ACTA DEL SEMINARIO DE LA ASOCIACIÓN RED DE ABOGADAS Y ABOGADOS PARA LA DEFENSA AMBIENTAL CELEBRADA EN EL C.E.N.E.A.M. (Valsaín) los días 24 y 25 de octubre de 2025

El 24 y 25 de octubre de 2025 la Asociación Red de Abogadas y Abogados para la Defensa Ambiental (RADA) celebraron su reunión anual en las instalaciones del Centro Nacional de educación Ambiental, en Valsaín, Segovia, para tratar sobre problemas de ciberseguridad y cuestiones prácticas relativas al expediente electrónico.
En materia de ciberseguridad se llevaron a cabo dos ponencias, impartidas por profesores expertos de la Universidad de Oviedo, como son el doctor en ingeniería informática y redes, Don Xicu Xabiel García Pañeda y Don David Melendi Palacio. También se trató el régimen legal en materia de protección de datos, exigible a los abogados, a cargo de Doña Ana Isabel Rigueira García, responsable de protección de datos en ámbito sanitario, terminando la sesión del día 24 con una conferencia del abogado, socio de RADA, Don José Antonio Ballesteros Garrido, experto en materia de consumo, que ha llevado múltiples casos de estafas tecnológicas.

Don **Xicu Xabiel García Pañeda** instruyó a los asistentes sobre las medidas de protección necesarias para hacer frente a la inseguridad de las comunicaciones a través de la red de internet, que tiene su origen en el propio diseño inicial pues no fue diseñada para uso general global sino para uso militar. Para hacer frente a los problemas de seguridad se van haciendo parques que, aun así, arrastran huecos de seguridad, agravados por la falta de formación de los usuarios, que los hachers aprovechan para mover mucho dinero a través de fraudes. Últimamente vemos que incluso los gobiernos lo usan como arma de guerra, en un mundo globalizado, sin fronteras, en el que no existen testigos. Es como vivir en el lejano oeste, en el que el ciudadano está totalmente desamparado. La conclusión es que la ciberseguridad no existe como producto, no se puede comprar, es un proceso continuo de aprendizaje y actualización de herramientas que como parches se van creando. Un consejo es que cuanto menor rastro dejemos en internet, mejor, para limitar ser objeto de fraudes.

Por su parte, **Don David Melendi Palacio** hizo una exposición sobre lo que se entiende por Criptografía y sus servicios asociados, como garantía de la integridad, confidencialidad u autenticidad de los datos que se manejan mediante el uso de redes, así como sobre las herramientas que a tal fin están disponibles en este momento. Aseguró que en general las conversaciones en red no son del todo confidenciales, si bien en ese proceso continuo de aprendizaje en pro de la seguridad de las comunicaciones ilustró a los asistentes sobre medidas mínimas a adoptar para evitar los cada vez más frecuentes fraudes que se vemos por internet: utilizar un programa de contraseñas,

utilizar diccionario de palabras que no tengan sentido, conexiones VPN para grandes empresas, no utilizar wifis públicas, cifrar las unidades extraíbles, destruir soportes de copias como discos o casetes en vez de borrarlos, hacer copias de seguridad en varios soportes, uno de ellos en la nube, tener siempre actualizados los programas que usamos, encriptar los ordenadores, etc.

