I. RELATORÍAS DE LAS I JORNADAS NACIONALES DE DERECHO Y CIBERSEGURIDAD

Evento académico desarrollado los días 20 y 21 de octubre de 2015, en el Salón de Grados de la Facultad de Derecho de la Universidad de León. Coordinado por la Prof. Dra. Dña. Isabel Durán Seco (Profesora Contratada Doctora (acr. Profesora Titular) de Derecho Penal en la Universidad de León) y por D. Francisco Pérez Bes (Secretario General de INCIBE, Abogado, Especialista en Derecho TIC).

Primera ponencia: "Retos de la ciberseguridad en España"

Ponente: Dña. Alejandra Frías López, Magistrada Asesora del Ministerio de Justicia, Vocal del Consejo Nacional de Ciberseguridad

Moderadora: Dña. Marisol Aldonza Vivanco, Departamento Jurídico INCIBE

Relatora: Dña. Patricia Prieto Padín, Investigadora contratada predoctoral FPU del Ministerio de Educación, Cultura y Deporte en la Universidad de León

Tras la inauguración formal de las I Jornadas Nacionales de Derecho y Ciberseguridad, se da paso a la primera ponencia del evento. Dña. Marisol Aldonza Vivanco (Técnico Jurídico del INCIBE), desempeñando el papel de moderadora, presenta a Dña. Alejandra Frías López (Magistrada Asesora del Ministerio de Justicia y Vocal del Consejo Nacional de Ciberseguridad), encargada de ilustrar al cuantioso auditorio asistente sobre los "Retos de la ciberseguridad en España". Agradeciendo la oportunidad de disertar en el ámbito académico universitario, donde –apunta– radica el germen de la sociedad y actividad profesional del futuro, el objetivo de su intervención centra la atención principalmente en aportar una visión integradora o global sobre el pasado y presente de las actuaciones en materia de ciberseguridad en España, así como sus perspectivas de futuro, abarcando también la perspectiva de coordinación y cooperación entre todos los agentes implicados.

En primer lugar, considerando que España no puede ser entendida sin Europa, su discurso focaliza el interés hacia el análisis del marco europeo en materia de ciberseguridad, haciendo hincapié y desglosando las ideas o aspectos fundamentales de los siguientes textos: 1) Estrategia de Ciberseguridad de la UE de 2013, analizando cómo las TIC's constituyen la piedra angular de nuestro crecimiento económico; 2) Dictamen del Comité Económico y Social Europeo, sobre el tema ciberataques en la UE, de 10 julio 2014, en virtud del cual todas las empresas deberían estar obligadas por ley en mantener un enfoque proactivo para protegerse

de los ataques en la red, al tiempo que procedería garantizar una formación del personal sobre las políticas de seguridad de la información[1] semejante a la que existe sobre asuntos de salud y seguridad laboral; 3) Conclusiones del Consejo de la UE sobre la Ciberdiplomacia, de 11 febrero 2015, el cual recuerda la necesidad de entender que las mismas normas, principios y valores que rigen en el mundo físico o real deben ser aplicables en el ciberespacio, en concreto derechos fundamentales y libertades públicas; 4) Estrategia para el Mercado Único Digital de Europa, de 6 mayo 2015, afirmando el necesario enfoque o tratamiento transversal las TIC; 5) Agenda Europea de Seguridad 2015-2020, presentada por la Comisión Europea el 28 abril 2015; 6) Conferencia General sobre el Ciberespacio, La Haya, abril 2015, en la cual quedó patente que, después de la prostitución y el tráfico de drogas, el cibercrimen es la modalidad delictiva más lucrativa; en fin, 7) Informe de evaluación sobre la 7ª ronda de evaluaciones mutuas del grupo GENVAL sobre la ciberdelincuencia, del Consejo de la UE.

En segundo término, y acotando el campo de análisis, fue examinado en detalle el marco de actuación nacional. Frías López destacó cómo el gobierno español, para cumplir con el objetivo prioritario –unánime en numerosos países– de garantizar la seguridad en el ciberespacio, ha centrado sus esfuerzos en la coordinación y colaboración, para lo cual ha establecido un marco regulador con un enfoque multidisciplinar, materializado en diversas actuaciones: la elaboración de la Estrategia de Seguridad Nacional (31 mayo 2013) y la Estrategia de Ciberseguridad Nacional (5 diciembre 2014), la creación del Consejo Nacional de Ciberseguridad (CNCS), la redacción del Informe Anual de Seguridad Nacional (el último de 24 abril 2015), como documento pionero en el mundo o, en fin, la aprobación del Plan Nacional de Ciberseguridad (31 octubre 2014), así como los Planes Derivados (14 julio 2015) de carácter transversal que versan, desde la cooperación internacional y a nivel europeo, la ciberdefensa o el intercambio de información sobre ciberamenazas, pasando por la ciberseguridad en las Administraciones Públicas, la protección en los sistemas que soportan infraestructuras críticas, el plan contra la ciberdelincuencia y el ciberterrorismo o la protección de las TIC en el sector privado[2], hasta el plan de cultura de ciberseguridad o referido al desarrollo industrial, capacitación de profesionales y refuerzo de la I+D+i, el cual prevé la modificación de los planes de estudio en los ámbitos técnico, operativo y jurídico.

Posteriormente, Frías López focalizó su intervención en el Plan contra la ciberdelincuencia y el ciberterrorismo, donde el Gobierno español aboga por una actualización permanente de los instrumentos y herramientas legales. Tras explicar la reciente actividad legislativa impulsada por el Ministerio de Justicia (amparada por normas internacionales), la cual cristaliza, tanto en el ámbito de la tipificación

---

1 Un esbozo en KIRSCH, L. y BOSS, S.: "The last line of defense: motivating employees to follow corporate security guidelines" en AA.VV.: *Proceedings of the 28th International Conference on Information systems*, Montreal, 2007, en: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1260&context=icis2007.

2 En el ámbito de las relaciones laborales, resulta de gran interés la obra de RODRÍGUEZ ESCANCIANO, Susana: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant Lo Blanch (Valencia), 2015, 300 págs.

penal (LO 1/2015 y LO 2/2015, de 30 de marzo) como en el campo de la investigación criminal (LO 13/2015, de 5 de octubre), recordó cómo, pese a la importancia en asuntos de ciberseguridad de la colaboración público-privada y el principio de responsabilidad compartida, la Administración Pública debe reservarse un papel predominante al amparo del art. 103 CE, el cual ordena satisfacer las necesidades derivadas del interés general.

Para finalizar, Frías López –invitando a la reflexión individual– evocó tanto la Recomendación de 23 de febrero de 1999, del Comité de Ministros del Consejo de Europa, sobre la protección de la privacidad en internet[3], como varios pronunciamientos judiciales[4]. Asimismo, recalcó que el gran reto de la sociedad del siglo XXI viene representado en saber encontrar en este ámbito el punto de equilibrio adecuado entre los derechos que afectan a la seguridad y cuantos atañen a la privacidad.

La moderadora agradeció a la ponente su participación en las Jornadas, destacando la calidad de sus ideas y el conocimiento de las normas e interpretación de las mismas, así como sus enriquecedoras aportaciones de cara al presente y futuro. El interés por la intervención de Dña. Alejandra Frías López quedó refrendado por el interesante turno de preguntas-debate entre los asistentes que cerró su participación en el evento.

Comentarios de la relatora

El indudable desarrollo del ciberespacio y, con ello, el auge de toda clase de interacciones comerciales, sociales y gubernamentales en el mismo, ha acarreado una simultánea proliferación de ciberataques. La preocupación por identificar, prevenir, controlar y neutralizar o contraatacar este tipo de acciones delictivas y, sobre todo, por asegurar la protección de las infraestructuras críticas y el respeto de los derechos y libertades fundamentales se ha materializado en una proliferación normativa evidente, tanto a nivel supranacional como estatal. Aun cuando las actuaciones llevadas a cabo sirvan para paliar o afrontar los graves problemas que despierta la era digital –en un campo de batalla que no conoce de fronteras geográficas, en permanente mutabilidad y susceptible de provocar daños con impactos transversales en todos los ámbitos y disciplinas–, siempre existirán retos a superar que exigen considerar múltiples aspectos: desde la necesidad de alentar una mayor concienciación de los ciudadanos o la conveniencia de ofrecer una formación especializada, hasta la ineludible y permanente tarea de coordinación y cooperación

[3] La cual ya advertía cómo "el uso de internet supone una responsabilidad en cada acción e implica riesgos para la intimidad, por cuanto cada visita a un sitio de Internet deja una serie de 'rastros electrónicos' que pueden utilizarse para establecer 'un perfil de su persona y sus intereses'".

[4] En lo sustancial, la STS 24 febrero 2015 (Rec. 1774/2014) que consagra una especie de derecho al propio entorno virtual y la STJUE 6 octubre 2015, Asunto C-362/14, Maximiliano Schrems *v* Data Protection Commissioner, que invalida el Marco de Puerto Seguro (Safe Harbor) entre Estados Unidos y Europa.

de todos los actores implicados en punto a seguridad cibernética en los diferentes países, única vía para luchar de una manera más proactiva y eficaz contra lo que no deja de ser una amenaza para la comunidad.

Segunda ponencia: "La fiscalía de cibercriminalidad informática"

Ponente: Dña. Elvira Tejada de la Fuente, Fiscal Coordinadora de la Fiscalía de Cibercriminalidad informática

Moderador: D. Francisco Pérez Bes, Secretario General de INCIBE, Abogado, Especialista en Derecho TIC

Relatora: Dña. Stephania Serrano Suárez, Doctoranda del Programa "Estado de Derecho y Gobernanza Global" de la Universidad de Salamanca, Colaboradora Honorífica del Departamento de Derecho Penal de la Universidad de León

Dña. Elvira Tejada de la Fuente inicia su intervención señalando que la evolución de las tecnologías de la información y la comunicación ha tenido incidencia en al ámbito de la ciberdelincuencia. En concreto, esto se evidencia en el surgimiento de nuevas conductas capaces de lesionar bienes jurídicos necesitados de protección, como son, por ejemplo, los daños informáticos o los accesos ilegales a los sistemas informáticos. De igual forma, están apareciendo nuevas formas de cometer actos ilícitos tradicionales que ya estaban tipificados como delitos por los ordenamientos jurídicos pero que como consecuencia de desarrollarse por las nuevas tecnologías aparecen variaciones en la ejecución criminal que hacen que no encajen bien en los tipos penales existentes. Esto representa un gran reto para el legislador, pues sobre este emerge la necesidad de redefinir las conductas delictivas existentes o de dar lugar a la creación de nuevas figuras jurídicas con las cuales hacer frente a este fenómeno.

A la variación en la forma de comisión de determinados delitos y la pluralidad de bienes jurídicos afectados, se añade el incremento progresivo de este tipo de investigaciones. Tejada de la Fuente señala que al hablar de ciberdelincuencia no estamos hablando de una categoría cerrada y concreta de algunos delitos, sino de un fenómeno criminal transversal que afecta a bienes jurídicos de distinta naturaleza: a la intimidad, al honor, a la libertad, la seguridad, a la indemnidad sexual de los menores (acoso, pornografía infantil a través de internet); así como también afecta bienes de carácter patrimonial (el numero más elevado de investigaciones son prácticamente estafas y fraudes informáticos) y puede afectar también a la seguridad colectiva (delitos como la utilización de internet con finalidad terrorista).

Tejada de la Fuente asegura que esta evolución cualitativa y cuantitativa del fenómeno hace que resulte problemático definir el concepto de ciberdelincuencia. Así, la ponente señala que si bien en 2010 se presentó una reforma en cuanto a estos delitos, ya fue necesaria otra en 2015, pues los tipos penales ya no eran suficientes.

Pero, según Tejada de la Fuente, no solamente es importante tener tipos penales adecuadas para actuar frente a determinadas conductas, sino que también resulta importante tener unas buenas herramientas de investigación, pues estos delitos no pueden investigarse con las técnicas tradicionales, por lo que es imprescindible que se usen en las investigaciones las mismas herramientas informáticas o tecnológicas que permitan lograr condenas para los responsables de esas conductas. La reforma de la ley de enjuiciamiento criminal tiene en cuenta lo anterior. Así, el legislador ha creado unas herramientas tecnológicas novedosas como el agente encubierto en la red o el registro remoto en sistemas informáticos (a través de un virus hacer una investigación criminal, autorizada policialmente).

