RIESGOS DE RESPONSABILIDAD CIVIL EN INTERNET .

AGERS 2.000

Gonzalo Iturmendi Morales.
Abogado.

Fuentes de riesgos de responsabilidad civil de Internet

Internet ha dejado de ser un simple sistema de transmisión para pasar a un sistema de negocios y de comunicación social.[1]

Juan Luis Cebrián afirmaba en una conferencia pronunciada en Bruselas a finales del año 1997 que "las nuevas tecnologías cambiarán la naturaleza del poder".. En la sociedad de la información la capacidad de control de los Gobiernos es muy inferior al de algunas grandes empresas como las de Bill Gates: el sistema Windows está implantado en el 80% de los ordenadores del mundo.

Una simple enumeración de posibles conflictos y manifestaciones de riesgos de responsabilidad civil en Internet [2] puede causar auténticos escalofríos, de ahí que se imponga su sistematización en conjuntos.

---

[1] Hay actualmente en el panorama editorial español varias obras que permiten al profesional interesado situarse en la nueva forma de entenderlos negocios y, en general, la visa en sociedad, que suponen las nuevas tecnologías de la información.

- López Garrido, D.: La sociedad informatizada y la crisis del Estado de bienestar. Revista de Estudios Políticos (REP), núm. 48, Nov.-Dic. 1985, 27
- Bustamante Donas, J.: ¿Sociedad informatizada, sociedad deshumanizada? Gaia, Madrid, 1998

[2] Por ejemplo, entre la muchas manifestaciones y problemas de responsabilidad civil en Internet encontramos:
1.- Responsabilidad civil profesional por errores y omisiones.
2.- Fraude informático.
3.- Abusos de E.MAIL. Por ejemplo: campañas de desprestigio, de marginación de productos o empresas, complots, etc...
4.- Virus informáticos. A) Accidentales. B) intencionados.
5.- Copyright.
6.- Pornografía.
7.- Fallos del sistema que provocan pérdidas.

Hay tres grandes grupos de problemas de seguridad. El primero tiene que ver con los actos malintencionados y la necesidad de proteger la información que fluye a través de la red. El segundo está relacionado con la intimidad de las personas y otros derechos fundamentales como la libertad de expresión, la privacidad, el honor, la propia imagen y el secreto de las comunicaciones. Y en tercer lugar todo lo relacionado con la seguridad de la contratación electrónica. Si bien es cierto que el primero y el tercero pueden resolverse –dado su carácter tecnológico- y con el tiempo dispondremos de medidas de prevención que minimicen estos riesgos, sin embargo, sin embargo el problema segundo es social al ser la red un sistema de comunicación social.

A nuevas tecnologías nuevos riesgos emergentes y de entre ellos destacan los que ahora nos ocupan, los relativos a las distintas manifestaciones de la responsabilidad civil en Internet , pues si bien es cierto que las nuevas tecnologías ayudan al desarrollo, no es menos cierto que su aparición en la sociedad genera un sinfín de riesgos de responsabilidad civil cuya primera máscara a simple vista puede atemorizar por la novedad y sofisticación técnica del medio virtual donde se manifiestan. Sin embargo un estudio detallado de estos nuevos riesgos emergentes de responsabilidad civil nos permitirá ubicarlos en el justo marco que les corresponde, mediante el necesario retorno a los fundamentos y principios básicos de la responsabilidad civil que nos posibilite abordar la selva mediática sin complejos y en el convencimiento de que estos fenómenos novedosos son perfectamente susceptibles de sistematización y estudio.

La globalización comunicacional conlleva cambios tecnológicos vertiginosos que encuentran su principal campo de operaciones en Internet . En todo caso, los beneficios van a ser superiores a los riesgos si afrontamos los desafíos con un cambio de mentalidad. .

8.- Intimidad. Acceso a datos de carácter personal. Acceso a correo sin autorización. Grabaciones sin consentimiento de ficheros, sonido, imagen, etc.
9. – Honor. Informaciones. Propaganda. Publicidad. Opiniones.
10.- Imagen. Utilización indebida. Derechos de propiedad intelectual. Derechos de imagen.
11.- Chateo.
12.- Acceso no autorizado a datos de terceros.
13.- Comercio electrónico e incumplimientos contractuales.
14.- Infidelidad de empleados.
15.- Delitos informáticos.
16.- Terrorismo cibernético.

Los especialistas coinciden en afirmar que Internet adquirirá la máxima relevancia en las aplicaciones de negocio y tendrá una influencia menor en el entretenimiento. El impacto será grande en el ámbito de las comunicaciones móviles, en el control de dispositivos y aparatos domésticos y en el de la automatización industrial.

La capitalización total del mercado de ordenadores es aproximadamente de seis billones de dólares, mientras que el de las empresas de Internet es ahora de un billón. Quizá Internet esté metido en una burbuja bursátil, pero los mismos que creen en ella esperan que el mercado de Internet se multiplique, por lo menos, por seis.