Don José Antonio Ballesteros Garrido, abogado consumerista y miembro de RADA expuso una serie de sistemas de fraude o estafa con utilización de medios tecnológicos que se vienen produciendo, con un gran incremento de casos año a año y con continua renovación de las estrategias y técnicas utilizadas, con una combinación de prácticas de ingeniería tecnológica y social. Entre ellas, expuso cómo se envían mensajes en que el emisor aparece falsamente identificado con un banco o institución que contienen alertas con enlaces a webs clonadas para capturar las claves de acceso y poder operar en ellas. Una vía complementaria es la recepción de llamadas en que el número de teléfono llamante aparece identificado falsamente como alguno de los servicios del banco, también con el fin de conseguir claves o autorización de disposiciones. Otra vía de fraude que explota debilidades de las medidas de seguridad de las aplicaciones y servicios de pago es la captura de las cuentas de cliente en distintos sitios de compras para poder realizar compras contra la tarjeta de la víctima, cuando no se exige doble autenticación de la operación por estar la tarjeta "toquenizada". Una práctica más, que aprovecha algunas malas prácticas bancarias en la concesión de crédito, es la solicitud de crédito a nombre de la víctima, para inmediatamente extraer el importe obtenido. También es frecuente que se convenza a la víctima para descargarse programas que permitan al atacante manejar a distancia su aparato, con la excusa de una previa alerta sobre una operación sospechosa en su cuenta bancaria o de supuestos sistemas de ganancias económicas seguras. Otro sistema fraudulento alternativo es la venta por internet de cursos de alto coste y financiados que supuestamente permitirían alcanzar conocimientos sobre técnicas de inversión o trading en bolsa que darían lugar a ganancias diarias. Alertó también sobre el riesgo de captura de correos electrónicos con facturas u otros documentos, en que el estafador altera los datos de la cuenta corriente de pago para lograr que éste se realiza a su propia cuenta, aprovechando descuidos en la seguridad de los servidores por los que circulan esos correos. Otros casos que mencionó son los del fraude del CEO, los del hijo que supuestamente perdió su móvil y se encuentra en apuros; el fraude del amor; las herencias de grandes fortunas que precisan de alguna ayuda para poder cobrarse; alertas de multas o expedientes sancionadores de la agencia tributaria o seguridad social. También se dan ataques como el bloqueo del ordenador para reclamar el pago de un "rescate", que puede ir seguido de sucesiones peticiones de importes crecientes.

Doña Ana Isabel Rigueira, formada como responsable en materia de protección de datos de carácter personal, como son los datos sanitarios hospitalarios, alertó a los asistentes, dada su condición de abogados que manejen datos de carácter personal, sobre la necesidad de implementar un sistema de protección de dichos datos, que cumpla los requisitos del Reglamento de Protección de Datos, de manera que ante una fuga de datos o una inspección de la Agencia de Protección de Datos, se pueda demostrar que se han tomado todas las medidas necesarias, previsibles y disponibles. Y es que, aunque se adopten dichas medidas, como se ha venido demostrando en anteriores ponencias, la plena seguridad no existe. La política de protección de datos comporta la implementación de un conjunto de operaciones para el cumplimiento de una finalidad que ha de estar definida, la identificación de un responsable del tratamiento, la evaluación del impacto y la notificación en caso de quiebra del sistema. Expuso recomendaciones y requisitos como la elaboración de una Memoria de Gestión de Riesgos, previa a la elaboración de la política de gestión, medidas de almacenamiento de datos como el cifrado de archivos, hacer auditorías de seguridad, terminando por recomendaciones sobre el uso de la inteligencia artificial dado que las generativas utilizan los datos que aportamos para obtener respuestas.

La segunda parte del seminario tuvo lugar el día 25 de octubre de 2025 y se dedicó a exponer los requisitos legales y problemas detectados por los abogados ambientalistas en los expedientes electrónicos confeccionados por las administraciones públicas, especialmente en materia de medio ambiente, dada la complejidad y tamaño de los expedientes que se manejan. Intervinieron como ponentes Doña **María Rubio Palomino**, abogada en ejercicio con experiencia en la generación de expedientes electrónicos, y Doña **Doña Elena Domingo Martín** , Jefa del Servicio Jurídico de Urbanismo del Ayuntamiento de Zamora.