Tejada de la Fuente sostiene que también es necesario reforzar la cooperación internacional, debido a que los delitos que aquí se analizan no tienen territorios ni límites, ya que pueden estarse ejecutando en distintos lugares al mismo tiempo. La colaboración debe realizarse bajo los parámetros de: aproximación normativa y reforzamiento de los instrumentos de cooperación internacional. La convención de Budapest, el documento a nivel internacional más importante, aunque está circunscrito al ámbito del Consejo de Europa, ha sido firmado por muchos países que no son miembros del consejo de Europa y ahí es donde se está creando un marco común de normas comunes para fundamentar una buena cooperación en la investigación criminal. Respecto al ámbito de cooperación en materia de prueba, Tejada de la Fuente puntualiza que la Policía o el Ministerio Fiscal pueden ordenar al operador de comunicaciones o a cualquier persona que tenga a su disposición datos informáticos que los conserve para investigaciones, mientras se logra una autorización judicial. Asimismo, la ponente señala que se ha propuesto la cooperación con Latinoamérica, con las mismas características como la que existe en Europa.

Tejada de la Fuente afirma que los nuevos fenómenos criminales generan para el Ministerio Fiscal el reto de ser eficaces en la actuación o intervención judicial, sin que ello suponga limitar o restringir los derechos y libertades fundamentales de las personas, de conformidad a un respeto absoluto a las garantías de un Estado Social de Derecho. En ese sentido la entidad ha hecho una apuesta por la especialización. La función del Ministerio Fiscal es la defensa de la legalidad de los derechos de los ciudadanos y de interés general y se rige por cuatro principios: 1) Legalidad, 2) Imparcialidad, 3) Unidad de actuación y 4) Dependencia jerárquica. El Estatuto Orgánico del Ministerio Fiscal se reformó mediante la ley 24/2007, con el fin de darle mayor autonomía, realizar un despliegue territorial adecuado y fortalecer la especialización, que tiene como finalidad abordar de forma especial los fenómenos criminales más complejos, coordinar investigaciones que afectan a diferentes territorios, potenciar el principio de unidad de actuación y favorecer las relaciones entre otros instituciones y organismos. Para ello se tienen en la Fiscalía: Fiscalías especiales y redes nacionales de especialistas. En cuanto al área de especialización de criminalidad informática, Tejada de la Fuente sostiene que existen tres hitos fundamentales: la creación de la plaza de Fiscal de Sala de criminalidad informática, la publicación de instrucción (2/2011) FGE, y por último la creación de servicios territoriales de criminalidad informática.

En síntesis, la organización del área de especialización del Ministerio Fiscal es del siguiente modo: 1) Fiscal de Sala Coordinador, 2) Fiscales Adscritos, 3) Red nacional de Fiscales Delegados Provinciales. El Fiscal de sala coordinador en materia de criminalidad informática (en el 2007 hubo un antecedente, pero se crea en el 2010) tiene competencia a nivel nacional para dirigir o intervenir en cualquier investigación en territorio nacional que desarrolle en esta materia. La instrucción pretende definir las materias objeto de especialización y definir funciones tanto del Fiscal de Sala como de red de especialistas. Para identificar los delitos competencia de la especialidad, debe aludirse a qué se entiende por criminalidad informática: 1) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC's; 2) Delitos en los que la propia dinámica criminal se encuentra plenamente vinculada al uso de las TIC's; y, 3) Delitos en los que la actividad criminal se sirve de las TIC's para su ejecución y cuando como consecuencia de ello se genere una especial complejidad en la investigación (la que a su vez demande de conocimientos específicos en la materia).

Según Tejada de la Fuente, algunas de las funciones del Fiscal de Sala son: coordinar y fijar criterios de actuación, supervisar el funcionamiento de los servicios en cada fiscalía de criminalidad informática, incoar diligencias de investigación en casos excepcionales, además de coordinar las que llevan los demás fiscales. Igualmente, realiza una memoria anual, a partir de información de todas las provincias, la cual se ofrece al legislador y al ejecutivo para el diseño de políticas criminales en esta materia. Por otra parte, las secciones de criminalidad informática se encuentran en las fiscalías provinciales, excepcionalmente en fiscalías de área. En función de las necesidades en esta materia se han ido reforzando los servicios territoriales. Su dirección está a cargo del delegado provincial, que debe coordinar su servicio, potenciar la unidad de actuación en la provincia, coordinación de investigaciones, mantener el contacto dentro del territorio con fuerzas de seguridad y unidad de investigación, realizar un control de procedimientos y elaborar el informe anual que evidencia qué problemas se detectan.

Como conclusión, Tejada de la Fuente señala que las áreas de especialización tienen como objetivo: 1) La unificación de criterios interpretativos de normas penales y procesales; 2) El establecimiento de pautas uniformes de actuación; 3) La coordinación a nivel nacional de investigaciones; 4) Fuerzas y Cuerpos de seguridad (Instrucción 1/2008 FGE); 5) Seguimiento y control de procedimientos judiciales y diligencias de investigación, 6) Facilitar cooperación con otras instituciones y organismos y 7) La cooperación internacional. Finalmente, Tejada de la Fuente asegura que se están dando pasos en esta materia en una buena dirección aunque todavía falta mucho camino.

Comentarios de la relatora

La propia arquitectura de los sistemas informáticos y la dificultad de persecución y por ende de intervención del Derecho penal en el ámbito del ciberespacio, hace necesaria la especialización y de cooperación para combatir el cibercrimen. En el ámbito de la cooperación, coadyuvo lo señalado por la ponente en la posibilidad,

viabilidad y necesidad de reforzar la cooperación con América y en general una cooperación mundial. También es necesario en todo caso, para permitir "la alerta temprana"[5], difundir información de los nuevos métodos, patrones y herramientas de ataque para poder recomendar mecanismos de protección adecuados. Los problemas planteados en el ámbito del cibercrimen se presentan en materia sustantiva y procesal, se refieren a la jurisdicción y competencia de los tribunales, a la intervención de comunicaciones a través de sistemas informáticos, a la diligencia de entrada y registro con intervención de material informático y en general a la naturaleza y licitud probatoria de la información digitalizada[6]. Finalmente, cabe indicar que los esfuerzos del legislador en la tipificación de las conductas no alcanzan a solventar la problemática que se encuentra en constante evolución, lo que dificulta ofrecer una respuesta jurídica adecuada.

Tercera ponencia: "Aspectos de Derecho Público de la ciberseguridad"
Ponente: D. Alberto Torró Molés, Abogado del Estado, Jefe en León
Moderadora: Dña. María José Santos González, Departamento Jurídico INCIBE
Relatora: Dña. Marta González Aparicio, Investigadora en la Universidad de León

La tercera ponencia de las efectuadas en la primera jornada corrió a cargo de D. Alberto Torró Molés, Abogado del Estado Jefe en León, en mesa moderada por Dña. María José Santos González, perteneciente al Departamento jurídico del Instituto Nacional de Ciberseguridad –INCIBE–. La ponencia versó sobre los aspectos de Derecho Público de la ciberseguridad, y en la misma se realizó un análisis de la legislación administrativa aplicable en éste ámbito, la cual ha sufrido profundos y recientes cambios,-y así se destacó a lo largo de la exposición-, así como la forma en la que se aplica esta legislación y las perspectivas de futuro en relación a su desarrollo y resultados.

D. Alberto Torró inició su ponencia poniendo en relieve la estrecha relación entre el Derecho Público y la ciberseguridad, relación que en la ciudad de León se ha materializado en el convenio de colaboración suscrito entre el INCIBE y la Abogacía del Estado en León, colaboración que incide fundamentalmente en el asesoramiento y representación en cuestiones de índole jurídico.

El ponente destacó las importantes novedades legislativas que afectan de manera directa al Derecho público de la ciberseguridad, las cuales se condensan en dos textos legales de reciente aprobación:

[5] MOLIST, MERCÉ y MEDINA, MANEL. *Cibercrimen*. Barcelona. Tibidabo ediciones. 2015, págs. 195 y 202.
[6] FLORES PRADA, IGNACIO. Criminalidad informática. Valencia. Tirant Monografías. 2012, pág. 302.

1. Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
2. Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

A continuación, expuso con detalle el contenido de las reformas contenidas en sendos textos legales, así como la estructura y apartados más relevantes de cada uno de ellos.

En primer lugar, la Ley 36/2015, de Seguridad Nacional, la cual es fruto de diferentes esfuerzos, fundamentalmente los derivados de la Estrategia de Seguridad Nacional y de la Estrategia Nacional de Ciberseguridad. Como novedades destacables, el Título Preliminar de este texto legal incorpora una definición de seguridad nacional en su artículo 3, vinculando tal definición con distintos valores constitucionales, lo que ofrece sin duda una idea de la transcendencia de la misma y del calado de que el legislador la ha querido dotar. Así, el mencionado precepto señala *"A los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos"*.

Por otro lado, la Ley 36/2015 identifica en su artículo 10 lo que denomina "ámbitos de especial interés de la Seguridad Nacional", refiriéndose en primer término a la ciberseguridad. El mencionado precepto establece que tales ámbitos requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A fin de proteger estos extremos, este texto legal impone una serie de obligaciones específicas a las Administraciones públicas, las cuales recaen sobre los siguientes aspectos:

- Política de Seguridad Nacional (art. 4) y Cultura de Seguridad Nacional (art. 5).
- Conferencia Sectorial para los Asuntos de Seguridad Nacional (art. 6).
- Colaboración privada (art. 7) y participación ciudadana (art. 8).

El desarrollo de tales competencias es encomendado a distintos órganos de la Administración, por ello, el artículo 12 de la Ley 36/2015 delimita la estructura orgánica en esta materia, estableciendo los órganos competentes en materia de seguridad nacional, los cuales abarcan distintos niveles ejecutivos y legislativos, tanto en el ámbito estatal como autonómico.

El resto del articulado de la Ley se dedica a desarrollar el concreto sistema de seguridad nacional y la gestión de todas aquellas cuestiones relacionadas. Así, el Título II de la Ley 36/2015 delimita el "Sistema de Seguridad Nacional", mientras que el Título III se ocupa de la gestión de situaciones de crisis. Destacó el ponente en este apartado la importancia de la definición que establece el artículo 23 de la Ley de "situaciones de interés para la seguridad nacional", pues será en estas situaciones en las que las Administraciones encargadas de ello desplegarán las actuaciones

previstas para la gestión de crisis de seguridad en éste ámbito, las cuales, tal y como señala el antedicho precepto, se afrontarán *"a través de la coordinación reforzada de las autoridades competentes y bajo la dirección del Gobierno, garantizando el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles, no pudiendo suponer en ningún caso la suspensión de los derechos fundamentales y libertades públicas de los ciudadanos"*. Alude de este modo nuevamente el articulado de la Ley a los derechos constitucionales, estableciéndolos como límite a la gestión de tales situaciones de crisis.

Para que los distintos órganos de la Administración desempeñen los cometidos encomendados por este texto legal, y gestionen con eficacia las posibles situaciones de crisis, es necesario que los entes encargados del desarrollo de las actuaciones previstas en caso de amenaza a la seguridad nacional dispongan de los recursos necesarios para ello, por lo que el Título IV de la Ley 36/2015 prevé la contribución de recursos a la seguridad nacional, para lo que se establece un catálogo de recursos en el artículo 28 de la Ley, el cual debe ser aprobado por el Gobierno, mediante acuerdo del Consejo de Ministros, a propuesta del Consejo de Seguridad Nacional. Destaca el carácter heterogéneo de este catálogo, pues integra no sólo medios materiales de muy diversa índole, sino también recursos humanos.

