

FUNDAMENTOS DE DERECHO

PRIMERO: Sobre el planteamiento del litigio en la instancia.-

Es objeto del presente litigio la demanda que es formulada por los actores D. JUAN, D. JULIÁN, D^a M^a CARMEN, D^a PATRICIA, D^a JULIA y D. PEDRO, directamente encaminada a la obtención de la condena solidaria de las entidades codemandadas CARRITOS DEL NOROESTE S.L. y TOPSA S.L., por los daños y perjuicios sufridos, como consecuencia del acceso inconstituido a sus datos personales y bancarios, por parte de un tercero cuya identidad se desconoce, siendo utilizados los números y códigos CVN de sus tarjetas de crédito para realizar distintas compras, en varias páginas webs de comercio electrónico de países del Este, con la finalidad de adquirir productos informáticos. Las sumas que se reclaman, en las presentes demandas acumuladas, son las relativas a dichos cargos, más un 10% de su importe, en concepto de daño moral.

En la demanda se invocan los arts. 112 del TRLGDCU, 13 a 17 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, 12 y 19.1 de la LO 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, 1902 y 1258 CC, con cita de las correspondientes Directivas Comunitarias.

Por la parte demandada se solicitó la desestimación de la demanda, con base a los argumentos, que analizaremos en la fundamentación de esta sentencia.

SEGUNDO: Sobre los hechos declarados probados.-

A los efectos de la resolución de la presente controversia judicializada hemos de partir de los siguientes hechos, que expresamente se declaran probados, consecuencia de la actividad probatoria desplegada a instancia de los litigantes en aplicación del art. 216 de la LEC.

A) Los actores fueron clientes de la entidad codemandada CARRITOS DEL NOROESTE S.L., realizando diversas compras on line, en distintas fechas, a lo largo de los años 2014 y 2015, de productos para bebés, que comercializa dicha mercantil, tanto mediante atención personal en su establecimiento como a través de una página web.

B) Los demandantes en este proceso, navegando por la precitada página, eligieron los productos que les interesaban y pagaron mediante tarjeta de crédito. Los bienes adquiridos les fueron posteriormente remitidos a sus respectivos domicilios o lugares de entrega especificados, mediante servicio de paquetería. Por tales compras a distancia no se formula reclamación alguna en este proceso.

C) El sistema de pagos electrónicos de CARRITOS DEL NOROESTE S.L. fue diseñado por la mercantil WEBDESIGN, S.L., la cual utilizó, para ello, una herramienta informática denominada Secure Payment, que genera un fichero denominado "data.log", en el cual se almacenan los datos personales de los clientes, incluyendo sus números de tarjeta de crédito. Las medidas de seguridad empleadas en tal diseño eran las habituales en el mercado.

D) CARRITOS DEL NOROESTE tiene contratado el servicio de provisión de acceso a Internet con TELEFÓNICA, y aloja su página web (bajo el nombre de dominio www.carritosdelnoroeste.es) con el prestador de servicios de alojamiento TOPSA S.L., entidad que presta servicios de asistencia técnica y alojamiento de espacio en Internet a las empresas locales.

E) Así las cosas, a las 04.32 horas, de la madrugada del día 14 de noviembre de 2015, por un hacker, cuya identidad se desconoce, se llevó a efecto un acceso no autorizado a los servidores de TOPSA, con descarga de datos a una ubicación desconocida. Entre los ficheros ilícitamente transferidos se encuentra el denominado "data log", que contiene los números de tarjeta de crédito de 104 clientes, que utilizaron el servicio de pagos de CARRITOS DEL NOROESTE.

F) Por los referidos hechos se siguieron diligencias previas penales nº 2456/15, por delito informático, descubrimiento de datos personales y estafa, ante el Juzgado de Instrucción nº 2 de A Coruña, que fueron sobreesidas, al no haber sido identificado su autor, al haber usado complejas técnicas de enmascaramiento informático para ocultar su rastro.