Si se pretende que Internet contribuya a reducir desigualdades no va a faltar trabajo. Un sondeo de PricewaterhouseCoopers entre un millar de ejecutivos concluye que la red está ampliando el abismo que separa los países ricos de los pobres. Aún hay 2.000 millones de seres humanos, un tercio de la población mundial, que nunca ha usado el teléfono.

Nos proponemos la tarea de diseñar un pequeño mapa que permita "navegar" por la vorágine de las distintas fuentes de responsabilidad civil de Internet . Para ello nos ayudaremos de los tres ejes disponibles al alcance de cualquier investigador que desee iniciarse o bien profundizar en la materia que nos ocupa: las normas vigentes, la doctrina científica y las todavía escasas resoluciones judiciales pronunciadas sobre estos conflictos.

I

La seguridad en Internet . Hechos malintencionados, delitos informáticos, fraude, hackers y virus informáticos.-[3]

Encontramos un primer núcleo de fuentes de responsabilidad civil en las derivadas de la comisión de delitos y faltas.

La responsabilidad puede derivarse de actos ilícitos tipificados en la ley penal, que lleven aparejada la obligación de resarcimiento al perjudicado como consecuencia de la comisión del delito o falta, tal es el caso de la responsabilidad civil por ilícito penal.[4]

Una cosa es la responsabilidad criminal, imputable a quienes realizan actos voluntarios subsumibles en las leyes penales, y otra bien distinta la obligación civil de reparar daños que, aunque tengan su origen remoto en los mismos hechos que la ley declara punibles, se rigen por disciplina diferente y están sometidos al conocimiento de la jurisdicción civil.

Es doctrina reiterada de la Sala Segunda del Tribunal Supremo que la jurisdicción penal es soberana para declarar la procedencia de la indemnización de daños y perjuicios, sin más límites que las siguientes:

a) Que consten los datos fácticos indispensables para poder determinar los perjuicios o daños, de modo que las bases, no su cuantía, es lo que queda sujeto a la revisión.

b) Que la antedicha libertad de cuantía queda tan solo limitada, por las cantidades que se fijen por las acusaciones públicas y privada cuando ejercitan la acción civil derivada de la penal.

---

[3] El pensamiento jurídico y económico se han venido ocupando desde hace ya varios años del gravísimo peligro que, para la economía y el orden político de una sociedad, suponen los delitos informáticos. A este respecto, pueden consultarse:

- Gutiérrez Francés M.L. Fraude Informático y Estafa, Ministerio de Justicia, Madrid, . 1991.
- Settembrino, F.:¡Ya ha llegado el nuevo *cookie*!, Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XV, nº 65, primer trimestre de 1999

[4] Responsabilidad criminal o delictual, que lleva aparejada la responsabilidad civil accesoria (Artículos 1902 del Código civil, 116 al 122, y 125 del Código penal).

Podemos distinguir en el nuevo Código Penal dos grandes grupos de delitos cometidos con la intervención de la Informática: por una parte, los delitos contra la intimidad [5], y por otra, los delitos contra el patrimonio y el orden socioeconómico[6].

---

[5] **-Delitos informáticos contra la intimidad.-**

Artículo 197.-

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunde, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta tipificada en el párrafo anterior.

4.Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 y 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198.-

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Lo dispuesto en los dos artículos anteriores será aplicable también al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes (art. 200 del Código Penal).

[6] **Delitos informáticos contra el patrimonio y el orden socioeconómico.-**

Robo con fuerza en las cosas.-

El Código Penal tipifica en el artículo 239 como robo con fuerza en las cosas el uso de tarjetas magnéticas o perforadas perdidas u obtenidas por un medio que constituya infracción penal. De acuerdo con la normativa comunitaria cabe afirmar la exoneración de responsabilidad del titular de tarjeta sustraída por los cargos realizados con posterioridad a la denuncia del hecho de la sustracción y la limitación de su responsabilidad a 150 euros por las disposiciones anteriores a la denuncia. En el supuesto, más que difícil, de que se encuentre al autor de la sustracción y se le condene por este delito, será éste el responsable de la reparación de los perjuicios económicos causados.

Estafa.-

El artículo 248.2 del Código Penal dispone que:

> "También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero."

Con arreglo al estricto concepto de estafa establecido en el número 1 del mismo precepto, estas conductas quedarían impunes por ausencia del requisito del engaño, por cuanto no puede ser destinatario del mismo una máquina. El requisito del engaño es sustituido por el de manipulación informática o artificio suficiente. Se recoge por tanto, una expresión de gran amplitud que permite encuadrar todos los supuestos de manipulación informática que produzcan una transferencia patrimonial no consentida en perjuicio de tercero.

Daños.-

El artículo 264.2 del Código Penal establece:

> "La misma pena (prisión de uno a tres años y multa de doce a veinticuatro meses) se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos."

Propiedad intelectual.-

El Código Penal dentro del Título XIII, dedicado a los delitos contra el patrimonio y contra el orden socioeconómico, regula en el Capítulo XI los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores.