En la segunda parte de la ponencia, el conferenciante centró su exposición en los aspectos con incidencia directa en el ámbito de la ciberseguridad contenidos en la Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas. Este texto normativo pretende extender la tramitación electrónica como regla general en las relaciones con el sector público en los distintos procedimientos administrativos, lo cual tiene evidentes consecuencias en el ámbito de la ciberseguridad. Por ello, el objetivo de la Ley en este punto es lograr mayor eficacia y eficiencia en la relación con la Administración a través de medios telemáticos, pero ofreciendo al tiempo mayores garantías para los ciudadanos en la gestión de estas relaciones, sobre todo en lo relativo a la protección de las comunicaciones realizadas con la Administración empleando la tramitación electrónica. Considerando tales objetivos, es clara la importancia y los efectos que despliega la ciberseguridad, a fin de proteger los datos y el contenido de tales comunicaciones.

El artículo 14 de la Ley 39/2015 plasma el objetivo supra señalado en relación a la generalización de la tramitación electrónica en las relaciones entre Administración y administrados en un doble sentido: como un derecho y como una obligación. Así, el artículo 14. 1 de la Ley señala que las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos, con lo que, en principio, deja al arbitrio de los administrados personas físicas la elección del modo en que van a llevar a cabo sus comunicaciones con la Administración. No obstante, el citado precepto, *in fine*, exceptúa esa libertad de elección en los casos en los sujetos estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas, añadiendo que el método elegido en un primer momento podrá ser modificado por el administrado a posteriori. No es éste el único límite a tal capacidad de elección del administrado persona física, pues el mismo artículo 14, en su punto 3, establece que las Administraciones podrán establecer la obligación de

relacionarse con ellas a través de medios electrónicos para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos, quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios. Por tanto, la Ley expresamente suprime la libertad de elección del medio para relacionarse con la Administración en varios supuestos, dejando la vía de las comunicaciones electrónicas como único camino posible.

En el caso de otros entes que no son personas físicas –personas jurídicas, entidades sin personalidad jurídica, aquellos que ejerzan una actividad profesional para la que se requiera colegiación obligatoria o que representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración y los empleados de las Administraciones Públicas– el artículo 14.2 de la Ley 39/2015 elimina tal posibilidad de elección en las relaciones con la Administración, estableciendo la obligatoriedad de comunicarse exclusivamente a través de medios electrónicos para la realización de cualquier trámite en un procedimiento administrativo.

El ponente prosiguió exponiendo cuáles son los derechos de los administrados en su relación con las Administraciones Públicas, previstos con el fin de garantizar la seguridad y protección de las comunicaciones llevadas a cabo a través de medios telemáticos, lo que afecta ya de manera directa a la ciberseguridad. Estos derechos, que aparecen enumerados en el artículo 13 de la Ley 39/2015, son fundamentalmente dos:

- Derecho a comunicarse con las AAPP a través de un Punto de Acceso General electrónico de la Administración (artículo 13.a) de la Ley 39/2015).
- Derecho a ser asistidos en el uso de medios electrónicos en sus relaciones con las AAPP (artículo 13.b) de la Ley 39/2015).

A continuación el conferenciante puso de manifiesto diversas exigencias contenidas en el texto de la Ley 39/2015, de carácter puramente práctico y que son claro ejemplo de lo que se puede denominar *electronificación* de las Administraciones Públicas. Entre estos ejemplos destacan la identificación y firma de los interesados (artículos 9 y 10 de la Ley 39/2015), el Registro electrónico de apoderamientos (artículo 6 de la Ley 39/2015), el Registro electrónico para cada Administración Pública (artículo 16 de la Ley 39/2015) y la práctica de las notificaciones (artículo 41 de la Ley 39/2015). Todas ellas son manifestación evidente del protagonismo de tales relaciones digitales y de la relevancia de los datos transmitidos a través de la red, y, por ende, de la importancia de su protección.

D. Alberto Torró Molés finalizó su ponencia valorando los efectos de las reformas normativas expuestas en el ámbito de la ciberseguridad, los cuales calificó de positivos y acordes al devenir de los tiempos, sin olvidar que para lograr su efectiva aplicación es necesario su posterior desarrollo reglamentario, así como la dotación a los organismos competentes de los recursos suficientes para desempeñar su cometido en esta materia.

Por último, se inició una ronda de preguntas en la que se plantearon dos cuestiones al ponente. La primera de ellas relacionada con la necesaria homologación de procedimientos debido a la internacionalización de Internet y si tal extremo se reconocía en la Ley 26/2015, de Seguridad Nacional, a lo cual D. Alberto Torró Molés respondió que, si bien no se ha previsto en la Ley 36/2015, si se contempla expresamente en la Ley 39/2015 que es necesario reconocer, aunque sólo en el ámbito comunitario, todos los certificados incluidos en el listado de servicios de confianza, a lo que añade que el reconocimiento extracomunitario requerirá de la celebración del convenio correspondiente, lo que no está exento de dificultad ya que Internet escapa de fronteras territoriales. La segunda de las cuestiones planteadas se refirió a si las comunicaciones llevadas a cabo con las distintas Administraciones Públicas, ya sean estatales o autonómicas, se desarrollarán a través de un registro común o de un registro propio para cada Administración, lo cual, según el ponente, va a depender fundamentalmente de la implantación y desarrollo de la Ley, si bien, en materia de registros electrónicos se prevé un registro para cada Administración Pública, incluso un registro para cada organismo público si así fuera necesario.

Comentarios de la relatora

El meteórico desarrollo de las Tecnologías de la Información y la Comunicación ha generado un nuevo sistema de relaciones caracterizado por la facilidad e inmediatez en las comunicaciones y en los intercambios de información. La rápida y masiva implantación de estas tecnologías en la sociedad actual, llegando a ser una constante en las relaciones de la más diversa índole, ha traído consigo la aparición de amenazas que provocan inestabilidad, pudiendo llegar a afectar a la propia seguridad nacional. Estos motivos hacen que la ciberseguridad juegue un papel primordial en su utilidad en el contexto de un Estado de Derecho, pues su garantía por parte del legislador sobrepasa la dimensión individual, alcanzando una magnitud institucional, lo que incide de manera inmediata en la seguridad colectiva. Tal parece ser la intención del legislador plasmada en la Ley 36/2015, de Seguridad Nacional, que prioriza la ciberseguridad y su protección como uno de los pilares en los que descansa la seguridad nacional.

Por otro lado, aunque del mismo modo, fruto del papel esencial que ocupan las nuevas tecnologías en el mundo actual, son importantes en este campo muchas de las novedades contempladas en la Ley 39/2015, de Procedimiento Administrativo Común. Este texto normativo prioriza la tramitación electrónica como regla general en las relaciones con la Administración, dejando a la tramitación en papel un carácter puramente supletorio. El fundamento de tales medidas, atendiendo a lo señalado por el legislador, es la mejora en la eficiencia en las relaciones entre Administración y administrado, así como el incremento en la seguridad jurídica, objetivos posibles, pero, en todo caso, supeditados al desarrollo de la Ley.

Tal desarrollo se configura como elemento decisivo, pues, si bien predecir el alcance y los resultados de la legislación contenida en sendos textos normativos resulta sumamente difícil en este momento, debido a su reciente aprobación, determinar su concreto alcance, tanto en el ámbito de la tramitación electrónica de los

procedimientos administrativos, como en el de la protección de la ciberseguridad, dependerá, sin duda, de los recursos y esfuerzos que las distintas Administraciones con competencias en la materia destinen a su desarrollo e implantación, tal y como acertadamente señaló D. Alberto Torró Molés.

Mesa redonda/Debate: "La privacidad y la ciberseguridad"

Participantes: Prof. Dr. D. Miguel Díaz y García Conlledo, Catedrático de Derecho Penal de la Universidad de León; Prof. D. Miguel Carriegos Vieira, Profesor Titular de Álgebra, Director del Instituto de Ciencias Aplicadas a la ciberseguridad; Prof. Dra. Dña. Esther Seijas Villadangos, Profesora Titular (acr. Catedrática) de Derecho Constitucional de la Universidad de León; Dña. María Marcos Salvador, Comisaria Jefe de León

Moderadora: Dña. Ana Belén Casares Marcos, Profesora Titular de Derecho Administrativo de la Universidad de León

Relatora: Dña. Mª Nieves Alonso García, Personal Investigador en Formación Homologado, Área de Derecho Constitucional de la Universidad de León

La moderadora inicia su intervención señalando que la privacidad es una preocupación constante y creciente en nuestra sociedad actual, global e internacional, de carácter interdisciplinar, y que resulta muy cambiante al chocar no sólo con la propia evolución de la tecnología sino también con la aparición de nuevas amenazas y preocupaciones por parte de los ciudadanos. No en vano, la privacidad se enfrenta a mantener un tenso equilibrio entre los derechos y libertades fundamentales del individuo, quien utiliza y comparte la información que considera pertinente y las necesidades de interés general y seguridad pública a todos los niveles.

D. Miguel Díaz y García Conlledo centra su ponencia en analizar las amenazas que para la privacidad suponen las múltiples actividades que se realizan en la red desde una perspectiva jurídico-penal. Su punto de partida es destacar el carácter fundamental del Derecho Penal como *ultima ratio*, poniendo de manifiesto la tendencia del legislador en la actualidad a que se convierta en *prima ratio*. Asimismo, y aun cuando la función del Derecho Penal sea eminentemente preventiva siempre llega tarde y si es una cuestión relacionada con la tecnología esa demora es superior, de modo que cuando interviene ya existen nuevas amenazas. El riesgo al buscar seguridad, y en este caso, ciberseguridad, es que no se superen y vulneren los límites y garantías que deben regir en el Derecho Penal y que no pueden olvidarse.

En nuestro Código Penal, y con anterioridad a la reforma de 2015, la privacidad se protegía en el artículo 197 en el que se tipifica el delito de descubrimiento y revelación de secretos. Tras la reforma LO 1/2015 se incluyen otras conductas

relacionadas con los medios tecnológicos, introduciéndose los artículos 197 bis, en el cual se abarca toda conducta de intromisión en todas sus variantes, el 197 ter, en el que se recogen los actos preparatorios de esas conductas, el 197 quater, que castiga especialmente el delito si se ha cometido en el seno de una organización o un grupo criminal y el 197 quinquies, que extiende la responsabilidad a las personas jurídicas. El artículo 197.7 responde a la tendencia del legislador a la mediatización del Derecho Penal, ya que este delito parece ser reflejo del mediático conflicto de la concejal de Los Yébenes, Olvido Hormigos, por la difusión de un vídeo íntimo en Internet sin su consentimiento.

Díaz y García Conlledo concluye abogando por que el recurso al Derecho Penal en la búsqueda de ciberseguridad se produzca respetando los límites que deben operar en esa rama del Derecho y, desde luego, no sea el que opere en primera línea, y porque además sea el propio individuo quien vele por la protección de su seguridad en la red, no exponiendo datos, imágenes o vídeos especialmente íntimos, para lo cual es muy importante una adecuada labor educativa. Asimismo, considera fundamental el desarrollo de medios técnicos, no sólo de protección sino también de investigación y recalca el importante papel que desempeñan las instituciones no jurídicas como las empresas tecnológicas o los centros de investigación.

Seguidamente, D. Miguel Carriegos, toma la palabra e incide en destacar los problemas que afrontan los investigadores en el uso de los métodos de investigación tecnológica por los límites legales a los que han de someterse. Destaca como uno de los problemas principales el uso del ordenador personal en el puesto de trabajo por la dificultad que supone establecer un equilibrio entre el uso de un mecanismo de propiedad privada en el puesto de trabajo y el acceso a un tipo de intranet que se ajuste a los requerimientos legales. En cuanto a la enumeración exhaustiva que realiza el artículo 197 CP, y como muestra de la rapidez en los avances tecnológicos, si bien se incluyen las emisiones electromagnéticas, en la actualidad, a través de ondas mecánicas puede llegar a saberse lo que se ha escrito en el teclado en un ordenador, quedando fuera de la previsión legal.

Desde el punto de vista de la investigación, lo especialmente valioso para que tenga un valor añadido es que la aplicación sea rápida, valiosa, ágil y sobre todo real. El principal problema al que se enfrentan los investigadores es la carencia absoluta de datos reales. Si los métodos de investigación no contrastan con datos reales no dejan de ser métodos puramente teóricos que no tienen el valor añadido necesario.

