario o incluso con quien se ha comprado un androide? Martínez San Macario señala que a lo mejor con la herramienta viene la obligación de su responsabilidad, de su mantenimiento, pues nuestra falta de cuidado podría generar un daño para alguien. De otra parte, el ponente plantea que si tiene un expediente en el ordenador y desaparece, esto sería un problema, porque a lo mejor ese cliente no quiere que se enteren que tiene más de 20 antecedentes penales (datos penales sensibles). Esta actuación puede generar en el perjudicado un perjuicio. En el caso de que ese descuido se cometa por una máquina que tiene inteligencia artificial por yo haberme descuidado lo suficiente, ¿generaría responsabilidad penal en mí? El ponente cree que en ese caso particular no. Martínez San Macario señala que los grandes bufetes están utilizando trabaja con datos que no son apreciables a simple vista. Es evidente que un escrito de acusación de un Fiscal, se merece un escrito de defensa en consecuencia, pero el analizar el sentido de la sentencia de un juzgado determinado para poder alegar determinadas cosas, implica una gran cantidad de datos que una persona humana no es capaz de hacer bien, lo que el sistema Watson (inteligencia artificial) entra a suplir. ¿Va a suprimir eso al abogado?, ¿el diagnóstico del a defensa de tu defendido lo va a hacer una máquina?, ¿si utilizas la máquina y le condenan estás sujeto a responsabilidad civil? El ponente concluye señalando que, desde su punto de vista, lamentablemente va a suceder que la evolución de nuestro Derecho penal va a ir por donde viene, esto es, legislar a golpe de telediario o también que la dureza del Código Penal es directamente proporcional con el número de votos. Al respecto, señala que es muy probable que en breve tengamos una responsabilidad penal "in vigilando" de quienes no hayan cumplido los deberes de control sobre una "cosa" delincuente, lo que, para él, sería algo como un "nuevo Lombroso". Finalmente Martínez San Macario refiere que le gustaría que sucediera la total transversalidad del derecho: hay que mirar qué daño se ha producido y ver si la consecuencia es que el androide ingresa en prisión 25 años o si la consecuencia es que el humano responsable tiene que resarcir de alguna manera, es decir, más responsabilidad civil y menos responsabilidad penal. Pero esto, sostiene el ponente, no va a suceder.

Comentarios de la relatora

Si bien las personas nos estamos acostumbrado a la facilidad de las relaciones y de ciertas tareas por medio de las nuevas tecnologías, resulta útil plantearse futuros interrogantes que pueden surgir con el auge de la vida artificial y la inteligencia artificial. El surgimiento de sistemas expertos, redes neuronales artificiales, robots móviles y agentes autónomos múltiples sin duda están planteando retos para el derecho penal y el derecho civil. Razón por la cual es de gran importancia la capacitación de los nuevos juristas en estos ámbitos.

SEGUNDA MESA DE TRABAJO:
"Las nuevas medidas de investigación tecnológica y garantías constitucionales. Estabilidad del proceso penal con un pie en cada siglo", D. Pedro Álvarez Sánchez de Movellán, Profesor Titular de Derecho Procesal de la Universidad de León
"La libertad de conciencia ante el desarrollo de las nuevas tecnologías de la información y la comunicación", D. Salvador Tarodo Soria, Profesor Titular de Derecho Eclesiástico del Estado de la Universidad de León
"Internet y la contratación electrónica en el escenario tecnológico internacional", D. David Carrizo Aguado, Profesor Ayudante de Derecho Internacional Privado de la Universidad de León
Modera: Dña. Susana Rodríguez Escanciano, Catedrática de Derecho del Trabajo y la Seguridad Social de la Universidad de León
Relatoría: Alfredo Alpaca Pérez, Investigador Contratado Predoctoral de la Universidad de León