En los artículos 270 a 272 el Código Penal recoge la protección penal que nuestro ordenamiento jurídico da a la propiedad intelectual. El Texto Refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo, de 12 de Abril de 1.996, define el objeto de la propiedad intelectual en su artículo 10:

> "Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro."

Y a continuación dicho artículo enumera una serie de creaciones susceptibles de constituir propiedad intelectual citando entre ellas expresamente los programas de ordenador.

El artículo 270 del Código Penal por un lado ampara el derecho a la producción y creación literaria, artística, científica y técnica contra los plagios y la reproducción, distribución o comunicación inconsentida; y por otro lado, ampara el derecho de explotación exclusiva y el control de las creaciones, obras y programas informáticos de los autores o asimilados.

Artículo 270.-

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio especificamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

El artículo 271 del Código Penal recoge dos subtipos agravados que se refieren a cualquiera de las conductas castigadas en el artículo 270, cuando concurra alguna de las siguientes circunstancias:

a) Que el beneficio obtenido posea especial trascendencia económica.

b) Que el daño causado revista especial gravedad.

La responsabilidad civil derivada de los delitos relativos a la propiedad intelectual se regirá por las disposiciones de la Ley de Propiedad Intelectual. El Código Penal remite por tanto, a los artículos 133 a 135 del Texto Refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo, de 12 de Abril de 1.996.

El artículo 133 otorga acciones al perjudicado, tanto para exigir el cese de la actividad ilícita, como la indemnización por daños y perjuicios. El artículo 134 determina los distintos grados y formas del cese de la actividad ilícita. Y el artículo 135 dispone que la acción para reclamar prescribe a los cinco años desde que el legitimado puede ejercitarla.

Propiedad industrial.-

El Código Penal ampara el derecho exclusivo que la patente o el modelo de utilidad confieren a su concesionario. El artículo 273 sanciona las conductas de los que con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabriquen, importen, posean, utilicen, ofrezcan o introduzcan en el comercio objetos amparados por tales derechos. Asimismo sanciona a los que de igual manera, y para los citados fines, utilicen u ofrezcan la utilización de un procedimiento objeto de una patente, o posean, ofrezcan, introduzcan en el comercio, o utilicen el producto directamente obtenido por el procedimiento patentado. En el apartado 3° de este artículo se hace una referencia especial a los modelos o dibujos industriales o artísticos o topografías de productos semiconductores.

- Espionaje industrial.-

Son los artículos 278 a 280 del Código Penal, bajo el epígrafe de delitos relativos al mercado y a los consumidores los que tipifican el espionaje industrial.

Aparte de estos dos grupos de delitos en los que se hace una referencia expresa en el nuevo Código Penal al medio informático, no cabe duda de que también se pueden cometer otros delitos utilizando para ello la informática. No hay que olvidar que la informática es un instrumento o herramienta con que se pueden hacer muchas cosas tanto lícitas como ilícitas.

Según un estudio de la Comisión Federal de Comercio de Estados Unidos la mayoría de las conductas delictivas de fraude en el comercio electrónico ya se daban antes de Internet , de manera que la mayor parte de los fraudes son tan antiguos como la vida misma; la novedad es la vía que se utiliza que, a diferencia de los fraudes anteriores, no tiene fronteras y, por tanto, son más difíciles de perseguir.

Las autoridades norteamericanas han alertado sobre los diez fraudes más habituales en el comercio electrónico, recomendando consejos generales que van desde la lectura atenta de los contratos, mostrarse escéptico ante empresas que no suministren su dirección postal y teléfono y desconfiar de las oportunidades[7].

Artículo 278.-

1. El que para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos y otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

[7] La Comisión Federal de Comercio de Estados Unidos ha publicado la lista de las 10 estafas más frecuentes que se cometen en el comercio electrónico.
1. Subastas. No subastarás aquel objeto que no tengas, y el que tengas lo has de enviar y si no, devolver el dinero inmediatamente. Las autoridades han perseguido a la empresa Computers By Us de Pensilvania por olvidar estos *detalles*.
2. Letra pequeña. Empresas que dan acceso a Internet ofrecen horas gratis a cambio de suscribirse por un año. La empresa asegura en su formulario de contrato que todo aquel que quiera podrá darse de baja en cualquier momento, pero en letra pequeña añaden interminables cláusulas entre las que cuales figura el precio que hay que pagar en caso de darse de baja. La FTC aconseja leer la letra pequeña.
3. Tarjeta de crédito. Hay empresas que solicitan el número de la tarjeta de crédito para cualquier trámite, como para hacer una reserva o comprobar que se trata de un usuario adulto (en sitios eróticos), pero ya empiezan a cargar comisiones sin aviso y sin haber prestado el servicio.

Un estudio de Cybersource y Mindwave afirma que mientras las compras con tarjetas de crédito han aumentado el 5% en los Estados Unidos, el fraude cometido con tarjetas ha crecido el 50%.

Una de las primeras inquietudes que asaltan a cualquier neófito en esta materia es la aparente vulnerabilidad de los sistemas y procedimientos de seguridad empleados en Internet .