G) Como consecuencia de ese acceso in consentido a los datos personales y bancarios de los demandantes, fueron utilizados, el mismo día 14 de noviembre, los números y

códigos CVN de sus tarjetas de crédito, con los cuales se realizaron distintas compras de productos informáticos, en varias webs de comercio electrónico de países del Este, y de esta forma, utilizando los datos de sus tarjetas se efectuaron cargos en las cuentas bancarias de los demandantes por los importes siguientes: a D. Juan 950,00 €; a D. Julián 825,00 €; a D^a M^a Carmen, 753,30 €; a D^a Patricia, 910,00 €; a D^a Julia 1.168,00 €; y, por último, a D. Pedro 1.750,00 €.

TERCERO: Sobre la determinación de la responsabilidad civil postulada en la demanda.-

En la demanda se solicita la condena de ambas mercantiles interpeladas, por lo que analizaremos individualmente la responsabilidad civil de cada una de ellas, y determinaremos, en su caso, si opera la solidaridad impropia, cuya aplicación se postula como fundamento de la demanda.

3.1 Análisis de la responsabilidad civil de la entidad CARRITOS DEL NOROESTE S.L.

En este caso, la reclamación no se fundamenta en el incumplimiento de sus obligaciones, derivadas de los contratos de compraventa a distancia concertados con los demandantes en este proceso, sino a consecuencia de la obtención y utilización torticera de los datos personales de los compradores -que fueron previamente facilitados por éstos a dicha mercantil para la adquisición de sus productos- por parte de un tercero o terceros, que efectuaron ilícitos y clandestinos actos de disposición sobre las cuentas anudadas a dichas tarjetas.

En la demanda se hace responsable a la precitada persona jurídica, por no haber adoptado las medidas de seguridad y protección necesarias para evitar el acceso a dichos datos personales por parte de terceros. La pretensión resarcitoria de los daños y perjuicios sufridos se fundamenta con apoyo en los criterios jurisdiccionales conformadores de la "ratio decidendi" de las SSAP Barcelona, Secc. 11^a, 214/2015, de 23 de julio [JUR 2015\232662] y Secc. 14^a, 151/2013, de 7 de marzo [JUR 2013\71665]), en casos de disposiciones llevadas a efecto, de forma ilegítima, por parte de terceras personas, sobre

las cuentas de los clientes depositadas en las entidades bancarias demandadas.

Mas, en el caso que nos ocupa, no existe dicha identidad de razón; puesto que los datos personales de los actores, que han sido objeto del ataque cibernético sufrido, han sido obtenidos mediante el acceso no autorizado a los datos guardados por TOPSA, en su condición de prestadora de servicios de "hosting"; es decir, de alojamiento o almacenamiento de dichos datos, obrantes en el archivo "data log" de la página web de CARRITOS DEL NOROESTE, albergados en aquélla prestadora de servicios, como así resulta, del probado y no cuestionado hecho, de que es esta última entidad la que padeció la brecha en su sistema de seguridad, por ataque malicioso de un hacker o pirata informático, y la que recibe el reporte automático, que la pone en alerta sobre la descarga no autorizada, desde los servidores de una ubicación desconocida.

A CARRITOS no se le puede hacer responsable de los sistemas de seguridad ajenos, cuya gestión no le correspondía, sin perjuicio de que hubiera podido incurrir en responsabilidad por culpa in eligendo, sobre la que posteriormente volveremos.

Se cita en la demanda igualmente el art. 112 del TRLGDCU. El mentado precepto norma que: *"Cuando el importe de una compra o de un servicio hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, el consumidor y usuario titular de ella podrá exigir la inmediata anulación del cargo. En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del empresario y del consumidor y usuario titular de la tarjeta se efectuarán a la mayor brevedad"*.