Carriegos sostiene que en países como Estados Unidos se garantiza la disposición de datos reales. Un ejemplo de ellos es el escándalo ENRON, una corporación americana, que mediante la manipulación de los mercados arruinó Estados como el de California. Fruto de esta actuación se inició una investigación en Estados Unidos, tras la cual se puso a disposición de los usuarios de Internet, todos los datos de los emails de los responsables con el objetivo de que los centros de investigación puedan analizar las redes sociales de quienes se dedican a la comisión de delitos corporativos. Este ejemplo sirve para poner de manifiesto que, en algunos Estados, como Estados Unidos, la publicación de estas colecciones satisface todas las garantías legales. En España, sería de especial importancia que se regulara la

utilización de este tipo de colecciones a fin de facilitar la investigación. Carriegos incide en la necesidad de que los profesionales del Derecho colaboren en la investigación tecnológica a través del establecimiento de una normativa que justifique la utilización de los datos con la finalidad de dotar a la investigación del valor añadido necesario.

Posteriormente, toma la palabra Dña. Esther Seijas Villadangos, quien aborda el tema de la privacidad y la ciberseguridad desde el punto de vista constitucional, centrando su ponencia en una referencia jurisprudencial en el marco europeo, estableciendo una micro teoría constitucional de la privacidad y la ciberseguridad y concluyendo con los retos que suponen la articulación de una nueva rama del Derecho, el derecho digital o derecho de las TIC's, derecho de internet o ciberderecho.

La primera referencia jurisprudencial a la que Seijas Villadangos hace mención es una sentencia del TJUE de 6 de octubre de 2015 en la que se declara la no compatibilidad de la Directiva 200/520/CE que permite la transferencia de datos personales desde la Unión Europea a Estados Unidos. En el origen de esta sentencia está un estudiante austriaco que en el año 2011 solicita a Facebook toda la información que tenga sobre él, recibiendo un informe de 1222 páginas repletas de datos, de grupos a los que había pertenecido y de chats en los que había participado. La clave de la resolución es la no compatibilidad de la citada Directiva con la protección de la vida privada y de las libertades y derechos fundamentales de las personas. El complejo *patchwork* que se atisba en la Unión Europea es complicado, a lo que se une la descentralización territorial en Estados como España o Alemania.

En cuanto a la aportación del Derecho Constitucional, Seijas Villadangos destaca el surgimiento del *habeas data* que se erige como paralelismo al *habeas corpus*, ciñéndose el primero a los aspectos internos de la libertad (la identidad de la persona, su autodeterminación, su intimidad…) y el segundo a la dimensión física y externa de la misma. El *habeas data* constituye una garantía constitucional de reciente creación cuyo objeto es la tutela de los derechos fundamentales derivados de la dignidad y el libre desarrollo de la personalidad bajo el pleno respeto a la vida.

En nuestra Carta Magna nada se habla expresamente de la protección de datos de carácter personal como un derecho esencial de la persona humana. La referencia más aproximada a la cibernética se encuentra en el apartado cuarto del artículo 18, que no estuvo exento de polémica en los debates constitucionales. Es en el año 2000, con la impugnación de la LOPD cuando se sustenta el derecho fundamental a la protección de datos. A fin de constituir una dogmática, Seijas Villadangos plantea el análisis de la naturaleza jurídica, los límites y la categorización de este derecho. En cuanto a su naturaleza jurídica, el Tribunal Constitucional lo declara un derecho fundamental autónomo con todas sus garantías. Cabría constituirlo como un derecho bifronte, por un lado, como un derecho instrumental que sirve para la defensa de otros derechos fundamentales como el honor o la intimidad y por otro, como un derecho fundamental autónomo, cuya finalidad es controlar el flujo de informaciones, concernientes a cada persona para preservar su identidad y el pleno ejercicio de sus derechos. Asimismo, el derecho a la protección de datos personales

se ancla en el artículo 10.1 CE. Por lo que respecta a los límites de este derecho, están orientados a garantizar la armonía y el equilibrio del orden social, con el respeto a los derechos fundamentales de terceros y la salvaguarda del interés público. Y por último, y en cuanto a la categorización de este derecho cabrá decir que nos hallamos antes de un derecho de cuarta generación que trasciende la categorización de derechos de Pizzoruso.

Como reflexión final, Seijas Villadangos aboga por la necesidad de avanzar hacia una clarificación en las fuentes con el objetivo de constituir una Carta global de ciberderecho, calificando a este derecho como un "derecho fotonizado" al que se exige evolucionar y adaptarse a su objeto de regulación a la velocidad de la luz, poniendo de manifiesto que se trata de un derecho en expansión, paralelo a la penetración del universo digital en nuestras vidas y que precisa de la colaboración interdisciplinar. En ese sentido, propone como reto del derecho global ocuparse de las dimensiones que implican trabajar alrededor de internet: la infraestructura o el soporte físico que permite transportar la señal, el código que aglutina los estándares y protocolos que garantizan su funcionamiento lógico y, por supuesto, el contenido.

Dña. María Marcos Salvador parte en su intervención de la función asignada a las Fuerzas y Cuerpo de Seguridad del Estado en nuestra Constitución, que conforme al artículo 104 es la de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. Asimismo, y partiendo de la misión encomendada constitucionalmente, destaca que la seguridad total no existe. En el ejercicio de sus funciones, el Cuerpo Nacional de Policía debe asumir como la primera de ellas, la prevención, centrando la misma en la protección a aquellos colectivos más vulnerables, entre ellos los menores, las personas inexpertas en las técnicas de navegación por la Red pero también a quienes las dominan porque no están exentas de peligros. La segunda de las funciones es la investigación de los delitos, tanto a instancia de parte como de oficio en virtud de la regulación prevista para el cumplimiento de dicha función en el Código Penal y la Ley de Enjuiciamiento Criminal fundamentalmente.

En relación con los delitos cometidos a través de la Red, en la década de los noventa, el Cuerpo Nacional de Policía constituyó grupos reducidos de expertos en delitos cometidos a través de medios informáticos. Debido a la dimensión que adquirieron estos delitos, surgió la necesidad de una mayor especialización, fundándose una Unidad Central, en sus inicios en las grandes ciudades (Madrid, Barcelona, Valencia y Sevilla), para desembocar en una Unidad Central dentro de la Comisaría General de la Policía Judicial. Las funciones de prevención e investigación se llevan a cabo tanto desde la Unidad Central como a nivel periférico, así por ejemplo la Comisaría de León dispone de un grupo especializado en delitos tecnológicos que extiende sus funciones a las otras tres comisarías de la Provincia (Astorga, San Andrés del Rabanedo y Ponferrada). El incremento de los servicios especializados en delitos tecnológicos responde al aumento en la comisión de los mismos, habiéndose producido un incremento del setenta por ciento en el último año y un doscientos por ciento en los últimos cuatro años, siendo el delito de estafa el que cuenta con un mayor número de casos.

Uno de los problemas a que se enfrentan estas unidades durante el proceso de investigación es que no sólo han de velar por la protección de los derechos de las víctimas sino también de los presuntos autores, razón por la cual se ha creado una unidad especializada en la Comisaría General de la Policía Científica cuya función principal es la informática forense. Asimismo, durante este proceso pueden obtenerse evidencias tanto de un delito informático como de otro tipo de delitos que se estén cometiendo a través de los medios informáticos como pueden ser la trata de personas con fines sexuales, el tráfico de drogas, secuestro o amenazas. El análisis de evidencias ha de cumplir tres especificaciones básicas: la recogida de las mismas debe llevarse a cabo por medios fiables, probados y reales, no deben ser alteradas bajo ninguna circunstancia y debe mantenerse siempre la cadena de custodia. El Cuerpo Nacional de Policía desempeña su misión dentro de la legalidad, con el respeto a la Constitución Española, el Código Penal, La Ley de Enjuiciamiento Criminal y los Convenios Internacionales ratificados por España, siendo de especial importancia la cooperación en este ámbito.

Comentarios de la relatora

A modo de conclusión, y desde la perspectiva del Derecho Constitucional, el reconocimiento por el Tribunal Constitucional del derecho a la protección de datos como un derecho fundamental autónomo con todas sus garantías es el basamento sobre el que se fundamenta la especial protección de la privacidad. Conforme a su naturaleza jurídica, y a fin de velar por la protección de este derecho es necesario, dado su carácter interdisciplinar, la clarificación en las fuentes, tal y como establece Seijas Villadangos, a fin de constituir un Carta global de ciberderecho.

Cuarta ponencia: "INCIBE y la ciberseguridad en la abogacía"

Ponente: D. Francisco Pérez Bes, Secretario General de INCBE y abogado especialista en TIC

Moderador: Prof. Dr. D. Pedro Álvarez Sánchez de Movellán, Profesor Titular de Derecho Procesal de la Universidad de León

Relator: D. David Carrizo Aguado, Profesor Ayudante de Derecho Internacional Privado de la Universidad de León

Se inicia la sesión con la presentación del ponente que es llevada a cabo por el moderador de mesa, D. Pedro Álvarez Sánchez de Movellán. D. Francisco Pérez Bes es Licenciado en Derecho, con más de 15 años de experiencia en asesoramiento jurídico en actividades de negocio, focalizada en las últimas etapas en el ámbito del derecho de la publicidad y el cumplimiento legal y normativo relacionado con el juego *online*. Su perfil se complementa con su participación actual como miembro de la comisión jurídica del Consejo General de la Abogacía Española -CGAE-, la

vicepresidencia y secretaría de la Asociación de Expertos Nacionales de Derecho TIC –ENATIC– y la secretaría de la Asociación Española de Responsables de Comunidades *Online* y Profesionales del Social Media (AERCO-PSM). Destaca asimismo, su faceta como profesor universitario en materias como Derecho de Internet y las TIC, Propiedad Intelectual, Derecho de la Privacidad, Publicidad *online* y Comercio Electrónico. Además, ha sido galardonado con el Premio «Derecho en Red» al mejor perfil jurídico.

La ponencia comienza con una breve mención acerca de qué es y qué desarrolla el Instituto Nacional de Ciberseguridad -INCIBE-, tanto desde la perspectiva teórica como práctica esencialmente enfocada hacia el mundo de la abogacía. Se alude efímeramente a la celebración coetánea de ENISE (Encuentro Internacional de Seguridad de la Información) pues de manera paralela a estas Jornadas, los días 20 y 21 de octubre de 2015 en el Parador San Marcos de la ciudad de León, se llevó a cabo tal encuentro.

Pérez Bes recalca el inusitado impacto de las nuevas tecnologías en el desarrollo profesional del abogado. En el día a día, este colectivo se encuentra con numerosos problemas y lagunas normativas por ser una materia que presenta complejidad técnica y es de carácter transversal conllevando ello una difícil aplicación. La revolución digital en la que estamos inmersos ha cambiado radicalmente la forma de comunicarnos. El nuevo panorama, basado en las nuevas tecnologías y los dispositivos electrónicos, plantea nuevos escenarios en los que la privacidad o la seguridad informática corren peligro. Nacen continuamente nuevas iniciativas emprendedoras y nuevos modelos de negocios de base tecnológica basados en Internet y que necesitan de un asesoramiento especializado. Para ello, en el plano profesional del jurista ejerciente, se hace imprescindible la formación, pero no únicamente la formación jurídica sino que debe conocer las tecnologías existentes, las problemáticas que ofrecen el uso de las mismas así como en la medida de lo posible conocer y ser capaces de entender su funcionamiento. El "abogado digital", ante la normal falta de regulación en la que sustentarse, ha de ser además proactivo, adelantándose de este modo a los obstáculos jurídicos que puedan plantearse y evitando así posibles incumplimientos futuros.

En este punto, Pérez Bes, menciona a D. Orlando Ayala, presidente de Microsoft, pues es uno de los especialistas en temas relacionados con la inteligencia artificial. Con ello, lo que pretende es plasmar los retos que plantea su canalización legal en el marco de una sociedad global y en continuo cambio. Para enmarcar esta idea, expone al aforo asistente el proyecto que IBM tiene en marcha con el ordenador "Watson", que es una tecnología cognitiva que procesa la información más como un ser humano que como un ordenador. Introduce como interrogante que los procesadores informáticos comienzan a tomar decisiones y debemos pensar cómo va a afectar en nuestra sociedad trasgresora y cambiante. En el Derecho debemos hallar sendas repuestas, principalmente en materia de responsabilidad. Pérez Bes expone a modo de ejemplo, la eventual responsabilidad de un coche sin conductor o en el campo de la medicina, la negligencia cometida por una máquina inteligente. Se pregunta el ponente si se necesita una ley que regule este tipo de situaciones. En este

terreno, los códigos de conducta están adquiriendo bastante peso, pero se cuestiona si son suficientemente válidos para otorgar soluciones viables y seguras.