¿Estamos ante un gigante con los pies de barro?. Muchas de las noticias vertidas recientemente en los medios de comunicación resultan ciertamente alarmantes. Por ejemplo, los ataques de la "hackers" durante el año 2.000 han causado daños a las empresas norteamericanas por valor de 266 millones de dólares (49.742 millones de pesetas), lo que supone el doble del año 1.999, según un estudio del Instituto de Seguridad Informática del FBI. Además, el número de ataques crece, buena prueba de ello es que en la primera mitad del año 2.000 se contabilizaron un total de 8.836 incidentes de seguridad, casi tantos como los registrados en todo 1.999 [8].

¿Quién no recuerda alguna noticia sobre "hackers" entrando hasta los archivos y lugares más recónditos de la NASA, el Pentágono o la propia Microsoft?

El diario *Wall Street Journal* daba la primicia de que unos desconocidos, gracias a un virus troyano, habían entrado en el sistema informático de la compañía Microsoft en Redmond. Se calculaba que, hasta haberse detectado la intrusión, podían haber estado husmeando durante tres meses y llegado al código fuente de algunos productos claves de la firma.

---

4. Cambio de dial. Un truco que va a más: ofrecer gratuitamente material para adultos, pero el sitio cambia la conexión del módem de acceso del usuario a un número de teléfono de larga distancia. La FTC recomienda vigilar la factura telefónica.

5. Albergue de páginas. Se ofrece el albergue en la red de una página personal gratuitamente durante 30 días de prueba. Se cobra el servicio aunque el cliente se haya dado de baja tras el período de prueba.

6. Pirámide. En Estados Unidos hay variantes del sistema de mercadotecnia piramidal prohibidas.

7. Vacaciones gratis. El gancho oculta comisiones, extras milagrosos que se multiplican por todas partes, y unas condiciones de hoteles en donde lo más inimaginable es la foto que te enviaron por la *web* .

8. Ofertas de empleo . Promesas de ganar dinero a cambio de comprar un material con la excusa de la formación profesional. Este dinero nunca será recuperado. Incluso es muy difícil tener la oportunidad de hablar con alguien de esa fantasiosa empresa.

9. Inversiones. Al calor de los *daytraders*, de los inversores aficionados y de los millonarios veinteañeros, algunas empresas ofrecen grandes ganancias en la Bolsa que nunca se producen. Y, aunque se produzcan, nunca llegan a tu bolsillo.

10. Curas milagrosas. En otros tiempos ofrecían por correo cremas para agrandar el busto o el pene, ahora por *e-mail* mandan pruebas para saber si tienes el SIDA y pócimas milagrosas. El consumidor nunca analizará la pócima que le envían. " (EL CIBERPAIS 9-11-2000)

[8] Diario EL PAIS, 3 de octubre de 2.000

La aparición de un virus informático en cualquier ordenador, sea particular sea de una empresa, es un hecho tan usual como traumático, que siempre acarrea pérdidas.

Dos factores han influido en el auge de la aparición y expansión de los virus informáticos: la creación de la World Wide Web, y el ataque constante que sufre el sector empresarial e incluso algunas instituciones.

El problema de los virus informáticos transmitidos por Internet tiene una doble dimensión desde el punto de vista de la responsabilidad civil en función del origen del contagio.

Pensemos en primer lugar en el supuesto del contaminador de virus que los crea y transmite con ánimo malintencionado. Este es un caso bastante claro en el que concurren los requisitos de la responsabilidad civil y posiblemente, según los antecedentes, también de la responsabilidad penal. Sin embargo resulta bastante más complejo de valorar el supuesto de transmisión de virus de forma involuntaria o concurriendo fuerza mayor (hecho imprevisible, inevitable ajeno al presunto responsable y de tal fuerza que suponga un obstáculo invencible para quien transmita un virus informático, por ejemplo, por medio del correo electrónico). En esta segunda hipótesis estaríamos hablando de un usuario de correo electrónico que transmite, sin saberlo, un virus previamente contraído por dicho correo, cuya detección resulta a todas luces imposible en el momento en el que se recibe y transmite a terceros por ser un virus aún no catalogado o por otra causa que impida su identificación con arreglo a la técnica normal requerida para el ejercicio de la actividad desarrollada. Posiblemente en este segundo supuesto no concurran los elementos de la responsabilidad, siempre y cuando el contagiado que transmita el virus no tenga la posibilidad material de haberlo detectado y evitar así el contagio posterior a otros terceros.

Uno de los estudios más relevantes realizado acerca de la problemática de los virus, es el realizado por la compañía norteamericana ICSA, encargada de cuantificar anualmente los daños producidos por los virus informáticos, sirva a modo de ejemplo de 300 compañías seleccionadas, el 99,67% han sufrido ataques de virus y que frente a 10 infecciones al mes por cada 1000 ordenadores en 1996, se ha pasado a 90 infecciones en el año 2.000.

