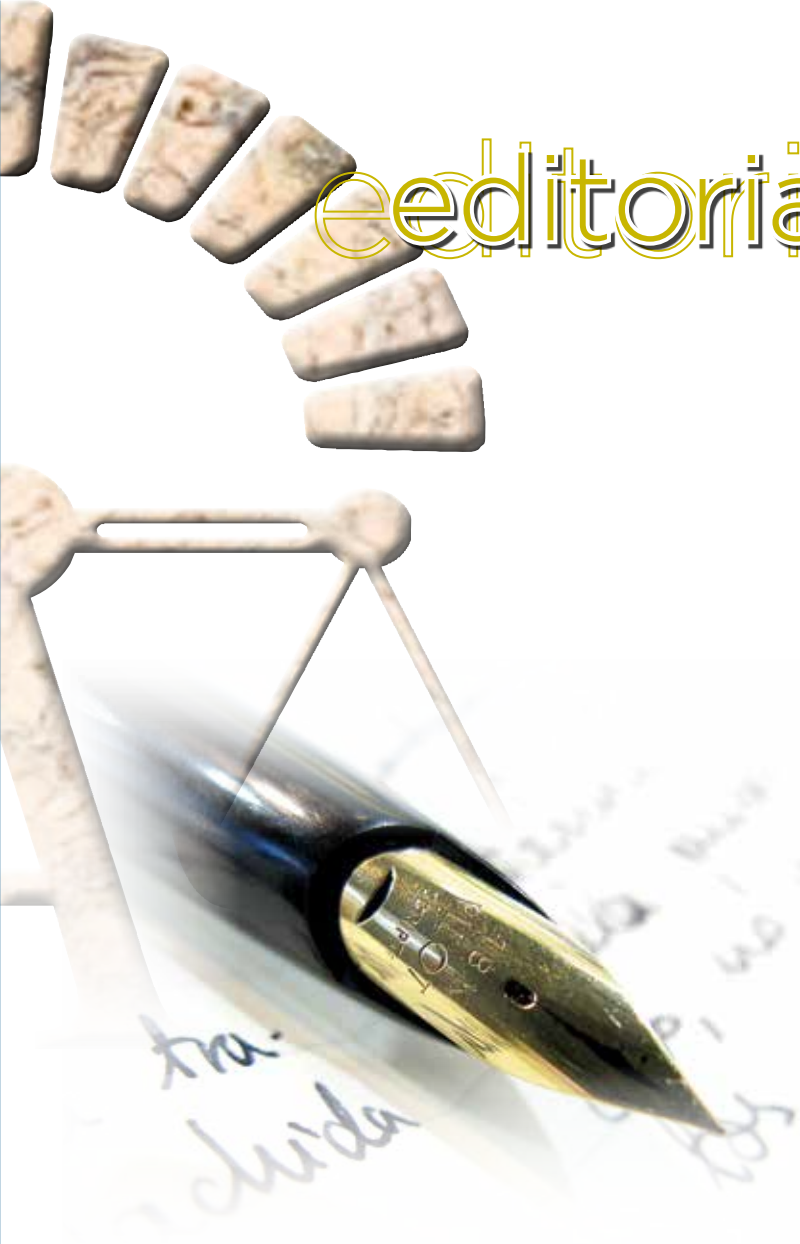
editorial



La protección de datos en los siniestros de tráfico

por **Javier López y García de la Serrana**
Director

En la era digital que vivimos, la protección de datos personales se ha consolidado como un derecho fundamental dentro del ordenamiento jurídico español y europeo, adquiriendo una relevancia sin precedentes. El marco normativo, articulado principalmente a través del Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), establece un riguroso sistema de obligaciones para quienes tratan datos de carácter personal.

La vulneración de esta normativa no solo expone a los infractores a significativas sanciones administrativas impuestas por la Agencia Española de Protección de Datos (AEPD), sino que también abre la puerta a la exigencia de responsabilidad civil. De este modo, cualquier persona que haya sufrido un daño material o inmaterial como consecuencia de una infracción de dichas normativas tiene derecho a recibir una indemnización del responsable o del encargado del tratamiento, configurándose así un nexo indisociable entre la protección de datos y el derecho de daños que obliga a los profesionales del derecho a dominar ambas disciplinas.