Tampoco consideramos aplicable tal precepto a la presente controversia judicializada, ya que, con las tarjetas de los actores, no se han efectuado cargos fraudulentos, ni fueron indebidamente utilizados para la adquisición de los productos comercializados por CARRITOS DEL NOROESTE S.L. -insistimos que ninguna queja se formula por mor de los contratos de compraventa a distancia celebrados entre los demandantes y la mentada mercantil-, sino que la utilización indebida de dichas tarjetas se llevó a efecto en empresas de informática de países del Este, únicas a las que, en su caso, les sería aplicable tal precepto, de

consentirlo su legislación interna. Y las que podrían llevar a efecto las anotaciones de adeudo y reabono.

El título de imputación susceptible de serle aplicado a la a CARRITOS derivaría de la falta de observancia de las medidas de seguridad, que imponían las circunstancias concurrentes en la comercialización de sus productos, mediante la utilización de su página web. Juicio de reproche que entendemos no procede en función de las consideraciones siguientes.

CARRITOS es una entidad que gira bajo la forma de una sociedad de responsabilidad limitada, cuyo objeto social consiste en la venta de carritos y sillas para bebés y niños de corta edad, con domicilio social en esta ciudad de A Coruña. Es cierto que cuenta con una página web, diseñada por la empresa WEBSSEDIGN S.L., que según la pericial judicial cuenta con las medidas de seguridad habituales en el mercado. Ningún reproche podemos hacerle, por lo tanto, al haber contratado con una empresa autónoma, especializada en dichos diseños, la elaboración de su web, así como la herramienta informática denominada secure payment, generadora del fichero "data log", en el que se archivan los datos personales de sus clientes, como tampoco por haber convenido el servicio de provisión de acceso a internet con TELEFÓNICA.

No fueron fallos en las medidas de seguridad de tales servicios las que produjeron la ilícita captación de los números y códigos CVN de las tarjetas de crédito de los actores, fraudulentamente utilizadas en su perjuicio. El problema de seguridad se produjo en el servidor donde estaba alojada la página, es decir en TOPSA.

No existe prueba alguna, en autos, que permitiese conocer a CARRITOS DEL NOROESTE que las entidades WEBSSEDIGN S.L. o TOPSA S.L. carecieran de la cualificación suficiente para asumir las obligaciones contractuales concertadas con ellas o que sus mecanismos de seguridad fueran deficitarios, tratándose de empresas consolidadas en el mercado, que actuaban con normalidad en el tráfico jurídico mercantil, contratando no sólo con CARRITOS DEL NOROESTE, sino con otras personas físicas y jurídicas, que demandaban sus servicios.

La existencia de culpa in vigilando exigiría que la demandada CARRITOS se hubiera reservado facultades de control, intervención o vigilancia en la actividad desplegada por la codemandada TOPSA, o como señalan las SSTS de 30 de diciembre de 1992, 17 de marzo de 2009, y 1 de junio de 2010, cuando existe "un nexo entre dos personas caracterizado por la existencia en una de ellas de facultades de impartir órdenes e instrucciones a la otra", lo que, desde luego, no acontece en el caso que nos ocupa, al hallarnos ante entidades independientes, que despliegan sus objetos sociales en distintos sectores de la actividad económica: comercialización de carritos de niños, y proveedora de servicios de alojamiento de datos en internet.

En definitiva, por lo general, no puede decirse que quien encarga cierta obra o servicio a una empresa autónoma en su organización y medios, y con asunción de los riesgos inherentes al contenido que desempeña, deba responder de los daños ocasionados por ésta, a menos que se hubiese reservado en ellos, facultades de vigilancia y dirección, que, como venimos razonando, no concurren, ni CARRITOS se encontraba cualificada para ejercerlas.

Por otra parte, tampoco la jurisprudencia ha llegado al extremo de erigir el riesgo como criterio de responsabilidad con fundamento en el artículo 1902 CC (SSTS 5 de abril de 2010 y 3 de diciembre de 2015), y ha declarado que la objetivación de la responsabilidad civil no se adecua a los principios que informan su regulación positiva. La responsabilidad de tipo subjetivo es el sistema común de responsabilidad, o lo que es lo mismo, la responsabilidad extracontractual responde al principio de la culpa del autor del daño, no convirtiéndose en objetiva por la facilitación de la prueba, ya que como afirman las SSTS de 27 enero 1987 y 7 de enero 2008, si ello fuera así, "se caería en una responsabilidad por el resultado, propia de épocas primitivas".