El problema es de un calado extraordinario y puede comprometer seriamente la viabilidad de empresas, profesionales y Administraciones

Públicas, sobre todo si tenemos en cuenta el mal endémico de las pequeñas y medianas empresas en España a la hora de dedicar escasos recurso a la prevención de riesgos. Surge, como ya se ha apuntado, por la aparición de Internet , y la cantidad de posibilidades que la red ofrece, ya que si con anterioridad a la misma los virus que se creaban se expandían a través de ficheros, es decir, mediante el intercambio de software, posteriormente ese software se encontraba en la red y el intercambio se hizo innecesario.

Virus como *I love you* o *Melissa* traen en jaque a muchas empresas. El problema quizá reside en la importante inversión que debe realizar un empresario si quiere estar parcialmente a salvo de los virus, ya que no sólo debe proteger sus ordenadores con antivirus y con sus actualizaciones, sino también debe proporcionar a sus empleados la necesaria información (si es que no la tienen), acerca de las modalidades de agentes infecciosos y cómo enfrentarse a ellos, porque está comprobado que los mayores daños que causa uno de estos pequeños pero peligrosísimos virus son consecuencia de una errónea actuación de los afectados.

Por ello es imprescindible invertir en formación, conclusión a la que llegan muchas empresas, lamentablemente, sólo después de ser infectadas y sufrir pérdidas cuantiosas.

Igualmente surge la pregunta de la posible solución a la creación de virus cada vez más sofisticados y cuyas consecuencias pueden ser fatales, sirva como ejemplo la paralización de todo el sistema de Microsoft por el virus *I love you*. Esa respuesta es muy diversa según los Estados, y va desde una legislación penal enormemente dura, como es la norteamericana, al polo opuesto, como ocurrió en Taiwan con el creador del antedicho virus que no fue denunciado y consiguió un contrato con una conocida empresa fabricadora de antivirus.

No obstante, siempre queda la vía de la responsabilidad civil a la hora de reclamara los daños producidos por estos agentes, claro está, siempre y cuando sea identificable el agente causante del daño y concurran los requisitos de exigencia de responsabilidad.

II

La privacidad en Internet [9]

El artículo 18.4 de la Constitución Española instaura el imperativo legal de la *limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

---

[9] La consideración que la intimidad tiene en los ordenamientos jurídicos occidentales, que la han venido considerando un bien jurídico susceptible de protección constitucional, nos permite hacernos una idea de la importancia de las intromisiones propiciadas por las nuevas tecnologías. La importancia de esta cuestión en sectores claves de la economía como el asegurador ya se destacó en el CEGERS de 1998, cuyo tema fue precisamente Riesgos informáticos y panorámica actual de otros grandes riesgos Cf. Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XV, nº 62, segundo trimestre de 1998

Otras publicaciones de interés son:

- Agencia de protección de datos: El Consejo de Europa y la protección de datos personales, Madrid, 1997.
- Lucas Murillo de la cueva, P: Informática y protección de datos personales. Estudio sobre la L.O. 5/1992, de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal, Centro de Estudios Constitucionales, Madrid, 1993.
- Gay, C.: Intimidad y tratamiento de datos en las administraciones públicas, Editorial Complutense, Madrid, 1995.
- Agencia de protección de datos: Jornadas sobre el Derecho español de la protección de datos personales, Madrid, 28, 29 y 30 de Octubre de 1.996, , Madrid, 1997
- Ortí Vallejo, A.: Legislación de datos de carácter personal,. Tecnos, Madrid
- Delitos informáticos, número monográfico de la Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XIII, nº 51, tercer trimestre de 1995.
- Domaica Montoro, J.M.: El fraude informático, ¿un riesgo asegurable?, Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XII, nº 47, tercer trimestre de 1994
- Domaica Montoro, J.M., Riesgos de los delitos relacionados con las tecnologías de la información y las comunicaciones, Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XV, nº 60, cuarto trimestre de 1997
- Garriga Domínguez, A.: La protección de los datos personales en el derecho español, , Dykinson, Madrid, 1999.
- Estadella Yuste, O.: La protección de la intimidad frente a la transmisión internacional de datos personales, , Tecnos, Madrid, 1995.

Este principio se encuentra recogido en el Proyecto de CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA establece que toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente (Artículo 8. De la Ley Protección de datos de carácter personal) [10]

El derecho a la intimidad garantizado en el art. 18.1 CE, que se identifica con el derecho de toda persona a no ser objeto de injerencias arbitrarias en su vida privada y familiar, reconocido con términos casi idénticos en los arts. 12 Declaración Universal de Derechos Humanos de 10 Dic. 1948, 8.1 Convenio de Roma 4 Nov. 1950 (protección de los derechos humanos y de las libertades fundamentales) y 17.1 Pacto Internacional de Derechos Civiles y Políticos de 19 Dic. 1966, se concreta, por lo que al ordenamiento español se refiere, en el art. 18.2, 3 y 4 CE, en el que se encuentra el reconocimiento de la inviolabilidad del domicilio, la garantía del secreto de las comunicaciones y la previsión de una ley que limite el uso de la informática en defensa de, entre otros derechos, la intimidad personal de los ciudadanos.[11]