Doña María Rubio Palomino centró su exposición sobre el "Régimen jurídico del expediente administrativo electrónico y su adaptación a las normas de interoperabilidad", analizando con especial hincapié los artículos 70, referido exclusivamente al expediente administrativo, 53 y 82 referidos al acceso y copia del mismo, así como los artículos 14,16, 26 todos ellos de Ley 39/2015 y a los artículos 46.2 y 52 del Real Decreto 203/2021, así como al Esquema Nacional de Interoperabilidad.

Puso de manifiesto que la Ley 39/2015 de procedimiento Administrativo Común es la primera ley de Procedimiento General (había otros presentes normativos, el ROF y la ley de 2007) que se ocupa del expediente administrativo, dedicándole un artículo específico, el artículo 70 que lo define, delimita su contenido, enumera qué documentos deberán necesariamente formar parte del expediente y cuáles no y establece la obligación para la administración del formato electrónico, así como los requisitos formales del mismo.

En cuanto a la obligatoriedad para la administración de que el formato del expediente sea electrónico, introdujo previamente la dualidad existente, en cuanto que hay sujetos obligados a relacionarse electrónicamente con la administración, enumerando los mismos y sujetos que no (pueden hacerlo si quieren y lo ponen de manifiesto o no), por lo que si los documentos del interesado ingresan en papel se digitalizan y si el interesado lo pide en papel se imprimen para entregárselos, pero el expediente que gestiona la Administración es obligatoriamente electrónico.

Explicó que el expediente electrónico debe cumplir las normas del Esquema Nacional de Interoperabilidad, debe incluir: 1.- Documentos electrónicos: Pueden ser individuales o agrupados en carpetas. Cada documento debe cumplir con la Norma Técnica de Documento Electrónico. 2.- Índice electrónico: Se genera automáticamente y recoge la relación de documentos que contiene el expediente. Este índice debe estar firmado electrónicamente para garantizar su integridad y autenticidad. 3.- Metadatos mínimos obligatorios: 4.- DIR3 del órgano responsable del expediente. 5.- Fecha de apertura del expediente. 6.- Clasificación del expediente. 7.- Estado del expediente. 8.- Tipo de firma. 9.- Interesados (opcional).
Destacó la importante Sentencia del Tribunal Supremos 566/2025 de 14 de mayo, en la que fija doctrina casacional sobre los requisitos de validez de los documentos electrónicos.

Al hablar del contenido, en particular de los documentos que la ley dice que no formarán parte del expediente, como todos los que contengan información auxiliar o de apoyo, enumerando una informes y notas internas, planteo una serie de cuestiones y dudas, entre otras, es la lista de los mismos que recoge el artículo abierta o cerrada?, así como la propia contradicción del artículo 70, cuando en esa lista excluye los informes internos, para más adelante decir salvo que se trate de informes, preceptivos (una norma jurídica ordena de manera expresa su solicitud) y facultativos (no están previstos en ninguna norma y el instructor juzga necesarios para resolver) por lo que planteó en alto la siguiente cuestión: -¿ qué otra clase de informes hay-?
Para concluir que sólo se podrán excluir del expediente aquellos informes que no tengan valor jurídico y que todos los documentos en los que se fundamenta la resolución deben constar en el mismo.

En cuanto a los requisitos formales del expediente para cuando en función de una norma éste deba ser remitido, tal y como expresa la literalidad del artículo 70.3, como son: completo, foliado, autentificado y con un índice también autentificado de los documentos que contiene, son exigencias que el expediente debe cumplir en todo momento, no sólo cuando se remita al juzgado, o al superior jerárquico en alzada, porque así lo dice la ley -

agregación ordenada de documentos- y, sobre todo, porque el interesado podrá en virtud del artículo 53 acceder a él en cualquier momento y solicitar copia (que se entenderá cumplida con la puesta de manifiesto), por lo que deberá cumplir con todos los requisitos de la remisión.