Para que una reclamación por daños y perjuicios derivada de la vulneración de la normativa de protección de datos pueda prosperar, la doctrina y la jurisprudencia exigen la concurrencia de cuatro elementos esenciales que deben ser acreditados por el perjudicado. En primer lugar, debe existir una infracción de la normativa, que puede manifestarse de múltiples formas, como el tratamiento de datos sin una base de legitimación válida, la vulneración de los principios rectores del tratamiento (licitud, lealtad, transparencia, minimización), el incumplimiento del deber de información, la falta de adopción de medidas de seguridad adecuadas o la cesión de datos a terceros sin el debido amparo legal. Seguidamente, es imprescindible la existencia de un daño, que puede ser de naturaleza patrimonial (pérdidas económicas directas) o no patrimonial, categoría en la que destaca el daño moral, entendido como el sufrimiento, la angustia o la zozobra generada por la pérdida de control sobre la propia información personal. En tercer lugar, debe probarse un nexo causal directo e inequívoco entre la infracción cometida y el daño sufrido, de modo que este último sea una consecuencia lógica de la primera. Finalmente, es crucial la correcta im-

putación de responsabilidad al responsable o al encargado del tratamiento, cuya identificación precisa es un presupuesto indispensable para el éxito de la acción, tal y como ha subrayado la jurisprudencia en casos complejos que involucran a grupos empresariales o plataformas tecnológicas.

La gestión de datos en siniestros de tráfico y el nuevo marco normativo

La gestión de siniestros de circulación representa un ámbito de especial sensibilidad, donde el tratamiento de datos personales, y en particular de datos de salud, es una constante. El nuevo «**TÍTULO V: Protección de datos personales» de la Ley sobre Responsabilidad Civil y Seguro en la Circulación de Vehículos a Motor** (LRCSCVM), incorporado a través de la Ley 5/2025, de 24 de julio, que introduce en el texto refundido de la norma los nuevos artículos 144 a 150, constituye un importante avance legislativo, pues aunque el objetivo de este título no sea regular ex novo esta materia, si viene a aclarar –tal y como se expresa en la propia exposición de motivos de la norma que lo incorpora- la aplicación de las normas existentes explicitando las bases jurídicas para los distintos tratamientos de datos personales.

Esta normativa sectorial viene a clarificar una cuestión largamente debatida, estableciendo una base de legitimación específica que permite a las entidades aseguradoras tratar los datos personales de los implicados en un siniestro, incluidos los relativos a la salud, sin necesidad de recabar su consentimiento expreso. Dicha legitimación, amparada en los artículos 6.1.c) y 9.2.f) del RGPD, se fundamenta en la necesidad del tratamiento para el cumplimiento de las obligaciones legales que la propia ley impone a las aseguradoras, como la valoración del daño y la formulación de la oferta motivada o si, en el caso de datos sensibles, el tratamiento es necesario para la formulación, ejercicio o defensa de reclamaciones legales.

No obstante, esta habilitación legal no constituye una carta blanca. El tratamiento debe ser estrictamente necesario, idóneo y proporcional para la finalidad de gestionar el siniestro, y las aseguradoras siguen plenamente obligadas a respetar los principios de minimización de datos, transparencia y seguridad, así como el deber de informar a los interesados sobre el tratamiento de su información personal, tal y como se desprende de los nuevos artículos 146 y 147 de la citada LRCSCVM.

El uso del correo electrónico y la diligencia en la comunicación de datos sensibles

En la práctica diaria de la gestión de siniestros, el correo electrónico se ha convertido en una herramienta indispensable para el intercambio de documentación entre aseguradoras, abogados, peritos y centros médicos. Si bien su uso agiliza notablemente las comunicaciones, también introduce un vector de riesgo significativo para la seguridad de los datos personales, especialmente cuando se transmiten categorías especiales de datos como los datos genéticos, biométricos, o de salud que pueden contener informes médicos o las historias clínicas.

Una brecha de seguridad, como el envío de un correo a un destinatario equivocado o el uso de canales no cifrados, puede exponer información altamente sensible y generar una responsabilidad directa para la entidad o el profesional que no ha actuado con la diligencia debida. La normativa, en particular los artículos 25 y 32 del RGPD, exigen la aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad para los derechos y libertades de las personas.

Esto implica la necesidad de adoptar protocolos robustos, como el cifrado de datos, el uso de plataformas seguras de intercambio de información y la verificación de la identidad de los destinatarios, tal y como se sugiere en el nuevo **artículo 147.3 de la LRCSCVM,** introducido por la Ley 5/2025. La falta de estas precauciones puede ser constitutiva de una infracción que, además de las sanciones administrativas, puede fundamentar una reclamación de responsabilidad civil por los daños derivados de la exposición no autorizada de la información.