El Profesor Dr. Álvarez Sánchez de Movellán comienza agradeciendo a los organizadores por la invitación y por llevar a cabo el seminario, para luego afirmar que presentará algunas ideas generales para comprender la modificación de la LECr para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, llevada a cabo por la Ley Orgánica 13/2015, de 5 de octubre. El ponente alude al título octavo, que tiene el nombre de "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución" (83 artículos). Al respecto, señala que el panorama es absolutamente diverso, lo tangible desaparece y reina lo tecnológico. Según el ponente, el punto de inflexión entre el antiguo título octavo y el actual título octavo está en el artículo 18 de la Constitución, que tiene que ver con la intimidad, inviolabilidad del domicilio y el secreto de las comunicaciones. La Constitución y muy particularmente el desarrollo jurisprudencial del Tribunal Supremo y el Tribunal Constitucional, tirando de la analogía mucho más allá de lo que esta permite. En opinión del ponente, aquella labor jurisprudencial ha tenido alguna ventaja, pues ha permitido, gracias al esfuerzo de los tribunales, una labor de síntesis y de reflexión muy útil y que está muy presente en la reciente reforma. Seguidamente, Álvarez Sánchez de Movellán presenta la estructura de la reforma. Se ha contemplado el capítulo cuarto de disposiciones comunes; el capítulo quinto, referido a la interceptación de las comunicaciones telefónicas y telemáticas; el capítulo sexto, referido a la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; el capítulo séptimo, sobre la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización; el capítulo octavo, sobre registro de dispositivos de almacenamiento masivo de información; el capítulo noveno, sobre registros remotos sobre equipos informáticos; y el capítulo décimo, relativo a las medidas de aseguramiento. El ponente desea concentrarse en el capítulo cuarto pues, desde su punto de vista, ahí se encuentran los principios, esto es, lo que él denomina la "ideología" del legislador. En ese sentido, Álvarez Sánchez de Movellán propone una ruta para entender el capítulo cuarto. Una primera ruta (denominada "de garantías" por el ponente) vincula la solicitud (artículo 588 bis b), la resolución (artículo 588 bis c) y el control (artículo 588 bis g). Esto es así pues la solicitud va a marcar lo que se puede otorgar por parte

del Juez. La resolución, a su vez, como medida ejecutiva, va a permitir la delimitación del contenido (el cómo, el qué, el cuándo) de la nueva investigación. El control de la medida, por su parte, va a ser el elemento de cierre, esto es, lo que permita constatar que la resolución está siendo eficaz, que la resolución se adapta a lo que se ha solicitado y por lo tanto que lo que cabe esperar de toda la diligencia es algo válido. Una segunda ruta (denominada "cronológica" por el ponente) para entender las disposiciones comunes puede ser mediante la vinculación entre la duración (artículo 588 bis e), la solicitud de prórroga (artículo 588 bis f) y el cese de la medida (artículo 588 bis j). En esta segunda ruta entran en juego los principios de efectividad o motivación. Por último, una tercera ruta (de "garantías específicas") contiene al secreto (artículo 588 bis d), la afectación a terceras personas (artículo 588 bis h), la utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales (artículo 588 bis i) y la destrucción de registros (artículo 588 bis k). Todas tienen como referente común el garantizar los derechos que se ven afectados por las medidas. Ahora bien, con respecto a los principios rectores de las disposiciones comunes (artículo 588 bis a), el ponente señala que en estas disposiciones están contenidos diversos principios (especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad) que responden a la misma idea común: restricción. Seguidamente, el ponente desarrolla cada uno de tales principios, según lo dispuesto por el propio precepto. Para finalizar, Álvarez Sánchez de Movellán se vuelve a referir a las disposiciones comunes para profundizar algunas apreciaciones. Sobre la solicitud, que se prevé que sea de oficio (Ministerio Fiscal o Policía Judicial), se ha generado interés, pues según el ponente, se entiende que esta restricción responde al carácter público de este tipo de investigaciones. Estas actuaciones propias del proceso penal; se entiende, siempre y cuando se entienda que es una legitimación directa (el Ministerio Fiscal puede ir directamente, por ejemplo), pero que indirectamente las partes podrían solicitarlas, aunque esto es algo que está en discusión. Entre la solicitud y la resolución, señala el ponente, que el perfil es prácticamente el mismo. Es importante el tema de la finalidad, por lo que la resolución debe decirse cuál es la finalidad a la que responde la medida que se va a acordar, ya que esa finalidad va a ser elemento de chequeo para el control (recordar aquí la primera ruta descrita por el ponente) y si esa finalidad no se obtiene no se alcanzará la medida. El secreto, que, como antes señaló el ponente, está al servicio de la tutela de derechos, siempre se trata de actuaciones secretas aunque no se haya acordado el secreto en el sumario. Con respecto a la duración, más que a los plazos, se trata más bien de la referencia a un tiempo imprescindible, pues al tratarse de afectación de derechos, habría que tratar de resolver en el menor plazo posible.