Se trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios. El art. 18.4 CE no sólo entraña

---

[10] La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (L.O.R.T.A.D.), de 29 de Octubre de 1.992, derogada por la **Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal**, vino a dar cumplimiento con cierto retraso al precepto contenido en el artículo 18.4 de la Constitución Española, de 6 de Diciembre de 1.978, según el cual:

> **"La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."**

El ámbito de aplicación de la Ley 15/1999 se refiere a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. En consecuencia, **se rigen por esta Ley Orgánica todo tratamiento de datos de carácter personal:**

> a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
> b) Cuando el responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho internacional público.
> c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito (art. 2)

[11] TS. TRIBUNAL SUPREMO (Sala 2) 05/11/1999 Granados Pérez

un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona --a la "privacidad"--, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos.

De tal manera que está prohibido tajantemente el uso de los datos para finalidades distintas de las que motivaron su recogida, así como su exactitud y puesta al día, siendo este un principio general de la protección de datos, la congruencia y racionalidad de su utilización, en cuya virtud ha de mediar una nítida conexión entre la información personal que se recaba y trata informáticamente y el legítimo objetivo para el que se solicita y, en consecuencia.

El art. 18.1 de la Constitución Española garantiza "el derecho al honor, a la intimidad personal y familiar y a la propia imagen" reuniendo así tres derechos diferentes en razón de que en muchas ocasiones hay un nexo o conexión entre ellos, y por ello la LO 1/1982 de 5 May. (protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen) unifica su protección civil. No obstante, dichos derechos continúan siendo diferentes, de manera que no estamos de un derecho tricéfalo, sino ante tres derechos diferenciados, como diferentes pueden ser los ataques a los mismos, ya que el derecho al honor se refiere a la estimación de la persona en y por la sociedad y contribuye a configurar el estado social de la misma; el derecho a la intimidad personal y familiar se refiere a una vida secreta y privada de la persona sustraída a indagaciones ajenas; y el derecho a la propia imagen se refiere en su esencia a poder impedir la reproducción de la figura humana en cualquier medio de expresión.

En la sociedad actual, con el desarrollo acelerado de la informática, las comunicaciones y las redes abiertas, la limitación y protección que impone el meritado artículo de nuestro texto constitucional, puede chocar con el creciente tratamiento automatizado de los datos de carácter personal, tratamiento que tiene también encuadre constitucional, concretamente en el artículo 20 (libertad de expresión e información). Conforme a la declaración programática del art. 18.1 CE, los derechos al honor, a la intimidad personal y familiar y a la propia imagen, de incuestionable rango constitucional, ofrecen suficiente entidad para que, a tenor del art. 20.4 CE, vengan a constituir un verdadero límite al ejercicio de la libertad de expresión, y de ahí que la LO 1/1982 de 5 May. (protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen), al fijar el ámbito en que han de desenvolverse los derechos regulados en el

art. 2, enumera una serie de supuestos de vulneración de tales derechos y en su art. 7.7 recoge como supuesto de intromisión ilegítima la divulgación de expresiones o hechos concernientes a una persona cuando implique difamación o desmerecimiento en la consideración ajena.

Los derechos al honor, a la intimidad personal y familiar y a la propia imagen son derechos subjetivos que no tienen, a diferencia de los restantes derechos fundamentales, el carácter de irrenunciables en cuanto que la autorización o el consentimiento de las violaciones de los mismos hecha por el ofendido supone una renuncia a la tutela legal (art. 1 LO 1/1982 de 5 May., protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen), pero si esto no ocurre, la intromisión ilegal producida da lugar a la correspondiente indemnización, ya que la LO 1/1982 citada establece, en su art. 9, una objetivización del daño derivado de la intromisión ilegal al presumirlo en todo caso.

Surge así el problema de la protección del ámbito personal de los ciudadanos, frente a los "ataques" que provienen de los medios telemáticos e informáticos. Y no se trata sólo de proteger datos, sino de proteger lo que en términos anglosajones se conoce como privacy (privacidad en castellano), concepto que engloba tanto el conjunto de datos de una persona, como el perfil que de ella se puede obtener a partir de los mismos.

El derecho al honor, protegido como derecho fundamental en nuestra Constitución, carece de definición legal. En la doctrina, se ha aceptado unánimemente la definición italiana que lo conceptúa como una dignidad personal reflejada en la consideración de las demás y en el sentimiento de la propia persona. La doctrina del alto Tribunal sobre el derecho al honor añade la nota de que dicho derecho debe estar afectado por una tarea de ponderación con relación a la **libertad de información**, teniendo en cuenta la posición prevalente, que no jerárquica o absoluta, de ésta. Así se debe proclamar, puesto que la libertad de información del art. 20.1.d) CE además de tener el carácter de una libertad individual, indica que una opinión pública libre está indisolublemente unida al pluralismo político dentro de un Estado democrático y al principio de legitimidad democrática que proclama el art. 1.2 CE y que es la base de toda la ordenación jurídico-política.