3.2 Responsabilidad civil de TOPSA.-

TOPSA es igualmente una entidad mercantil, que gira bajo la fórmula de una sociedad de capital, modalidad de responsabilidad limitada, con domicilio social, también, en esta ciudad A Coruña.

Se trata de una empresa de hosting, palabra que traducida al español significa "alojamiento", o dicho en los términos del art. 16 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, una prestadora de servicios de alojamiento o almacenamiento de datos. Son entidades que dentro de sus cometidos proveen espacios en Internet para los sitios web, como es el caso que nos ocupa.

No obstante, no consideramos que la presente cuestión controvertida deba dirimirse mediante la aplicación del art. 16.1 de la mentada Disposición General, conforme al cual "los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que: a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización"; toda vez que los datos almacenados por la codemandada, relativos al archivo "data log", no eran inmorales o ilícitos, no atentaban contra los derechos de propiedad intelectual o industrial, ni poseían un contenido difamatorio o delictivo de connotaciones sexuales o de otra naturaleza ilícita, sino que estaban constituidos por datos personales relativos a las tarjetas de crédito de los clientes de la codemandada, precisos para atender a su peticiones de compra, tratándose de datos protegidos pero perfectamente ajustados a la legalidad.

El indicado art. 16 atiende a la intención del legislador comunitario de introducir en el régimen de atribución de responsabilidad por daños reglas específicas dirigidas a ofrecer una cierta cobertura a los prestadores de servicios de intermediación, es decir, la garantía de que, cumplidos determinados requisitos, no podrán ser declarados responsables por los daños derivados de los contenidos ajenos; pero en este caso no es un problema de contenidos, ni del deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando, sino de acceso clandestino a los datos personales almacenados, que evidencian un fallo en los mecanismos de seguridad de la prestadora de servicios.

La responsabilidad del art. 16, según resulta de su numeral primero, es por la información almacenada, y, en este caso, insistimos, la indemnización postulada en demanda no proviene del contenido por ser ilícito, sino de la falta de adecuadas medidas de seguridad; siendo de aplicación el numeral primero del art. 13 de dicha Ley, cuando norma que "los prestadores de servicios de la sociedad de la

información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley”.

No ofrece duda que TOPSA asume, dentro de sus más elementales obligaciones contractuales, salvaguardar la integridad de la información que alberga, así como la seguridad de la misma. Es más la Ley le exige hacer constar las medidas de protección con las que cuenta en el art. 12 bis de la LSSICE.

Pues bien, en el caso presente, es indiscutible que se produjo un resultado indeseado, directamente ligado a su obligación de custodia de los datos que almacenaba, como prestadora de servicios de hosting, cual es la ilícita obtención de los mismos mediante ataque cibernético y su descarga a una ubicación desconocida.

Consideramos que ello es consecuencia de que las medidas de protección utilizadas no eran las adecuadas para cumplir con los servicios ofertados, garantizando la inaccesibilidad de la información a terceros ajenos a la misma, como así resulta del análisis crítico de la prueba practicada como exige el art. 218.2 de la LEC.

En efecto, CARRITOS DEL NOROESTE aporta una pericial, según la cual el servidor TOPSA presenta unas medidas de seguridad inusualmente bajas, que no incluyen el sistema Top Protect, usado habitualmente en el mercado, lo que ha causado la vulnerabilidad aprovechada por el hacker.

En el informe pericial aportado por TOPSA no se rebate tal afirmación, como sería lo procedente, de no compartirla o reputarla incierta o técnicamente inasumible, sino que desvía su responsabilidad a una tercera entidad WEBDESING S.L., que fue la que diseñó la página web de CARRITOS y la herramienta informática secure payment generadora del archivo data.log, en el que se almacenaban los datos personales de los clientes, achacándola la responsabilidad de los hechos por mor del mal diseño de la misma.