Seguidamente, toma la palabra el Profesor Dr. Salvador Tarodo Soria, quien comienza agradeciendo a los organizadores por permitirle estar presente en el seminario y así compartir algunas ideas sobre la libertad de conciencia ante el desarrollo de las nuevas tecnologías de la información y la comunicación. El ponente considera importante comenzar señalando qué es lo que entiende por libertad de conciencia: que cada uno pueda tener sus propias ideas y convicciones y que se tenga la libertad de expresarlas o no. Asimismo, señala que le gustaría subrayar que es muy importante que cada uno pueda comportarse de acuerdo a sus ideas y creencias porque no solo es un derecho fundamental, sino que es también necesario para la propia existencia de la democracia: si no tuviésemos cada uno nuestras propias ideas o creencias no existiría el sistema

democrático. Tarodo Soria anuncia que dividirá su intervención en dos partes: primero, se dedicará a proponer una reflexión a partir de un libro; y, segundo, se dedicará a recorrer algunos de los aspectos jurídicos en el que se ven afectados desde la libertad de conciencia. El libro desde el que el ponente propone un acercamiento al tema es un libro de 1990, llamado "La sociedad transparente" de Gianni Vattimo (representante de la "corriente débil" al que también pertenecía Umberto Eco), que defendía la idea del "fin de la modernidad", que supone que hay que analizar la realidad de forma parcial. El autor, en este libro, señala que esa necesidad de avalar esos grandes relatos que ya no son posibles para acercarse a la realidad proviene de dos factores: primero, el fin del colonialismo (que hace que pierdan vigencia todas las tesis etnocentristas de la interpretación de la realidad); y, segundo, el desarrollo de los *mass media*. El ponente quiere llamar la atención sobre una interrogante que se plantea Vattimo: ¿el desarrollo de los *mass media* (pensando el autor, conforme a su época –1990–, en la televisión y en la radio) provoca una mayor homogeneización de la sociedad en la que todos vemos la realidad desde los mismos parámetros? ¿O provoca justo lo contrario: una explosión y multiplicación de las distintas visiones del mundo? Ante esta disyuntiva, el ponente ofrece su punto de vista: los *mass media* y las nuevas tecnologías de la información no provocan por sí solo ninguno de los efectos antes mencionados, sino que es el uso que hagamos de ellas: es el uso de los *mass media* y las nuevas tecnologías de la información lo que puede llevar a una mayor homogeneización o empobrecimiento o a una mayor diversidad o pluralismo. Seguidamente Tarodo Soria se pregunta: ¿qué necesitamos para garantizar un buen uso? Para esto se necesita, entre otras cosas, la intervención del derecho, esto es, que se adopten medidas para garantizar algún tipo de autorregulación o algún tipo de control o regulación por parte del Estado. Aquí es cuando el ponente anuncia la segunda parte de su ponencia, relacionada al abordaje jurídico del tema. ¿Qué aspectos son relevantes desde el punto de vista de la necesidad de proteger que cada uno tenga sus propias convicciones? En primer lugar, la intimidad, que es un derecho básico. La intimidad, entendida no solo como un espacio de abstención de la intervención de terceros, sino también un espacio en el que uno se autorealiza como persona. En segundo lugar, el derecho a la educación. Allí donde no hay educación, no es posible tener un juicio autónomo, y si no hay juicio autónomo, no es posible interpretar todas las informaciones que tenemos a nuestro alcance (que hoy en día se encuentran principalmente en internet). Por tanto, si los *mass media* homogenizan o no homogenizan, depende de la capacidad crítica del receptor, y esa capacidad crítica depende, a su vez, de la protección del derecho a la educación. En tercer lugar, el derecho a la libertad de información y de expresión, que tienen una peculiaridad jurídica: además de ser derechos fundamentales, son también, según el Tribunal Constitucional, garantías institucionales (son garantías de una opinión pública libre) y, por lo tanto, requieren de una protección reforzada cuando entran en conflicto con otros derechos.