En cuanto al contenido del expediente que debe ser remitido a los tribunales destacó la sentencia del Tribunal Supremo 1336/2023, de 26 de octubre, en la que, aunque no era el motivo de casación sí especificó, en el fundamento de derecho tercero, como debe ser el índice del expediente administrativo.

La intervención de **Doña Elena Domingo Martín**, Jefa del Servicio Jurídico de Urbanismo del Ayuntamiento de Zamora se centró en la confección del expediente administrativo a nivel local, los problemas que plantea, en particular cuando los procedimientos, como son los urbanísticos, son muy complejos a lo que se añade que un buen número de ellos se iniciaron en papel con un numero de registro, y la implantación de golpe de la Administración Electrónica obligó a pasarlos a formato electrónico cambiando el numero de expediente. Explicó que la herramienta informática que utiliza el Ayuntamiento de Zamora es GESTIONA, la cual ya hace automáticamente un índice, que permite un acceso rápido al documento específico que se desea consultar, pues al guardar los documentos en el título ya figura una alusión a su contenido y tipo de documento. Si buen para que ese índice tenga utilidad, la unidad administrativa que tramita el procedimiento debe tener identificados y nominados todos los documentos electrónicos que componen el expediente. Otro problema advertido es el supuesto de las actuaciones urbanísticas que además de licencia precisan de autorización de uso excepcional de suelo rustico, pues este último procedimiento ha de incardinarse en el de concesión de licencia; en estos supuestos GESTIONA no distingue ambos procedimientos, que se tramitan en subcarpetas, al incorporar los documentos al Índice por orden cronológico, por lo que se mezclan los documentos de ambos procedimientos dificultando su comprensión para la persona y órgano que recibe el expediente.

Tras las anteriores intervenciones sobre el expediente electrónico se llevó a cabo un **Taller de abogados**, a modo de conclusiones, en el que se estudiaron casos concretos y propuestas para mejorar las malas prácticas detectadas en los expedientes que les llegan a los Tribunales, los cuales, en muchas ocasiones, ni están ordenados, ni indexados, ni disponen de títulos de los que se pueda deducir el contenido del documento. Ello obliga a hacer un trabajo excesivo y laborioso de "reorganización del expediente" - tras la lectura de miles de páginas- para poder entender el procedimiento seguido en vía administrativa, reorganización que no puede trasladarse al Tribunal, al ser de parte. Ello crea indefensión para los abogados pues, por una parte, temen que, en las condiciones que se presentan

los expedientes, el Juez que haya de dictar sentencia, se encontrará con las mismas dificultades a la hora de hacer una valoración razonada de los hechos. Por otro lado la entrega a los Tribunales de expedientes que no cumplen la ley, exige a los abogados requerir a la administración el complemento del expediente, una y otra vez, con el consiguiente retraso del procedimiento. Es muy frecuente que obtener de la Administración un expediente más o menos entendible (mediante reiteradas solicitudes de complemento del expediente) retrase más de un año la tramitación del procedimiento.

Para evitar estas malas prácticas detectadas y facilitar la defensa ambiental ante los tribunales, los asistentes, como abogados comprometidos con una defensa eficaz y efectiva del derecho proponen las siguientes medidas para que los expedientes electrónicos se adapten a la ley:

a) Confeccionar un documento con los requisitos que tiene que reunir un expediente electrónico (incluyendo normativa y jurisprudencia de apoyo) que estará a disposición de los asociados a RADA .
b) Hacer una recopilación de resoluciones judiciales relativas a los problemas derivados de las malas prácticas detectadas para lo cual se solicitará la ayuda de las propias salas de lo contencioso-administrativo de los tribunales y de los colegios de abogados, con arreglo a un modelo de solicitud que se redactará por RADA.
c) Tras la recopilación de las anteriores resoluciones, hacer propuestas normativas y/o de mejora al Ministerio de Justicia y el Consejo General del Poder Judicial.
d) Difundir una nota de prensa sobre las conclusiones del seminario en cuanto a los expedientes administrativos.