Sin embargo, en la pericial judicial, se concluye que las medidas de seguridad empleadas en el diseño de la mentada web son las habituales en el mercado.

No obstante, se indica, también, en este informe, que TOPSA carece del sistema top protect utilizado por las grandes empresas de comercio electrónico, aunque sí utiliza las habituales en el sector de las pequeñas y medianas empresas.

Ahora bien, dicha codemandada no es una simple empresa que comercializa sus productos mediante comercio electrónico, sino que opera en el tráfico mercantil como proveedora de almacenamiento de datos en internet, ofertando sus servicios a terceros mediante la correspondiente percepción de un canon, lo que exigía que adoptara más rigurosas medidas de seguridad, empleando el sistema top protect, conocido y utilizado por otros operadores, que hubiera evitado la brecha de seguridad sufrida, y que es habitualmente empleado en el sector.

De ninguna manera se ha acreditado -pues al respecto no existe en el procedimiento prueba alguna- que el coste de implementación de tal medida de protección resultase desproporcionada para la facturación de TOPSA y para los servicios que la misma efectivamente presta a quienes con ella contratan.

Siendo obvio que quien actúa en el mercado de prestadores de servicios de internet deberá garantizar, como esencial obligación, la integridad y seguridad de los datos almacenados, sin que se pueda subordinar tan esencial deber legal y contractual a la mayor rentabilidad de su negocio o subordinarla a sus exigencias presupuestarias. La seguridad es innegociable.

Por otra parte, TOPSA ostenta la condición de encargada en el tratamiento de datos personales. Como se considera en el Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», adoptado el 16 de febrero de 2010, por el órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad, creado en virtud del artículo 29 de la Directiva 95/46/CE, en el que se señala que la definición del encargado del tratamiento abarca una amplia variedad de agentes que pueden desempeñar ese papel («persona física o jurídica, autoridad pública, servicio o cualquier otro organismo»), y en concreto, con respecto a la posición jurídica de los proveedores de servicios de alojamiento de datos en internet, se sostiene que un ISP que presta servicios de alojamiento de datos es, en principio, un encargado del tratamiento de datos personales publicados en línea por sus clientes, que utilizan este ISP para el alojamiento y mantenimiento de su sitio web”.

El artículo 3.c) de La LOPD define el tratamiento como “operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de

comunicaciones, consultas, interconexiones y transferencias".

Por su parte, el artículo 5.1.t) del RLOPD lo define como "cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

La conservación de datos de carácter personal es, pues, un tratamiento de datos.

Por todo ello, aceptando tal consideración jurídica, sería igualmente responsable TOPSA, por la vía del art. 9.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que norma que: "el encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

Consideramos que el estado de la tecnología, la función de dicha codemandada como servidora hosting, y la inexistencia de prueba acreditativa de la imposibilidad de implementación del sistema de seguridad Top Protetc, conocido y habitual en el sector, que hubiera impedido la ilícita captación de datos, tratándose de además de una entidad profesional en el sector, y como tal perfectamente consciente de los riesgos de su actividad, conforma, con base en el conjunto argumental expuesto, la imputación objetiva del daño reclamado.

CUARTO: Sobre la cuantificación de los daños y perjuicios sufridos por los demandantes.-

En este apartado es punto controvertido, no el perjuicio patrimonial sufrido por los cargos efectuados en las cuentas bancarias de los actores, sino la indemnización postulada, en concepto de daño moral, cifrada en el 10% de las sumas reclamadas en demanda.

Es cierto que la jurisprudencia del Tribunal Supremo ha ampliado el ámbito de la apreciación del daño moral no sólo en el campo de la responsabilidad extracontractual, como el

caso que nos ocupa, sino incluso a la contractual, constituyendo buena muestra de ello las SSTS de 9 de Mayo de 1984, 27 de Junio de 1994, 22 de Noviembre de 1997, 14 de Mayo y 12 de Julio de 1999 y 3 de mayo de 2006, adoptándose una orientación cada vez más amplia, con clara superación de los criterios restrictivos que limitaban su aplicación a la concepción clásica del "pretium doloris" y los ataques a los derechos de la personalidad (STS de 19 de Octubre de 1998).