Posteriormente, toma la palabra el Profesor David Carrizo Aguado, quien comienza agradeciendo a los organizadores por la invitación al seminario y señala que su ponencia gira en torno a dos cuestiones: primero, cómo internet, como tal, está regulada en el ámbito internacional; y, segundo, lo relativo al comercio electrónico, específicamente, cuándo interviene el elemento internacional en este tipo de contratación on line. Es conocido que la evolución tecnológica en la que nos

encontramos en la actualidad ha conducido a una expansión masiva de los servicios electrónicos de tipo interactivo. En el plano técnico, el elemento fundamental es internet, pues hace que podamos afirmar que el entramado mundial de redes vinculadas entre sí haga posible la comunicación inmediata (o casi inmediata) desde cualquier dispositivo electrónico en cualquier lugar del mundo. De esta afirmación deduce el ponente el elemento internacional, presente en el ámbito de las comunicaciones y principalmente en el sector del comercio electrónico. Es conocido que esta globalidad en la comunicación implica ciertos riesgos sobre los que el derecho debe dar una respuesta efectiva. La manipulación de contenidos o la vulneración de derechos (principalmente en el campo del derecho al consumo internacional) suponen escenarios complejos que parecen acentuarse cuando se realizan en un escenario transfonterizo. En cuanto a las estructuras de gobernanza de internet, se puede decir que los Estados siempre se han mantenido al margen, por lo que parece haber una omisión en cuanto a la regulación de este asunto concreto. Si bien ha habido una intervención de gobiernos u organizaciones no gubernamentales del sector privado o inclusive la sociedad civil, no ha sucedido lo mismo con los Estados como tales, esto es, como agentes de los que emana legislación. Un asunto importante que ya se destacó en 2012 en el Consejo de Derechos Humanos de las Naciones Unidas, es el referido a que los Estados deben promover y facilitar el acceso a internet y a la cooperación internacional encaminada al desarrollo de los medios de comunicación e información en todos los países. A pesar de que esto puede reflejar una preocupación de los Estados en este ámbito, el ponente señala que no se ha dado un paso más allá. Carrizo Aguado propone mencionar brevemente qué instituciones existen en la actualidad que garantizan un funcionamiento seguro y un desarrollo de internet a través de ciertos protocolos y líneas de actuación emanados de estas instituciones. Fundamentalmente son cuatro: Internet Society o ISOC (intervienen de manera directa para delimitar los estándares técnicos que giran en torno a la utilización de la red de redes); Internet Architecture Board o IAB (busca investigar y desarrollar las tecnologías en ese sector); World Wide Web Consortium o W3C (que formula numerosas recomendaciones o estándares principalmente centrados en el ámbito del software) e Internet Assigned Numbers Authority o IANA (que se concentra en emitir informes sobre los nombres de dominio en el campo de internet). De todas estas instituciones interesa, según el ponente, reconocer que no son organismos estatales y solamente crean ciertas reglas escritas y estándares que siempre quedan supeditados a la aprobación de leyes por parte de las instancias estatales pertinentes. Inclusive podríamos cuestionar, según el ponente, la legitimidad que tienen estas instituciones para diseñar la línea jurídica en torno al campo de internet. Lo que no se puede negar es que constituyen una ayuda para fijar los estándares tecnológicos y la ordenación técnica de internet, pero, desde el ámbito jurídico, es posible encontrar ciertas deficiencias. Esta es entonces, de manera muy genérica, cómo se organiza la gobernanza de internet en el ámbito internacional. En cuanto a la segunda parte de su intervención, el ponente señala que la contratación electrónica constituye un campo bastante amplio que merece un abordaje más detallado. Carrizo Aguado parte reconociendo que la parte débil de una contratación on line puede ser el consumidor. Esta situación se complica, pues dado que tal contratación se realiza en el ámbito internacional, muchas veces uno contrata sin saber con quién lo hace, o dónde en el mundo se encuentra la persona con la que se realiza la contratación, qué legislación puede ser aplicable, dónde y ante quién reclamar en caso haya un incumplimiento