El acceso a la historia clínica: límites y garantías

La historia clínica representa el núcleo de la información más sensible de una persona, un compendio de datos, valoraciones e informaciones sobre su estado de salud y evolución a lo largo de los procesos asistenciales, tal y como la define el artículo 14.1 de la Ley 41/2002, básica reguladora de la autonomía del paciente. Su naturaleza confidencial y su contenido, calificado como categoría especial de datos por el artículo 9 del RGPD, imponen un régimen de acceso y tratamiento extraordinariamente restrictivo, cuya fina-

lidad primordial es, y debe ser siempre, garantizar una asistencia sanitaria adecuada al paciente.

El acceso a la historia clínica con fines judiciales encuentra su amparo en el artículo 9.2.f) del RGPD, que levanta la prohibición general de tratar datos de salud cuando "el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial". En consecuencia, los jueces y tribunales están facultados para requerir la aportación de una historia clínica cuando lo estimen imprescindible para la resolución de un proceso, aunque deben ponderar la necesidad y proporcionalidad de la medida, tal y como se desprende del artículo 16.3 de la Ley 41/2002, de 14 de noviembre.

Una cuestión de especial relevancia, analizada en el dictamen 3/2025 del Consejo de Transparencia y Protección de Datos de Andalucía, es la solicitud de acceso por parte de las Fuerzas y Cuerpos de Seguridad (FCS) en funciones de Policía Judicial. Si bien el artículo 7 de la Ley Orgánica 7/2021 establece un deber general de colaboración, este cede cuando legalmente se exige autorización judicial. El dictamen, en línea con la jurisprudencia del Tribunal Supremo (sentencia 971/2022, de 16 de diciembre), concluye de forma tajante que para acceder a datos de la historia clínica que unifiquen la identificación del paciente con la información clínico-asistencial (es decir, datos no anonimizados), es imprescindible y preceptiva una autorización judicial expresa. La mera solicitud policial, aunque sea motivada, no es suficiente para legitimar el acceso a esta información tan sensible.

Incluso contando con dicha autorización judicial, el centro sanitario está obligado a cumplir con el principio de minimización (artículo 5.1.c del RGPD). Esto implica que no deben facilitarse datos de terceros que puedan constar en la historia, ni datos del propio paciente que no guarden relación directa con los hechos objeto de investigación. Si la orden judicial es genérica, el centro sanitario puede y debe solicitar al órgano jurisdiccional una aclaración sobre los términos y el alcance del acceso autorizado para no incurrir en una vulneración de derechos.

Una limitación fundamental al derecho de acceso, incluso para el propio paciente, la constituyen las anotaciones subjetivas de los profesionales sanitarios. El artículo 18.3 de la Ley 41/2002 establece que los profesionales partici-



pantes en la elaboración de la historia clínica "pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas". Estas anotaciones se entienden como impresiones o comentarios personales del facultativo que, si bien pueden tener trascendencia clínica, no se sustentan en datos objetivos. Esta reserva protege la libertad de criterio del profesional, pero en caso de reclamación o procedimiento judicial, serán en última instancia los tribunales quienes determinen la procedencia de su revelación.

El acceso a la historia clínica por parte de las compañías aseguradoras es uno de los puntos más conflictivos. La regla general es que se requiere el consentimiento expreso e informado del interesado. Dicho consentimiento suele recabarse en el momento de la suscripción de la póliza de seguro. En este sentido, el nuevo **artículo 145 de la LRCSCVM**, introducido por la Ley 5/2025, referido al tratamiento de datos personales en el marco de la celebración del contrato de seguro, establece en su apartado primero que: "Las entidades aseguradoras podrán pedir a los interesados que hubieran solicitado la contratación con aquellas del contrato de seguro regulado en la presente ley cuanta información resulte necesaria, idónea y proporcional para poder determinar y cuantificar el riesgo asegurado. Las entidades tratarán como responsables del tratamiento los datos facilitados con la finalidad de poder realizar la proposición de seguro establecida en el artículo tercero de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro, encontrándose el citado tratamiento amparado en lo dispuesto en el artículo 6.1.b) del Reglamento (UE) 2016/679".