Seguidamente, el ponente desarrolla las líneas básicas del marco estratégico de ciberseguridad en España a través de los principios en los que se sustenta. En primer lugar, se encuentra la seguridad en las Administraciones Públicas, que la tiene asumida el Centro Criptológico Nacional –CCN–, organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración que sea especialista en este contexto. En segundo lugar, se hallan las empresas privadas, cuya seguridad está asumida a través de INCIBE; en tercer lugar, se sitúan las infraestructuras críticas que están custodiadas por el Centro Nacional de Protección de Infraestructuras Críticas -CNPIC-: este centro custodia y actualiza el Plan de Seguridad de infraestructuras críticas y el Catálogo Nacional de infraestructuras críticas. Y por último, todo lo relativo a la Defensa Nacional, la denominada «ciberdefensa», representada por los Ejércitos de tierra, mar y aíre.

A continuación, Pérez Bes expone como dato clave que la Agenda Digital para España es la que establece los objetivos generales que deben ser adoptados por el Gobierno en materia de ciberseguridad, y en esta sede INCIBE juega un papel fundamental. Además, como dato aclaratorio muestra la importancia que poseen los grupos de expertos en incidentes de seguridad informática; son los denominados CERT «*computer emergency response teams*». Al hilo de ello, ensalza la importancia de este último organismo en la seguridad del Estado; por ello existe un convenio de colaboración entre el Ministerio de Industria, Energía y Turismo y el Ministerio del Interior, cuyo objetivo es crear un CERT como herramienta de ayuda a empresas y particulares con el fin de asistir y apoyar ante el surgimiento de ciberataques. Las funciones principales del CERT se pueden sintetizar en base a tres criterios: lucha contra los ciberdelitos y el ciberterrorismo, la protección de las infraestructuras críticas, y por último, las labores de difusión, capacitación y formación.

En cuanto a la estructura en la que se apoya la Estrategia de Seguridad Nacional, Pérez Bes destaca los capítulos principales en los que se engloba: en primer término, el ciberespacio y su seguridad; en segundo lugar, el propósito y los principios rectores; como tercer y cuarto punto los objetivos de ciberseguridad y las líneas de Ciberseguridad Nacional, y por último se encuentra la Ciberseguridad en el sistema de Seguridad Nacional. Como elemento clave es apropiado indicar que el propósito fundamental de la Estrategia de Seguridad Nacional es la visión integradora basada en la coordinación de las diversas Administraciones Públicas, junto con el sector privado y los ciudadanos. Esa colaboración es el *quid* para el éxito de una ciberseguridad querida por y para todos.

Para continuar en el desarrollo de la ponencia, Pérez Bes centra su atención en la actividad de INCIBE. En cuanto al estatus jurídico, presenta la forma de sociedad anónima estatal dependiente del Ministerio de Industria, Energía y Turismo. Las

tareas para las que está capacitada la citada mercantil son básicamente las siguientes: dar respuesta a incidentes de seguridad, abarcando desde el ciudadano hasta el sector empresarial, poner en marcha iniciativas de colaboración público-privada para la mejora de los niveles de ciberseguridad en España, estudio de los riesgos emergentes para poder anticipar necesidades, adoptar medidas preventivas y, en definitiva, disponer de mecanismos de alerta temprana y todo ello bajo la coordinación con actores clave a nivel internacional en materia de ciberseguridad.

En lo que respecta al campo de la investigación que gira en torno a la ciberseguridad, el ponente indica la escasez de estudios que existen y anima e invita al auditorio a que se inicie en la búsqueda y exploración de todo lo que conlleva la ciberseguridad en los diferentes ámbitos y especialidades del Derecho.

Pérez Bes comenta que INCIBE también centra su atención en el plano formativo. En ese sentido, en la actualidad está desarrollando planes de ayuda para la celebración de másteres, estudios interdisciplinares, foros, etc., con el objetivo de impulsar el desarrollo de la ciberseguridad esencialmente en el tejido empresarial.

Como colofón, el ponente incide en la conexión que tiene el papel de la abogacía con INCIBE. Fruto de ello, está en vigor un convenio de colaboración con el Consejo General de la Abogacía Española –CGAE–, en el que alguno de sus cometidos principales son: trabajar e identificar necesidades de especialización, difusión y asesoramiento jurídico en la empresa, ampliar sectores de oportunidad tales como en el ámbito de los seguros, *compliance officer*, etc., además de la importancia de la responsabilidad social empresarial en este sentido.

En último término, D. Francisco Pérez Bes, agradece los esfuerzos que se han llevado a cabo para la consecución de estas "I Jornadas de Derecho y Ciberseguridad" celebradas en la Facultad de Derecho de la Universidad de León, y así da por concluida su conferencia.

Comentarios del relator

Gran parte de las transacciones y operaciones realizadas en Internet son internacionales, por lo que en tales situaciones hay presente uno o múltiples «elementos extranjeros». Ante este postulado se va a plantear la cuestión de determinar qué tribunales pueden conocer ante un eventual litigio y qué Derecho estatal debe regir en tal escenario. Los diferentes Estados cuentan con su propia organización de tribunales y sus propias leyes, por ello, la especificación de la jurisdicción competente y el derecho aplicable en los múltiples litigios con ocasión de la utilización de la red de redes, se materializará a través de las reglas de Derecho internacional privado.

La consecuencia jurídica más relevante del uso de Internet es la masificación internacional de los fenómenos jurídicos, pues un acto realizado a través de Internet tiene repercusión mundial. Desde la óptica *ius internacional privatista*, se deben encontrar criterios flexibles que estén sustentados en foros y puntos de conexión

abiertos. Lo anhelado sería hallar criterios adecuados que permitan a las partes la aplicación de una Ley concreta y previsible, para así evitar que todas las jurisdicciones del mundo se consideren competentes y soslayar la incertidumbre acerca de la precisión del régimen jurídico de las actividades desarrolladas en Internet. Con ello, lo que se pretende lograr es que cada uno de los sectores destacados, además de las técnicas de autorregulación y mecanismos alternativos de solución de controversias, puedan ofrecer sendas respuestas en materias entre las que podemos destacar: el comercio electrónico internacional, la propiedad industrial e intelectual, las prácticas desleales, la responsabilidad extracontractual por actos verificados en Internet e infracciones derivadas de los derechos de la personalidad, la responsabilidad por productos defectuosos, los daños informáticos y la protección de datos personales.

Por tanto, el Derecho internacional privado debe proporcionar normas que eviten inseguridad jurídica, esencialmente en la protección de los derechos individuales y así impedir abusos por parte de los sujetos que poseen mayor poder en las relaciones negociales. Lo deseable sería la creación de un conjunto normativo de aplicación directa y con carácter universal que pudiera recoger un derecho uniforme de los aspectos jurídicos internacionales de Internet. Es lo que un sector mayoritario de la doctrina denomina "*International CyberLaw*".

Quinta ponencia: "Los ciberdelitos en el Código Penal"

Ponente: D. Avelino Fierro Gómez, Fiscal de Menores y Cibercriminalidad de la Fiscalía de León.

Moderadora: Prof. Dra. Dña. María Anunciación Trapero Barreales, Profesora Titular (acr. Catedrática) de Derecho Penal de la Universidad de León.

Relator: D. Juan Pablo Uribe Barrera, Investigador Contratado Predoctoral de la Universidad de León.

La moderadora, Dña. María Anunciación Trapero Barreales**,** presenta al ponente y da cuenta de su sobrada competencia académica, profesional e intelectual, para hablar con propiedad acerca de temas relacionados con la denominada "ciberdelincuencia".

El ponente toma la palabra e inicia su exposición agradeciendo la invitación a realizar su ponencia. Seguidamente, realiza un breve marco sociológico sobre el exponencial aumento de la importancia de diferentes tecnologías (internet, redes sociales, telefonía móvil de punta, entre otros) en la configuración de la vida social a partir de un par de anécdotas sobre la cuestión. Estos comentarios iniciales, que ponen de relevancia la vertiginosidad de estos cambios, serán complementados durante el desarrollo de la ponencia por múltiples observaciones y apuntes llenos de agudeza que enriquecen la visión sobre el asunto y terminan por englobar toda una

perspectiva de las transformaciones en la interacción social al ritmo de los avances de la tecnología y la comunicación.

Terminados tales comentarios, llenos de sentido crítico, se pronuncia entonces sobre la imposibilidad de realizar un abordaje exhaustivo de la cuestión anunciada en el título de la ponencia, manifestando así mismo que, en todo caso, tratará de hacer apreciaciones sobre la generalidad de los "ciberdelitos", concepto que reúne un ámbito de la criminalidad que, de acuerdo a una clasificación comúnmente aceptada por la doctrina mayoritaria, recoge: delitos de intrusismo informático (intimidad, apoderamiento de información, acceso no consentido, interceptación de telecomunicaciones), delitos contra la propiedad intelectual, daños informáticos, defraudaciones, falsificaciones y, por fin, otros delitos cometidos a través de internet (delitos contra la integridad sexual de menores o incapaces, *sexting*, *ciberbullying*, delitos contra el honor y delitos contra el patrimonio).

Habiendo introducido tal esquema, Fierro Gómez dio paso a una primera referencia normativa respecto a la regulación de cada uno de estos subconceptos. Así, subrayó que la reciente reforma legislativa (LO 1/2015) originó ciertos cambios en el abordaje del intrusismo informático, al realizar modificaciones sobre el art. 197 del CP, y, así mismo, en lo referente a los daños informáticos, tras las variaciones en el art. 270 del CP. En cambio, manifestó que en materia de defraudaciones (modalidad criminal que puede llegar a constituir hasta un 75% de los delitos informáticos) y falsificaciones la normativa ha permanecido sin modificaciones.

Luego de lo anterior, Fierro Gómez realiza un breve tránsito por algunas de las principales características de este tipo delincuencia, siendo señales de identidad frecuentes rasgos como el que se cometen a distancia, afectan a numerosas víctimas y, por último, tienen un componente de transnacionalidad. Estas características marcan a su vez ciertas particularidades de la respuesta estatal, que en el ámbito procesal busca ajustarse a las comentadas señas de esta delincuencia articulando redes de cooperación en la investigación de estas conductas, resultando de allí una estrategia que aún presenta retos evidentes pero que no obstante, a juicio del ponente, ha dado buenos resultados. Este éxito, sin embargo, no ha existido en la práctica de pruebas periciales técnicas, pues el trámite de las mismas aún es lento, y, así mismo, también sigue siendo de especial dificultad la identificación del delincuente cibernético por la utilización de herramientas tecnológicas que facilitan su anonimato.

Con posterioridad a la enunciación de tales características, Fierro Gómez centró entonces su atención sobre la reforma legislativa que se ha introducido para el abordaje de los ciberdelitos, misma que termina caracterizando como todo un "tifón legislativo". Sin que pueda realizarse una transcripción pormenorizada de cada uno de los análisis llevados a cabo, se tratará entonces de abordar un esbozo de los elementos transversales que componen las críticas del ponente frente a la Ley Orgánica 13/2015 por medio de la cual se introdujeron modificaciones en la Ley de Enjuiciamiento Criminal, y la Ley Orgánica 1/2015 por la que se modificó el Código Penal. Así, en ese orden manifiesta que este "tifón legislativo" tiene como rasgos el tener fallos técnicos por su redundancia, por su intención de dar más trascendencia

al lenguaje técnico que al jurídico haciendo más farragosa la lectura de la normas sin que ello implique verdaderos avances. Y, si ello es característico de la reforma procesal penal, en la parte sustantiva se aprecian serias deficiencias en la mirada sistemática del Código Penal y de los bienes jurídicos, fallos en la tipificación por mala técnica legislativa que hacen de difícil interpretación los alcances de las figuras delictivas introducidas (se generan dudas entonces sobre los sujetos activos de conductas como el denominado *sexting*, conducta cuya punición se categoriza dentro de lo que se ha denominado como "derecho penal de amigo"). De la mirada crítica que el autor realiza en este punto cabe en todo caso destacar una detallada crítica al nuevo art. 183 ter 2 del CP, por sus dificultades de interpretación e, igualmente, el detallado examen (con amplia exposición de los reparos doctrinales del caso) al nuevo art. 197.7 del C.P. En este orden de ideas, termina entonces el ponente por concluir que estamos ante una reforma innecesaria e ineficiente que no termina por resolver satisfactoriamente la cuestión del abordaje de la ciberdelincuencia, particularmente en lo que tiene que ver con los menores que reúnen calidades de víctima y agresores en esta clase de criminalidad.