No obstante, también se ha sostenido que el daño moral no cabe alegarlo "cuando la lesión incide sobre bienes económicos, a modo de una derivación o ampliación del daño patrimonial" (SSTS 1031/2002, de 31 octubre y 443/2012, de 10 de julio).

La situación básica para que pueda darse lugar a un daño moral indemnizable consiste en un sufrimiento o padecimiento psíquico (SSTS de 22 de Mayo de 1995, 19 de Octubre de 1996 y 24 de Septiembre de 1999). De esta forma son indemnizables el impacto o sufrimiento psíquico o espiritual (SSTS de 23 de Julio de 1990), la sensación anímica de inquietud, pesadumbre, temor o presagio de incertidumbre (STS de 22 de Mayo de 1995), el trastorno de ansiedad, impacto emocional, incertidumbre consecuente (STS de 27 de Enero de 1998), impacto, quebranto o sufrimiento psíquico (STS de 2 de Junio de 1999)".

Ahora bien, en el caso presente, la utilización de la numeración de las tarjetas de los perjudicados no ha producido por sí sola, sin perjuicio del daño patrimonial experimentado, un especial impacto psíquico negativo bajo formas de crisis emocional, angustia, ansiedad o sufrimiento espiritual, dada la escasa entidad de las sumas apropiadas, que nos encontramos ante un daño estrictamente patrimonial que no incorpora un plus adicional perjudicial que, en las consideraciones concurrentes, exija resarcimiento compensador, amén de que el fraude fue inmediatamente descubierto y advertido a los actores, de manera tal que no sufrieron una especial situación de incertidumbre sobre la ulterior y posible utilización de sus tarjetas, pudiendo inmediatamente adoptar las medidas oportunas para preservar su patrimonio.

Desde luego, la situación no es identificable con los daños por ruina de un edificio destinado a habitación, en el que la jurisprudencias ha admitido igualmente la indemnización por daño moral al amparo del art. 1591 CC (SSTS de 15 de julio de 2011, en rec. 1122/2008 y 13 de abril de 2012, en recurso 934/2009).

Por todo ello, esta petición debe ser desestimada.

QUINTO: Sobre las costas procesales.-

La sustancial estimación de la demanda con respecto a la entidad TOPSA S.L. conlleva a que se le impongan las costas correspondientes a la acción contra ella dirigida. Sin embargo, la complejidad fáctica y de delimitación jurídica de las responsabilidades concurrentes en la otra entidad codemandada, unido a las dificultades de orientación previa de la reclamación efectuada, conduce a que no se haga especial pronunciamiento sobre la imposición de las costas procesales derivadas de la absolución de la entidad CARRITOS DEL NOROESTE S.L. (art. 394 LEC).

F A L L O

Con estimación parcial de la demanda deducida, debo condenar y condeno a la mercantil TOPSA S.L., a abonar a los actores las cantidades siguientes: a D. Juan 950,00 €; a D. Julián 825,00 €; a D^a M^a Carmen, 753,30 €; a D^a Patricia, 910,00 €; a D^a Julia 1.168,00 €; y, por último, a D. Pedro 1.750,00 €, con los intereses legales de dichas sumas desde la fecha de interposición de la demanda, y, a partir de la presente sentencia, los derivados del art. 576 LEC, con imposición de las costas correspondientes a dicho pronunciamiento.

Debo desestimar y desestimo la demanda con respecto a la entidad codemandada CARRITOS DEL NOROESTE S.L., absolviéndola de la misma, sin imposición de costas procesales.

Contra esta sentencia cabe recurso de apelación a interponer en el plazo de 20 días en este Juzgado, para su conocimiento por la Audiencia Provincial.

Así por esta mi sentencia, lo pronuncio, mando y firmo.