En el contexto de las reclamaciones de responsabilidad civil, las entidades aseguradoras no tienen un derecho de acceso directo a la historia clínica. Su acceso a datos de salud se legitima, bien por el consentimiento expreso e informado del lesionado (art. 99.7 de la Ley 20/2015, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras), bien por la nueva habilitación del TÍTULO V de la Ley sobre responsabilidad civil y seguro, pero siempre limitado a la información estrictamente necesaria para la valoración del daño derivado del siniestro. En este sentido, el nuevo **artículo 147 de la LRCSCVM** sobre el tratamiento de datos de salud en caso de siniestro, establece en su apartado primero que "Las entidades aseguradoras podrán proceder como responsables al tratamiento de los datos relativos a la salud de los perjudicados que hubieran sufrido daños personales con ocasión de un siniestro con la finalidad de dar cumplimiento a la obligación legal de indemnización establecida en esta ley. El tratamiento por las entidades aseguradoras de estos datos, incluyendo el informe médico pericial definitivo, al que se refieren los artículos 7.3.c) y 7.4.b) de esta ley, y los resultantes de la asistencia sanitaria que hubiera sido dispensada al perjudicado y el seguimiento de su evolución, se encuentra amparado en los artículos 6.1.c) y 9.2.f) del Reglamento (UE) 2016/679, como consecuencia de la acción directa reconocida al perjudicado por el artículo 7.1 de esta ley y de ser necesario para atender a su derecho a la indemnización, y en el artículo 99.1 de la Ley 20/2015, de 14 de julio".

La AEPD en su Informe 526/2003, ha matizado esta regla para un supuesto muy concreto: la cesión de datos por parte de centros sanitarios *públicos* a compañías de seguros derivada de la asistencia prestada en *accidentes de tráfico*. En este caso, se admite que no se exija el consentimiento del afectado para ceder los datos imprescindibles para la facturación, al entender que la aseguradora es responsable legal del pago de dicha asistencia. Es crucial subrayar que esta excepción es de interpretación restrictiva y no ampara un acceso generalizado a toda la información clínica, sino únicamente a aquella estrictamente necesaria para justificar el gasto. Para cualquier otra información contenida en la historia, el consentimiento del paciente sigue siendo un requisito indispensable.

Por su parte, los tribunales se han pronunciado al respecto estableciendo claramente que para acceder a la historia clínica de una persona se exige una motivación jurídica reforzada, explicitando claramente cuáles son los motivos por los que debe excepcionarse la confidencialidad médico-paciente.

En este sentido, el **auto de la Audiencia Provincial de A Coruña de 25 de marzo de 2025** (dictado en el Recurso 49/2025), deniega el recibimiento a prueba en segunda instancia interesado por la aseguradora demandada, que solicitaba el acceso al historial clínica de la víctima del accidente de circulación. La sala de apelación considera que se trata de una documentación confidencial cuya solicitud no está debidamente justificada. En este sentido, enfatiza que el acceso generalizado a las historias clínicas de los litigantes no puede convertirse en una práctica rutinaria con una finalidad meramente prospectiva.

La intervención de detectives privados: entre el interés legítimo y el derecho a la intimidad

Es una práctica habitual que las entidades aseguradoras recurran a los servicios de detecti-



ves privados para investigar las circunstancias de un siniestro y verificar la veracidad de las lesiones reclamadas, especialmente cuando existen sospechas de fraude. Esta actuación encuentra su base de legitimación en el interés legítimo de la aseguradora para proteger su patrimonio y combatir conductas fraudulentas (artículo 6.1.f del RGPD). Sin embargo, esta potestad investigadora no es ilimitada y debe ejercerse con un escrupuloso respeto al derecho fundamental a la intimidad y a la propia imagen del investigado (artículo 18 de la Constitución), lo que obliga a los tribunales a realizar una cuidadosa ponderación basada en el principio de proporcionalidad. En este sentido, conviene recordar que la Ley 5/2014, de 4 de abril, de Seguridad Privada, establece en su artículo 48.3 que "en ningún caso se podrá investigar la vida íntima de las personas que transcurra en sus domicilios u otros lugares reservados". La jurisprudencia reciente ha sido clave para delimitar qué se entiende por "domicilio o lugares reservados".