Para finalizar, Fierro Gómez realiza un par de consideraciones que complementan el sentido crítico de la introducción de la ponencia y que tienen que ver con la desconfianza de este respecto al rol cada vez más protagónico que las técnicas de la información y la comunicación tienen en los procesos de interacción social de los jóvenes. En efecto, advierte el ponente sobre ciertas señas de alarma respecto a los déficits que pueden producirse respecto a la empatía, el desarrollo de habilidades cognitivas y la formación de tejidos sociales cuando los intercambios entre el sujeto y la comunidad se presentan al hilo de estas nuevas tecnologías que desplazan formas más tradicionales de integración social.

Comentarios del relator

Al margen de la elaboración de la reseña de la ponencia, quisiera, en un breve comentario, destacar un elemento que hizo presencia permanente a lo largo de todas las "I Jornadas Nacionales de Derecho y Ciberseguridad" y que tiene que ver con el papel que juega el derecho en una sociedad que cambia sus formas de interacción al ritmo de exponenciales transformaciones en el campo de las tecnologías y las comunicaciones. Se trata, particularmente, del rol secundario que tiene el derecho en el análisis y la regulación de toda una serie de variantes que se introducen al cambiar intercambios directos por la mediación de un computador, teléfono o cualquier otro aparato electrónico de este tipo, en relaciones comerciales, sentimentales, entre muchas otras. En efecto, parece ser que una de las lecciones que queda de esta jornada es que el papel del derecho es en todo caso subsidiario al necesario autocuidado y la reflexión que debe realizar la sociedad, cada uno de sus integrantes, acerca de estas cuestiones, pues es el momento idóneo para plantearse unos límites propios respecto a cuestiones como la intimidad, el manejo de datos, el buen nombre, y toda una serie de variables que surgen de la omnipresencia y omnipotencia de las tecnologías de las comunicaciones y su actual rol protagónico en el desarrollo del tejido social.

Sexta ponencia: "La ciberseguridad en el ámbito nacional"

Ponente: Prof. Dr. D. José Gustavo Quirós Hidalgo, Profesor Titular de Derecho del Trabajo y la Seguridad Social de la Universidad de León.

Moderador: Prof. Dr. D. Juan José Fernández Domínguez, Catedrático de Derecho del Trabajo y la Seguridad Social de la Universidad de León.

Relatora: Dña. Cristina Llamas Bao, Investigadora de Derecho Procesal de la Universidad de León.

Realizada la presentación del tema que va exponerse por el moderador, D. Juan José Fernández Domínguez, se cede la palabra a D. José Gustavo Quirós Hidalgo, quien se dispone a comenzar su ponencia señalando que se centrará en las implicaciones jurídicas que conlleva la ciberseguridad en el ámbito laboral, fundamentalmente en el uso que los trabajadores hacen de los medios tecnológicos y el control que a su vez hace el empresario para comprobar que su uso es correcto y sus consecuencias jurídicas.

Quirós Hidalgo explica que, en cualquier empresa, cualquiera que sea su actividad, los trabajadores utilizan teléfonos móviles, tabletas, discos duros, impresoras, escáneres, bases de datos, etc. Normalmente, todos estos medios son propiedad de la empresa pero que son puestos a disposición del trabajador para utilizarlos en la prestación del servicio. Obviamente esto presenta innumerables ventajas pero también determinados riesgos de ciberataques en los que el factor humano es el elemento más importante, pudiendo ser externos, es decir, aquellos que den lugar a ciberdelincuencia o cibercriminalidad; o internos, aquellos en los que el propio trabajador de la empresa, por despecho, venganza o con ánimo de lucro, lleve a cabo esos ciberataques. En otros casos, es el propio trabajador, el que propicia o facilita, con un uso incorrecto de los medios, la posibilidad de ese ciberataque. A través del uso particular que de los trabajadores hacen de las TIC, se pueden generar multitud de daños para la empresa. Es por ello fácil pensar, que ante esta situación la empresa tenga algo que decir, o lo que es lo mismo, que esté justificado que ejerza un determinado control sobre el uso que de los medios tecnológicos hagan sus trabajadores.

En el ámbito laboral, ha existido una escasa y antigua regulación. Son dos los artículos del Estatuto de los Trabajadores que tendrían una implicación directa e indirecta en este ámbito: por un lado sería el artículo 18, que regula los registros en los efectos personales del trabajador. El típico supuesto sería aquel en el que se registra al trabajador para saber si ha robado algo de la empresa, pero este artículo contempla determinadas garantías, estableciendo el mismo, que debe respetarse la dignidad e intimidad del trabajador, realizarse el registro en el lugar y tiempo de trabajo y en presencia de los representantes de los trabajadores u otros testigos; y por otro lado, el artículo 20.3 en el que se reconoce el derecho o facultad del empresario para adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por parte del trabajador de sus obligaciones y deberes laborales, guardando su adopción y aplicación la consideración debida a su dignidad humana.

Teniendo en cuenta esta escasa regulación, son los tribunales quienes se han ido encargando de establecer unas reglas, que han de tenerse en cuenta por los trabajadores y las empresas a la hora de utilizar los medios tecnológicos como posible fuente de riesgo o peligro para la ciberseguridad de la empresa.

Estos criterios judiciales, han pasado por diferentes fases: un criterio inicial parte de una sentencia del Tribunal Constitucional del año 1995, en la cual había que valorar ese control empresarial a través de un triple criterio de proporcionalidad: 1) idoneidad, es decir, si esa medida o control era susceptible de conseguir el objetivo; 2) necesidad, o lo que es lo mismo, si no había otros medios menos dañinos o lesivos para los derechos del trabajador y, por tanto, ése era el que había que utilizar; 3) proporcionalidad en sentido estricto, es decir, que existiera un equilibrio entre los beneficios o ventajas que reporta ese control al empresario y los perjuicios de los bienes o derechos que están en juego. A partir de estos criterios, surgen multitud de pronunciamientos de los Juzgados y de los Tribunales Superiores de Justicia, siendo en muchos casos contradictorios, porque en definitiva valoraban, o bien, la propiedad de esos medios de la empresa, con lo cual entendían que siempre el trabajador estaba sometido a un control; o bien, se realizaba una interpretación permisiva, de tal forma que, si la empresa no decía nada, es decir, tanto si no lo autorizaba expresamente como tampoco lo prohibía, tácitamente estaba permitiendo el uso privado o particular de esos medios, con lo cual, no podría posteriormente ejercer controles dado que vulneraría los derechos de la intimidad o secreto de las comunicaciones. E incluso, dentro de esta misma corriente, habría criterios distintos, porque se entraría a valorar qué uso privado sería adecuado, cuándo empezaría un uso apropiado o razonable o cuándo un uso abusivo.

La segunda fase, vendría dada por una sentencia del Tribunal Supremo de 26 de septiembre de 2007 en el que se resolvió el siguiente supuesto de hecho: un trabajador que prestaba servicios en un despacho, en el que trabajaba con un ordenador, no tenía clave de acceso, con lo cual podría ser utilizado por cualquier otro trabajador. El ordenador estaba conectado a la red de la empresa. Siendo ésta la que sospechaba del mal funcionamiento que se estaba dando al mismo, una vez que el trabajador salió de su trabajo, se personó un técnico informático, comprobando que había un virus y que había visitado páginas pornográficas. Al día siguiente, se realiza el control estando el trabajador junto con el representante de los trabajadores, procediéndose a su despido.

Esta sentencia, según Quirós Hidalgo, vino a establecer tres cosas: el artículo 18 ET, no es aplicable a este tipo de controles, es decir, esas garantías de que se tengan que realizar en el lugar y tiempo de trabajo, con el representante de los trabajadores u otros testigos, afecta a los bienes personales del trabajador, dado que no se puede aplicar analógicamente a los bienes que son propiedad de la empresa y con los que se presta ese servicio. En segundo lugar, y acogiéndose a los pronunciamientos europeos, consagra el uso social de los medios tecnológicos, por lo tanto privado, de tal forma que si existe tolerancia empresarial, es decir, que si se viene dando ese uso social, la empresa admite tácitamente ese uso, creándose una expectativa de confidencialidad, que luego no puede vulnerar con esos controles la empresa, pero esto no impide, y así lo contempla el TS, que el empresario ejerza sus controles,

porque es una prerrogativa que tiene reconocida en el artículo 20 ET. Y en tercer lugar, por las exigencias de la buena fe contractual, la empresa lo que tiene que hacer es regular con antelación el uso de los medios tecnológicos, pero no sólo eso sino informar que va a realizar controles y determinar o concretar en qué van a consistir los mismos.

Una vez que estos criterios van siendo reconocidos por las empresas y proceden a establecer su regulación para evitar posteriores problemas, aparece una sentencia del TS del año 2011 que viene a completar una cuarta regla. Se trataba de un supuesto en el que la empresa había prohibido expresamente el uso privado de los medios tecnológicos, siendo el trabajador conocedor porque se le había entregado un documento y habiéndose firmado por aquél. El TS viene a precisar la última regla anterior, en el que si existe una prohibición del uso particular de las nuevas tecnologías, ello lleva implícito directamente una posibilidad de control, y por tanto, no es necesario de que se avise de que se van hacer controles, ni qué tipo de controles van a realizarse.

En otra fase posterior, el TC, en dos sentencias recientes, mantiene esta doctrina pero añade dos precisiones: 1) si existe prohibición expresa, el control es legítimo porque se ha utilizado un medio de la empresa y por tanto, debe considerarse como un canal abierto, o lo que es lo mismo, que el control de la empresa está por encima del secreto de las comunicaciones 2) si ya está tipificada como conducta sancionable en el convenio colectivo, eso implica una prohibición expresa del uso particular de los medios, lo que implica que el empresario, ya ni siquiera tiene que regularlo y tampoco tiene que advertir que tiene que hacer esos controles.

Aprecia Quirós Hidalgo que a partir de estos criterios se puede llegar a la reflexión de que la empresa posee amplias facultades para controlar el uso de los medios tecnológicos y mantener seguridad de su ciberespacio bien, de forma unilateral, elaborando documentos donde figuren reglas de uso o bien, a través de la negociación colectiva, siendo más aconsejable, desde su punto de vista, la negociación colectiva, regular a prohibir, dado que estas conductas digitales han tenido hasta ahora, su correspondiente versión analógica (leer el periódico, tomar el café…), añadiendo que el INCIBE impulsa, ayuda y ofrece múltiples opciones para ejercitar este control y concluye que, en cualquier caso, el incumplimiento de las obligaciones por parte del trabajador da lugar al ejercicio de la potestad disciplinaria del empresario, pudiendo exigir responsabilidad por daños y perjuicios en caso de que el daño se haya materializado por conductas dolosas o negligentes del trabajador, y siendo, cada vez más frecuente estas últimas, puede explicarse el auge de figuras como el "ciberseguro" o la contratación de servicios externos como empresas de ingeniería o informática.

Comentarios de la relatora

A colación con lo anteriormente expuesto, he de señalar por lo que a mi campo de investigación se refiere que, desde un punto de vista procesal, la Ley 13/2015 de 5 de octubre modifica la Ley de Enjuiciamiento Criminal con la que se pretende

"renovar" nuestra legislación adaptándose a las recientes formas de delincuencia surgidas del uso de las nuevas tecnologías, reforzándose las garantías procesales tantas veces discutidas en la intervención e investigación tecnológica amparadas en los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

Séptima ponencia: "La neutralidad de la red"

Ponente: Prof. Dra. Dña. Mercedes Fuertes López, Catedrática de Derecho Administrativo de la Universidad de León.