contractual. Todo esto podría sugerir una intranquilidad para el consumidor. En la práctica, una cuestión muy común tiene que ver con las cláusulas de sumisión a los tribunales: en el ámbito de la contratación electrónica es bastante usual que el empresario (que el consumidor, como antes se dijo, no conoce) introduzca una cláusula que señala que en caso de conflicto o incumplimiento contractual serán competentes los tribunales del domicilio del empresario. Esto va en detrimento de los derechos del consumidor. Carrizo Aguado, tomando en cuenta los reglamentos comunitarios pertinentes, señala que, en el ámbito de la contratación electrónica, parece ser que, en este caso, el pacto sería nulo: cualquier cláusula de sumisión establecida con anterioridad al surgimiento del litigio es nula. A pesar de esto, diariamente se encuentra esta situación en la red (por ejemplo, mediante la compra on line de billetes de avión). El ponente señala que los tribunales han incidido en la forma de resolución de este problema: ofreciendo mayor información (o información más clara o más directa) en la propia página web. En el marco de los contratos electrónicos, ante un eventual incumplimiento, es bastante común que el consumidor quede indefenso pues no sepa dónde reclamar o cómo interponer una reclamación. En los hechos, el procedimiento es complejo y costoso, pues la actuación jurisdiccional no es sencilla para el consumidor medio. Por ello, una de las últimas novedades al respecto a nivel comunitario tiene que ver con el tratamiento de la complejidad para el acceso a la vía jurisdiccional a partir de una contratación electrónica: mediante la habilitación de la vía extrajurisdiccional para efectuar reclamaciones en materia de contratación electrónica. Carrizo Aguado señala que el objetivo del establecimiento de esta vía extrajudicial es que un tercero neutral interceda en los intereses de las partes para intentar solucionar el conflicto que emana de una contratación electrónica o que surge de cualquier plataforma tecnológica habilitada al efecto. Esta regulación se sustenta en el principio de confianza que posee el consumidor para resolver el litigio y en la adhesión voluntaria del empresario a la resolución por la vía extrajudicial. Finalmente, destaca en ponente que, en cuanto a mecanismos extrajudiciales, existen dos normas: la Directiva 2013/11 (que no ha sido aún transpuesta por el Estado español a su legislación) y un Reglamento Europeo 524-2013 (de cumplimiento obligatorio a partir de 9 de enero de 2016, aunque España aún no ha habilitado la correspondiente plataforma en internet).

Comentarios del relator

Las intervenciones de los participantes en la segunda mesa de trabajo constituyen un claro ejemplo de las diversas manifestaciones que la utilización de internet supone en diversos ámbitos de la vida y que tienen trascendencia para el derecho. Primero, cómo las técnicas de investigación de hechos (en este caso, de delitos) deben actualizarse y adaptarse a la propia dinámica de las tecnologías de la información, de tal manera que puedan poseer una real capacidad de rendimiento de cara a una suficiente determinación de hechos que puedan resultar relevantes en el marco de un procedimiento penal. Este asunto es muy importante pues, como es evidente, tanto la delincuencia común como la de mayor complejidad (económica, por ejemplo) recurre frecuentemente a la utilización de dispositivos electrónicos (para facilitar la comunicación entre los participantes, para organizar el plan criminal, etc.) o a la utilización de bases de datos en donde conste información técnica (contable, financiera) que resulte funcional a la realización (y ocultamiento) del hecho. En ese

marco, la adecuación de las técnicas de investigación a las nuevas tecnologías, al suponer una intervención en esferas de índole privada (comunicaciones personales mediante correos electrónicos, mensajes de texto, etc.), genera necesariamente un debate sobre hasta qué punto es legítima esa capacidad de intervención en aras de la búsqueda de elementos de prueba a ser incorporados a un proceso. Segundo, cómo la libertad en el uso de las nuevas tecnologías de la información implica, como consecuencia, la responsabilidad de quien no lo haga correctamente. Qué criterios permitirían (o harían legítimo y razonable) una autorregulación o una regulación por parte del Estado, constituye un asunto que debe abordarse desde el ámbito del derecho. En ese sentido, como señaló el ponente, ha de tomarse en cuenta la concurrencia de los derechos que están en juego en este debate: el derecho a la intimidad, el derecho a la educación y el derecho a la libertad de información y expresión. Cualquier decisión que se tome sobre el tema representará, sin lugar a dudas, un escenario necesario de tensión entre los mencionados derechos. Constituirá una labor del jurista interesado en estos temas plantear una solución razonable y conforme a principios. Tercero, cómo el derecho debe resolver asuntos relativos al incumplimiento de contrataciones en escenarios, hasta hace unos años, completamente atípicos: donde las partes no se conocen, se encuentran espacialmente en lugares distintos (países e inclusive continentes diferentes) y cuyo único factor común puede ser el acceso a un dispositivo electrónico con internet. La proliferación actual de actos jurídicos que tienen por objeto bienes y servicios por medio de internet posiblemente sea un ámbito en el que falta perfilar aspectos específicos, de cara a nivelar las condiciones de los contratantes y, en la medida de lo posible, asegurar una situación de igualdad. Las cláusulas generales de contratación o las cláusulas de sumisión podrían constituir elementos que precisan de un mayor análisis jurídico, no solo para garantizar al consumidor que el bien o servicio objeto de su prestación será entregado o realizado conforme a sus expectativas, sino también para condicionar las actividades del empresario a una necesaria previsibilidad en los casos de conflictos emanados por incumplimiento de contrataciones electrónicas.