Es perfectamente posible hoy en día, obtener determinada información uniendo e hilando todos y cada uno de los pequeños datos que cada uno vamos dejando tanto en medios informáticos como de comunicación, información que se obtiene con las posibilidades que ofrecen los modernos medios tecnológicos y que ya no es la original, sino

una nueva, surgiendo entonces la pregunta de la titularidad, y por consiguiente, el poder sobre esa nueva información.

Ciertamente la opinión tiene más fuerza que la verdad y como dice la Exposición de Motivos de la Ley Orgánica 2/1997 de 16 de junio: *"La información no puede ser objeto de consideraciones mercantilistas, ni el profesional de la información puede ser concebido como una especie de mercenario abierto a todo tipo de informaciones y noticias que son difundidas al margen del mandato constitucional de veracidad y pluralismo"*. De ahí que dicha Ley responde a la necesidad de otorgar a los profesionales de la información un derecho básico en la medida en que ellos son el factor fundamental en la producción de informaciones. Su trabajo está presidido por un indudable componente intelectual, que ni los poderes públicos ni las empresas de comunicación pueden olvidar.

El derecho fundamental a la intimidad, que aparece consagrado en el art. 18.1 CE, impide las injerencias en la intimidad «arbitrarias o ilegales», y sólo la ley puede autorizar intromisiones por «imperativos de interés público». Todo derecho tiene sus límites, establecidos, en relación a los derechos fundamentales, en algunas ocasiones, por la propia CE, mientras que en otras ocasiones el límite deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionales protegidos

Ante estas realidades, es necesaria una protección eficaz, protección que tiene dos vertientes: defensa de los derechos que posee sobre la información su titular, y conocimiento de los ciudadanos, tanto de esos derechos, como de los niveles de confidencialidad que puede exigir en el tratamiento de sus datos.

La primera vertiente de la protección señalada, tiene reflejo en la legislación española e igualmente en el Derecho comparado. Esta vertiente no presenta excesivos problemas, pues prácticamente todas las legislaciones occidentales reconocen el derecho a decidir cuándo y cómo se va a utilizar la información que en unos casos se proporciona de manera voluntaria y otras por imperativo legal. Buen ejemplo de ello lo encontramos en nuestra Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, ley que se caracteriza por su carácter moderno e innovador.

Pero es la otra vertiente de la protección la que presenta los mayores problemas, y sin la cual la defensa de los derechos que amparan la

privacidad no resulta todo lo eficiente que debería ser: es precisamente el conocimiento del tratamiento de sus datos que puede llegar a exigir, lo que da virtualidad a la existencia de una defensa de los derechos que posee sobre ellos, podríamos decir que la información sobre el tratamiento de la información es lo que permitirá una respuesta eficaz y un cumplimiento escrupuloso de la obligación constitucional que recoge el artículo 18.

La Fiscalía General del Estado ha manifestado preocupación respecto de las distintas repercusiones penales por el tratamiento telemático y sus repercusiones en en relación con los derechos de artículo 18 de la Constitución.

Fruto de esta preocupación es la Circular 1/1.999 de la mencionada Fiscalía en la que: "La Fiscalía consultante somete a consideración un delicado problema interpretativo que además de cuestionar el alcance recíproco de dos derechos fundamentales íntimamente relacionados como son la libertad e inviolabilidad de las comunicaciones —art. 18.3 de la Constitución Española— y la libertad informática —art. 18.4 de la Constitución Española—, afecta también de modo directo a la definición de los límites que el Derecho positivo asigna a las facultades de investigación autónoma que el Ministerio Fiscal tiene atribuidas en el art. 5 del Estatuto Orgánico del Ministerio Fiscal."

Encabeza la consulta una interesante disquisición sobre las necesidades prioritarias que plantea la represión de una categoría nueva de delitos como son los relacionados con el uso de la informática.

El hecho particular que suscita la consulta se refiere a una empresa de sistemas informáticos que sufre un acceso indebido a sus ordenadores por parte de personas no identificadas que provocan el borrado de diversos ficheros.

La investigación e instrucción de la causa requiere en estos casos como primera diligencia la identificación de los abonados desde cuyos teléfonos o terminales se han realizado las conexiones telemáticas, lo que obliga a acudir al operador del servicio telefónico para recabar la información correspondiente.

En el caso que nos ocupa el Fiscal de propia autoridad y en el marco de una investigación preprocesal solicita del operador telefónico el conocimiento

de los números de abonado desde los que se verificaron las conexiones presuntamente criminosas.

La compañía operadora entiende que la información solicitada afecta al estatuto constitucional de inviolabilidad de las comunicaciones —art. 18.3 de la Constitución Española— y deniega el acceso a los datos en tanto no medie resolución judicial.

La consecuencia colateral de esta postura obstativa implica una restricción de las facultades de investigación del Fiscal en la medida en que el art. 5.2 del Estatuto Orgánico reduce la legitimación para la adopción de medidas de investigación a aquellas que no sean limitativas de derechos, por lo que la selección del régimen constitucional de garantía que le cuadra a este tipo de datos y contenidos, sea el estatuto de inviolabilidad del art. 18.3 de la Constitución Española, sea la libertad informática del art. 18.4 de la Constitución Española, repercute de inmediato en la afirmación de la existencia o inexistencia de posibilidades de investigación autónoma por parte del Ministerio Fiscal.