Moderadora: D. Ignacio Martínez San Macario, Abogado, Vocal de ENATIC.

Relatora: Dña. Tamara Álvarez Robles, PDI en formación de la Universidad de León.

El moderador, D. Ignacio Martínez San Macario, presenta a Dña. Mercedes Fuertes López como una persona ilustre, y enfatiza, más allá de su contribución al Derecho, su compromiso social, el cual se refleja en parte de las publicaciones en los medios de comunicación, señalando la larga trayectoria profesional de la ponente da paso a la misma para que nos introduzca en su conferencia, titulada *"Neutralidad en la Red"*.

Comienza Fuertes López manifestando la importancia de abanderar la neutralidad en la red. Hemos mordido la manzana de Internet, lo que no está en Internet parece no estar en el mundo. Internet está originando una transformación social en casi todos los aspectos de la vida, incluida la afección de los derechos más personales y fundamentales. Las libertades públicas han sido tocadas, afectadas por Internet desde donde se producen censuras por parte de los Gobiernos o se nos ofrece como una herramienta delictiva para lesionar intereses personales y patrimoniales de forma rápida. Numerosos son los riesgos que corremos; troyanos, gusanos, infinidad de virus, programas espías…hacen imprescindible que reclamemos seguridad en la red, seguridad en Internet a través de instituciones tales como el INCIBE, a través de la regularización en aras a proteger infraestructuras estratégicas, de nuevos y mejorados protocolos, de medidas de seguridad como son las encriptaciones o la firma de Convenios internacionales similares al Convenio de Budapest.

Esta seguridad reclamada, señala Fuertes López, es necesaria e imprescindible para el desenvolvimiento de la sociedad actual, dependiente de Internet. Empero, junto a esa seguridad, las banderas que hemos de levantar son las banderas de la Libertad e Igualdad en el proyecto de hacer un Internet abierto y libre. Hemos llegado al desarrollo de Internet gracias a personas, científicos, generosas que han garantizado y posibilitado mediante sus investigaciones Internet y, actualmente se corre el riesgo de que grandes multinacionales de las telecomunicaciones impongan sus reglas por encima de estos derechos, por encima de la igualdad y la libertad.

Aún no se han conseguido aprobar aquellos instrumentos necesarios para garantizar un mercado único digital, es por ello que nos falla y por lo que algunos defendemos la bandera de la neutralidad. Defender la neutralidad de la Red es, por tanto, tratar de asegurar una mínima igualdad de los ciudadanos, que no se discriminen de manera arbitraria las nuevas iniciativas empresariales y, sobre todo, que no se afecten los derechos fundamentales y las libertades públicas, como la libertad de expresión, de información o la de comunicación. La Comisión Federal de Telecomunicaciones definió esta neutralidad de Internet o en la Red como la conjunción de cuatro libertades básicas: la libertad de acceso a los contenidos que elija el consumidor; la libertad de usar las aplicaciones que cada consumidor elija, lo que tiene como corolario que las empresas que creen aplicaciones deben tener la confianza de que sus productos funcionarán sin discriminaciones; la libertad para conectar los dispositivos personales, y la libertad para conocer las condiciones y cláusulas de los servicios que han contratado, como las distintas opciones de servicio, los programas que les protegen de virus, espías o garantizando su intimidad.

De este modo, prosigue Fuertes López, la libertad de los usuarios y la transparencia en la gestión de las empresas, prohíben prácticas de bloqueo de contenidos, aplicaciones, servicios o dispositivos, impiden discriminar de manera arbitraria el tráfico legal de datos, etc. Si bien, destaca ésta última característica, el trato y/o tráfico de datos, su gestión, como uno de los principales pilares en los cuales se apoya la neutralidad de la Red. Los datos han de ser transmitidos en igualdad de condiciones, sin establecer prioridades, sin postergar informaciones, y con independencia de su origen y destino. Cierto es que se han de tener en cuenta los mecanismos que regulan o establecen la distribución del tráfico de datos, para de ese modo no quedar abrumados por la cantidad de información recibida, de spam, etc. Esta gestión de datos, en todo caso, habrá de operar bajo el principio de proporcionalidad, para que la misma no derive en pactos colusorios, como sabemos restringidos por el Derecho de la competencia.

Los peligros de no defender la neutralidad en la Red han de ser conocidos, existe el riesgo de que estos datos sean discriminados en favor de beneficios empresariales, que las empresas de telecomunicaciones puedan impedir el acceso a determinados canales de información, servicios o aplicaciones en función del dispositivo de conexión o la compañía, e incluso que afecten a la exigencia de contraprestaciones a las empresas prestadoras del servicio.

Fuertes López afirma que no defender la neutralidad de la Red conduciría a permitir la colonización de muchos espacios, a fragmentar Internet, a consolidar el incremento de cotos cerrados para determinados usuarios, no habría innovación al romperse el alma de Internet. Es por ello que resulta indisponible la regulación y puesta al día por la Unión Europea en estos términos, dado que existe un considerable retraso, si tomamos como referente el caso de Estados Unidos de América. Urge que la Unión Europea afronte con decisión la defensa de los derechos y libertades de los ciudadanos en Internet frente a las grandes empresas de telecomunicaciones y servicios, mediante la observancia de los derechos relativos a la intimidad, a la dignidad, a la información, a la comunicación e incluso a la libertad de empresa.

Desde el Derecho de la Unión se están haciendo grandes esfuerzos para responder a esta nueva circunstancia, estos retos y problemas, sin embargo, sostiene Mercedes, son insuficientes debido a la complejidad, temporalidad y territorialidad de los instrumentos Estatales, y ello a pesar de las Directivas aprobadas en 2009 y que se conocen como "*Paquete Telecom*", Directivas 2009/136 y 2009/140.

Junto a ello, señala Fuertes López, que la Unión Europea se encuentra en un período de carencia dado que el Tribunal de Justicia de la Unión Europea, a fecha 8 de abril de 2014 en sentencia C-293/12 anuló una Directiva de Servicios, Directiva 2006/24/CE, que señalaba que las empresas operadoras habían afectado a la intimidad por haber mantenido en sus servidores distintos datos. Esta directiva tenía como principal objetivo armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

Estamos, asevera la ponente, en un período de cambio con esta protección, protección que ha de mantenerse, porque de no hacerlo, de no defender la neutralidad, se estaría admitiendo la supervisión de las comunicaciones, de las búsquedas, supondría tener que bajar la mirada y no ser tan dignos en ese horizonte que hemos conseguido, de conquista de libertad, de garantía de nuestros derechos.

Fuertes López concluye con una alusión a Rousseau quien en su libro *"Discursos sobre el origen y los fundamentos de la desigualdad de los hombres"* señala que cuando no se defienden esas garantías de oportunidad y de igualdad, se quiebran las oportunidades, se quiebra la igualdad y aparecen los abusos de poder, las posiciones dominantes y la pérdida de libertad. La calidad de nuestra democracia, afirma Dña. Mercedes Fuertes López, depende ahora mismo de que internet sea abierto, libre, y en eso somos todos responsables.

Comentarios de la relatora

Internet afecta directamente a nuestros derechos fundamentales: libertad, igualdad e intimidad. Estos son derechos que resuenan en el debate constitucional y comunitario. La necesidad de perfeccionar este ámbito hace indisponible el trabajo conjunto desde una perspectiva multidisciplinar que abarque no sólo las distintas ramas del Derecho, público y privado, sino también aquellas ciencias tecnológicas y de las telecomunicaciones. Junto al carácter multidisciplinar, la internacionalización y/o armonización de la normativa. Nos encontramos ante un reto global, internacional, que precisa del compromiso de los gobiernos y de las organizaciones internacionales, en aras a lograr la apertura y libertad de Internet, la prohibición de toda discriminación y la garantía de la ciberseguridad. Ello motiva el presente resumen de la ponencia de Dña. Mercedes Fuertes López.

Fuertes López, Mercedes, *Neutralidad de la Red ¿realidad o utopía?*, Ed. Marcial Pons, Madrid, 2014, ISBN 9788416212491.

Mesa de debate y conclusiones
Participantes: D. Francisco Pérez Bes, Secretario General de INCIBE, Abogado, Especialista en Derecho TIC; D. Avelino Fierro Gómez, Fiscal de Menores y Cibercriminalidad de la Fiscalía de León; Prof. Dr. D. José Gustavo Quirós Hidalgo, Profesor Titular de Derecho del Trabajo y la Seguridad Social de la Universidad de León; Prof. Dra. Dña. Mercedes Fuertes López, Catedrática de Derecho Administrativo de la Universidad de León.
Moderadora: Prof. Dra. Dña. Isabel Durán Seco, Profesora contratada doctora (acr. Profesora Titular) de Derecho Penal de la Universidad de León.
Relator: D. Alfredo Alpaca Pérez, Investigador Contratado Predoctoral de la Universidad de León.

Interviene en primer lugar, en la mesa de debate y conclusiones, Fierro Gómez, quien hace referencia a la ponencia presentada previamente por Fuertes López y plantea sus dudas con respecto a la existencia de la libertad de empresa en la red. Asimismo, alude al tema del "control parental", escenario que permite plantear la pregunta de si los padres pueden intervenir en la información de sus hijos (revisar su ordenador, por ejemplo) y en el que, desde una perspectiva teórica, podría interpretarse desde la perspectiva de una causa de exclusión de la antijuridicidad. Este es un asunto, según Fierro Gómez, que resulta ser preocupante en la medida que no está resuelto jurídicamente, así como resulta preocupante, según Fierro Gómez, la supresión del derecho de corrección (desde diciembre de 2007, al haberse dejado de mencionar en el artículo 154 del Código Civil). Por otro lado, Fierro Gómez señala, con respecto a la reciente modificación de la Ley de Enjuiciamiento Criminal por la Ley Orgánica 13/2015, de 5 de octubre, que se ha producido una transposición, de forma acrítica por parte del legislador, de la Directiva 2006/24/CE y establece que no se puede investigar nada que no sea un "delito grave". Aunque no se encuentra a favor de esta modificación, Fierro Gómez señala que, afortunadamente, a partir de la reforma se va a dejar que se investigue y que no se vulnere un derecho fundamental (al secreto de las comunicaciones o a la intimidad) en el caso de cualquier delito cometido a través de medios tecnológicos. En todo caso, Fierro Gómez señala que los artículos modificados poseen muchas inseguridades y errores, por lo que difícilmente sean de utilidad a los prácticos.

Fuertes López interviene en segundo lugar, refiriéndose a la libertad de empresa, en la que puede encontrarse el dilema que se analiza en el Derecho público de la competencia y en el Derecho mercantil: ¿qué pasa con las nuevas iniciativas? Lo que se trata de hacer mediante el Derecho de la competencia es que los oligopolios no se consoliden, esto es, que haya nuevas iniciativas. Fuertes López destaca que en las resoluciones (sobre todo) de las Cortes americanas (aunque en España hay alguna) se ha conseguido que los distintos pactos entre operadores o empresas se declaren inválidos porque perjudicaban a una nueva iniciativa. Por otro lado, Fuertes López advierte la existencia del negocio de la determinación de los dominios. Esto, según afirma, equivale a «colonizar» internet. Fuertes López, propone, al contrario, una «colonización jurídica», la cual tendría que caracterizarse por ser llevada a cabo asegurando la defensa de derechos y libertades de los ciudadanos.

Seguidamente, se formulan en el público asistente algunas inquietudes sobre la libertad de empresa o la libertad en general en el ámbito de internet: ¿Cómo se podría plantear la regulación de la red si es que quien «tiene el mando» es una empresa privada ubicada en Estados Unidos? ¿Favorece realmente internet a la libertad? ¿Internet es una cosa pública o una cosa privada? Fuertes López niega la posibilidad de entender a internet como una cosa privada, y la califica como un gran conglomerado en donde confluyen cuestiones públicas y privadas. Internet es una gran red, aunque hoy existan diversos «bloques», diferenciados según los niveles de acceso que los países hacen posible (hay países que bloquean el acceso a determinada información en internet, y hay otros que permiten un acceso libre e ilimitado). Asimismo, según Fuertes López, no ha surgido un denominado "derecho global a internet". Si bien es cierto hay cartas de derecho (tanto en la Unión Europea como en España), la idea de la exclusividad de la gestión privada resulta discutible. Habría, en todo caso, que matizar por sectores: de las infraestructuras, de las obligaciones de servicios (obligaciones públicas que se imponen a empresas privadas), etc. Por todo ello, resulta discutible admitir una perspectiva reduccionista y afirmar en virtud de ella que internet se trata de una empresa privada. Fuertes López concluye señalando que hay suficientes instrumentos jurídicos para buscar un equilibrio (entre lo privado y lo público) en el ámbito de internet.