La jurisprudencia ha ido perfilando los límites de estas investigaciones, estableciendo una clara distinción entre la observación en espacios públicos y la injerencia en la esfera privada. Así, resoluciones como la **sentencia de la Audiencia Provincial de Las Palmas de 17 de octubre de 2024** o la **sentencia de la Audiencia Provincial de Madrid de 4 de diciembre de 2025**, han considerado lícitas las grabaciones y comprobaciones visuales realizadas en lugares públicos o desde la vía pública, aunque capten la entrada a un garaje o el exterior de una vivienda. En cambio, la **sentencia de la Sala de lo Social el Tribunal Supremo de 25 de mayo 2023**, ha sentado una doctrina contundente al declarar ilícita la prueba obtenida mediante la grabación de un trabajador en el jardín de su domicilio, por considerar que dicho espacio, aun siendo visible desde el exterior, forma parte de la esfera de intimidad personal y familiar y goza de una expectativa legítima de privacidad, asimilándolo al domicilio a efectos de protección. La obtención

de pruebas en estos espacios privados sin consentimiento del afectado o sin la preceptiva autorización judicial constituye una vulneración de derechos fundamentales que no solo invalida la prueba, sino que puede generar responsabilidad civil para la agencia de detectives y para la aseguradora que la contrató.

La línea divisoria es, por tanto, clara: la investigación es lícita en el espacio público, pero se convierte en una intromisión ilegítima si invade la esfera de privacidad, que comprende no solo el interior de la vivienda, sino también espacios anejos como el jardín, donde el individuo tiene una expectativa razonable de no ser observado. Asimismo, el nuevo **artículo 146 de la LRCSCVM**, introducido por la Ley 5/2025, establece en su apartado tercero que "en caso de acudir a terceras entidades para la investigación, peritación y valoración de los daños, estas tendrán la condición de encargados del tratamiento de las aseguradoras, debiendo suscribir con las mismas el contrato o acto jurídico regulado por el artículo 28.3 del Reglamento (UE) 2016/679".

Por último, conviene recordar que el uso de dispositivos de seguimiento como balizas GPS constituye una injerencia en el derecho a la intimidad y, por tanto, requiere autorización judicial, tal y como se regula en el artículo 588 quinquies b) de la Ley de Enjuiciamiento Criminal, tal y como se ponía de manifiesto en el informe redactado por la Unidad Central de Seguridad Privada de la Policía Nacional (2016/014) de fecha 15-02-2016, sobre "Uso de medios de localización y seguimiento por detectives privados", que establecía las siguientes conclusiones:

"1. El detective privado debe actuar investido de habilitación en sentido amplio, por cuanto no solamente debe cumplir escrupulosamente las exigencias formales en su actuación profesional, sino que debe hacerlo mediante la legitimación que su contratante debe ostentar como derecho jurídicamente reconocido y que faculta al investigador para actuar.

2. La actividad del detective exige, como pilar básico, la obligación de defender los derechos de su cliente y los del sujeto sometido a investigación, con especial atención al derecho a la intimidad de éste, de acuerdo a lo establecido en el artículo 18 de la Constitución.

3. El derecho a la intimidad del sujeto investigado puede entrar en conflicto con derechos jurídicamente reconocidos en el contratante, lo que se resolverá mediante el juicio de proporcionalidad, que determinará si una intromisión en la esfera íntima tiene las exigencias de útil, necesaria y equilibrada.

4. El uso de medios técnicos debe ajustarse al juicio de proporcionalidad por cuanto puede suponer de intromisión en la esfera íntima del investigado.

5. El uso de dispositivos de seguimiento requiere de una orden judicial previa."

Como conclusión de este editorial, podemos decir que la interconexión entre la responsabilidad civil y la protección de datos es una realidad jurídica consolidada y en constante evolución, que exige a todos los operadores jurídicos una especial diligencia y un conocimiento profundo de la normativa aplicable. La vulneración del derecho fundamental a la protección de datos no es una cuestión baladí, sino que activa potentes mecanismos de responsabilidad que obligan al infractor a reparar íntegramente los daños causados, incluyendo el daño moral.

La reciente introducción del TÍTULO V en la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, a través de la Ley 5/2025, de 24 de julio, supone un hito normativo que aporta seguridad jurídica tanto al sector asegurador como a las víctimas, pero que, a su vez, refuerza la necesidad de actuar con estricto apego a los principios del RGPD. En este complejo escenario, los profesionales del derecho tienen un doble papel: por un lado, asesorar a sus clientes (aseguradoras, empresas, profesionales) para garantizar un cumplimiento normativo riguroso que evite no solo sanciones administrativas, sino también reclamaciones civiles; y por otro, articular las vías de reclamación más efectivas para la defensa de los derechos de los ciudadanos cuyos datos han sido tratados de forma ilícita, garantizando así la tutela efectiva de uno de los derechos más preciados en la sociedad actual.

Abril 2026