Ante las inquietudes, formuladas por el público asistente, relacionadas a la posibilidad de que el empleador pueda acceder a las comunicaciones privadas del trabajador cuando tienen relación con un proceso penal, toma la palabra Quirós Hidalgo, quien señala que, ante todo, se deben distinguir dos ámbitos: el del Derecho penal, correspondiente al ámbito público, y el del Derecho del trabajo, que rige el ámbito laboral, de carácter privado, y aplicable en el marco de un conflicto entre la empresa y el trabajador. A pesar de esta diferenciación, el legislador, en el ámbito de la Ley reguladora de la jurisdicción social, modificó el artículo 90.4, que establece que cuando el empresario quiera acceder a documentos o archivos (en cualquier tipo de soporte) que pueda afectar la intimidad personal u otro derecho fundamental del trabajador, tiene que solicitarlo. Lo que habría que analizar, según Quirós Hidalgo sería determinar si esa modificación legislativa quiere insertar en el ámbito laboral un criterio jurisprudencial (establecida en una sentencia de mayo de 2014) o de complementar lo que ya existe: por un lado se puede entender que cada vez que el empresario quiera realizar esos controles, tendrá que ir a pedir la autorización judicial, o, por el contrario –y esto parece ser más razonable, sobre todo teniendo en cuenta los criterios jurisprudenciales que ya están asentados–, entendiendo que si hay una prohibición expresa o una regulación en un convenio colectivo, donde haya una prohibición de uso privado de los medios, se pueda extraer de ello una inexistencia de expectativas de intimidad, por lo que la prueba consistente en los controles que haya efectuado la empresa debería ser perfectamente válida. De esta manera, en el escenario en el que la empresa quiera hacer un control, porque tiene sospechas de un determinado trabajador, y existe una regulación previa por medio de convenios colectivos, entonces la empresa podría acceder a la información del trabajador e incorporar tal información como prueba en el marco del proceso correspondiente.

Seguidamente se plantea, por parte del público asistente, la inquietud referida al hecho de que, así como el empresario pone a disposición del trabajador los medios necesarios para prestar sus servicios, el trabajador puede poner sus cuentas personales a disposición de la empresa para trabajar. Ante ello, ¿Existiría posibilidad de control total del empresario de la información personal o se requiere de una autorización judicial? ¿Qué tipo de control quiere la empresa? ¿Cómo se protege? Ante ello, Quirós Hidalgo reconoce que en la actualidad cada vez más se fomenta la utilización de medios particulares en el ámbito laboral, con lo cual se podría apreciar un mayor margen del derecho a la intimidad y del secreto de las comunicaciones. Pero, desde el mismo momento en que ese medio privado se pone a disposición del trabajo, obviamente habrá determinadas conductas que no puedan ser sancionadas. En todo caso, según Quirós Hidalgo, cuando una persona, de forma expresa pone sus medios particulares al servicio del trabajo, existe una "conexión de laboralidad". Evidentemente, no será posible impedir que un medio particular, además de ser utilizado para el trabajo, sea utilizado para cuestiones personales. Otra cosa es, según Quirós Hidalgo, que se utilice tal medio particular en horas de trabajo, etc.

Seguidamente toma la palabra Pérez Bes, quien señala que las cuestiones antes mencionadas tienen una importancia más profunda de lo que parece. Específicamente, se tratan de consideraciones que tienen que ver con la seguridad. Uno de estos asuntos es el concepto del "*insider*", esto es, un el caso en el que un ciberataque provenga no de fuera de la entidad, sino del propio empleado (o de un descuido del propio empleado). Aquí cobra importancia la labor preventiva de las compañías de tener la política laboral de posible control en caso de ser necesario, pero tal política de control debe haber sido establecida con anterioridad. Si se tiene esa política ya prevista, bajo la forma de un procedimiento bien establecido, para cuando ocurra el suceso (la filtración de un expediente electrónico en un despacho de abogados, por ejemplo), este podrá ser abordado con seguridad jurídica. Según Pérez Bes, en el escenario descrito, estará más cubierto el punto de vista de seguridad, que en un escenario distinto en el que ocurra un hecho y recién a partir del mismo comience a plantearse una política de seguridad. Pérez Bes busca destacar entonces el concepto de "*insider*", pues se trata de un concepto que, en su opinión, aparecerá con asiduidad por desgracia. De esta manera, desde el punto de vista laboral resulta ser mucho más importante de lo que parece el hecho de tener regulado un determinado sistema interno de seguridad para abordar de manera eficaz cualquier escenario o incidencia en el que estén involucrados empleados de un despacho, compañía u organización.

A continuación el público asistente formula la inquietud consistente en la falta de convencimiento, en el ámbito de la sociedad, de la relevancia penal de una conducta que resulta ser repetida de manera reiterada, como puede ser la difusión de material privado de terceras personas a través de internet o de medios electrónicos. Fierro Gómez toma la palabra y señala, en primer lugar, que un ilícito no puede crear costumbre. Por ello, no se podría alegar la reiteración de una determinada conducta para desvirtuar la relevancia penal de la misma en el caso concreto. Asimismo, Fierro Gómez somete a consideración de los asistentes la idea relacionada a la posibilidad de criminalizar el denominado "*sexting*" (envío de contenidos de tipo sexual –principalmente fotografías y/o vídeos– producidos generalmente por el

propio remitente, a otras personas por medio de teléfonos móviles), lo cual, desde su punto de vista, parece un asunto complejo, en la medida que, desde su punto de vista, sería más adecuado recurrir a mecanismos previos a la intervención penal: a la autorregulación, a la autocomposición y también a la autoconcienciación. En una red social muchas veces no se pueden reconocer los peligros de la misma (puede haber suplantación de la identidad, por ejemplo), e inclusive, según Fierro Gómez, se podría decir que el escenario propio de las redes sociales son "criminógenos". Se trata de un asunto, en realidad, vinculado con la educación (sobre todo de los jóvenes, en quienes los casos de "*sexting*" resultan ser más frecuentes).

En el público se formula la inquietud acerca si en la nueva regulación española o comunitaria existen mecanismos para proteger a los usuarios de las llamadas «puertas traseras» (secuencia especial mediante la cual se evitan los criterios de seguridad para acceder a un sistema). Toma la palabra Fuertes López, quien señala que en la actualidad todavía no se ha ultimado el procedimiento de los instrumentos normativos de la Unión Europea que van a impulsar el mercado único digital (sobre todo en las infraestructuras) y que inciden en esas nuevas condiciones de los prestadores de servicios (condiciones dadas por el Tribunal de Justicia). Fuertes López señala que en el ordenamiento español se mantienen disposiciones (se hace referencia a un procedimiento de reclamación de las controversias ante la Secretaría de Estado de Comunicación de los años 2005 y 2007), que regulan un procedimiento pensado en que las reclamaciones de los usuarios deben incluir las discrepancias sobre las condiciones de uso de esos programas.

En el público asistente se formula una inquietud sobre la relación entre la web "normal" y la denominada "web profunda". Toma la palabra Pérez Bes, quien señala que esta última está pensada para el anonimato, y, a partir de ello, para la realización de actividades delictivas con cierta impunidad, o con una impunidad aparente hasta el momento. Pérez Bes, sin embargo, advierte que las fuerzas y cuerpos de seguridad del Estado (como el FBI, en Estados Unidos) ya están navegando por esas redes para tratar de identificar qué tipo de actividades se llevan a cabo en la "web profunda", así como a las personas que realizan las mismas. No se puede negar que la "*deep web*" es un caldo de cultivo para llevar a cabo actividades ilícitas (venta de armas, de drogas, de órganos, etc.). La "web profunda" es una especie de "lugar sin ley". Frente a esta situación, la alternativa, según Pérez Bes, debe ser seguir regulando la web normal y seguir trabajando para que no haya un internet "paralelo", en el que algunas personas puedan llevar a cabo actividades ilícitas de manera impune.

Seguidamente, en el público asistente se formula la pregunta consistente en la insuficiencia de medios para hacer posible el combate a la delincuencia informática. Pérez Bes reconoce que, en efecto, los policías pueden no tener todos los recursos suficientes para hacer frente a la delincuencia informática, y que tampoco pueden no tener la capacidad ni disponibilidad económica que tienen otras instancias policiales. Evidentemente, se necesitan más policías preparados en temas informáticos, con más recursos, más medios y mucha más formación. Fierro Gómez toma la palabra y complementa lo señalado por Pérez Bes, aportando la idea de que tampoco existe una jurisprudencia amplia ni uniforme sobre asuntos fundamentales como el denominado "daño informático". Según Fierro Gómez, hay pocos medios y hay

pocos peritos, lo cual también contribuye a reconocer el estado jurisprudencial incipiente del combate a la delincuencia informática. Pérez Bes toma la palabra nuevamente y agrega que una de las soluciones que propone el Ministerio del Interior son los convenios de colaboración con el Ministerio de Industria (particularmente, con INCIBE). Así, afirma que se han desarrollado internamente herramientas (como la denominada "*ASASEC*", que es un proyecto europeo centrado en la lucha contra la pornografía infantil) que se ponen a disposición de las Fiscalías. El "ANASEC", por ejemplo, es una tecnología de reconocimiento facial y de reconocimiento de superficies, de manera que cuando la policía investiga un caso de pornografía infantil o pedofilia, la herramienta reconoce la fotografía o los vídeos y los pone en relación con casos antiguos, por lo que la policía podrá acceder a elementos que permitan vincular el caso investigado con casos anteriores (ya resueltos o en investigación).

Comentarios del relator

Las diversas intervenciones en la mesa final de debate han permitido a los asistentes completar la amplia visión que implica el abordaje jurídico de la cibercriminalidad y la ciberseguridad, así como las principales manifestaciones de estos fenómenos en la vida diaria y que por su creciente importancia, se consideran en la actualidad merecedores de una adecuada atención por parte de derecho. Los comentarios de los participantes en la mesa final permiten dejar en claro, a mi modo de ver, dos importantes asuntos. Primero, que las malas prácticas que algunos malos usuarios pueden llevar a cabo a través de la utilización de sistemas informáticos, bases de datos o plataformas en Internet, deben ser abordadas desde una perspectiva multidisciplinar, pues por los diversos ámbitos en que la tecnología de la información ha ocupado un lugar fundamental (laboral, salud, económico, educativo, etc.), se requiere inexorablemente la utilización de todas las herramientas jurídicas necesarias que no solamente concedan al buen usuario la garantía de una utilización libre y segura de los recursos informáticos que en la actualidad resultan irrenunciables, sino también para la contención del abuso de los mismos y la detección de las posibles malas prácticas (estafas informáticas, comercio ilegal de drogas y armas, transacción de pornografía infantil, etc.) que puedan llevar a cabo ciertos individuos. Segundo, que principalmente en el ámbito de la ciberseguridad y la cibercriminalidad se evidencia la necesidad de que el derecho se constituya en una materia en actualización permanente, pues de lo contrario su función de instrumento para la regulación de la vida de los ciudadanos en sociedad se volvería no en mucho tiempo obsoleta. El derecho (en sus diversas manifestaciones) debe erigirse, entonces, como un sistema en constante vinculación y realimentación con las más variadas expresiones de la innovación informática y tecnológica. La vía más adecuada para solucionar los variados problemas generados por el abuso de los recursos informáticos por parte de malos usuarios está estrechamente vinculada, entonces, con el desarrollo y mantenimiento un derecho "modernizado", con una óptima capacidad de rendimiento para garantizar la libertad y seguridad a los buenos usuarios que emplean los recursos y herramientas del ciberespacio con responsabilidad.