La Fiscalía de procedencia se pronuncia sobre la cuestión y estima que el estatuto de inviolabilidad sólo opera cuando el acto de comunicación es interceptado en tiempo real, esto es, mientras se produce la transferencia del mensaje, pues considera que el bien protegido es el libre flujo de las comunicaciones, de modo que, extinguida la comunicación, los datos que se registran en soporte informático para la facturación del servicio prestado quedarían sujetos al régimen especifico del art. 18.4 de la Constitución Española y de la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, que no exige habilitación judicial para la cesión de información en favor del Ministerio Fiscal —art. 11.2 d)—.
También estima que la legislación de telecomunicaciones distingue conceptualmente entre interceptación de contenidos y acceso a los datos de tráfico, entre los que se incluyen los datos de identidad de los comunicantes, y que de conformidad con el art. 51 de la Ley 11/1998 de 24 de abril, General de Telecomunicaciones, sólo la interceptación del contenido exige licencia judicial, lo que a sensu contrario conduce a estimar no abarcados en el secreto de las comunicaciones los aspectos e informaciones no comprendidos en el contenido mismo. Se cita asimismo el art. 3.2 de la Ley 24/1998 de 19 de julio, del Servicio Postal Universal, que en relación con los datos sobre la existencia del envío, clase, identidad del remitente y destinatario, y sus direcciones, remite a la aplicación de la Ley Orgánica 5/1992 de 29 de octubre.

Concluye finalmente la Circular de la Fiscalía que: "El Ministerio Fiscal no puede inmiscuirse en datos incorporados al contenido sustancial del derecho fundamental al secreto de las comunicaciones sin licencia judicial. Exigir del operador telefónico la identificación de los números de abonado conectados en una concreta y determinada comunicación supone una restricción de derechos prohibida por el art. 5.2 del Estatuto Orgánico del Ministerio Fiscal, por lo que es preciso acudir al Juez de instrucción, justificar la necesidad de la medida e instar la incoación de diligencias previas. Si el proceso está en curso, el Fiscal también debe solicitar del Juez de instrucción la adopción de la resolución judicial legitimadora de la injerencia. Ni las diligencias de investigación preprocesal amparadas en los arts. 5 del Estatuto Orgánico del Ministerio Fiscal y 785 bis de la Ley de Enjuiciamiento Criminal, ni las posibilidades de investigación autónoma paraprocesal que cabe deducir de los arts. 781.2 y 792.1.2 de la Ley de Enjuiciamiento Criminal constituyen marco legal idóneo para exigir del operador de la red o del prestador del servicio la revelación de los datos de tráfico registrados en las comunicaciones establecidas."

Aún queda mucho camino por recorrer, pues es escasa, por no decir inexistente, la información que sobre la manipulación de los datos que vamos dejando en los medios telemáticos e informáticos se nos proporciona en nuestros tiempos, así como de las consecuencias que puede tener tanto suministrar esos datos, como de las acciones que se pueden llevar a cabo en el probable caso de que nos encontremos con un tratamiento que atente contra nuestra privacidad. Quién no ha recibido alguna vez publicidad, tanto por medio del correo ordinario, como por el moderno correo electrónico, de empresas u otras entidades y se ha preguntado cómo y de dónde han sacado nuestra dirección.[12]

Pues bien, si la educación sobre el tema de la protección de la privacidad es escasa y en ocasiones controvertida en los círculos jurídicos, donde sólo los interesados realmente en esta cuestión buscan información sobre ella y se preparan en profundidad, la educación para el resto de los ciudadanos es

[12] En previsión de los nuevos riesgos que el tratamiento automatizado de datos personales pueda originar para la plena efectividad de los derechos de los ciudadanos, se dispone en el art. 18.4 CE que «la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se trata, por tanto, de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos. De suerte que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta. TC. TRIBUNAL CONSTITUCIONAL (Sala 1) 08/11/1999 Cachón Villar

totalmente nula, y es en este campo desde el que debería empezarse a actuar si realmente se quiere llegar a una máxima protección del derecho a la intimidad, así como a la elección por parte de cada uno del grado de confidencialidad con el que sean tratados los inevitables rastros que sobre sí mismo va dejando en el mundo de las telecomunicaciones.

Secreto de las comunicaciones. Acceso no consentido al correo electrónico.-

El artículo 18.3 de la Constitución Española establece que: "*Se garantiza el derecho de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*".

Esta norma contiene el derecho fundamental del individuo frente al Estado, afirmando el derecho al secreto, plasmación singular de los principios declarados en el art. 10.1 CE --dignidad de la persona y afirmación del libre desarrollo de su personalidad como fundamento del orden público y de la paz social--, y que se encuentra íntimamente vinculado al derecho a la intimidad, pero sin confundirse plenamente, ya que toda comunicación es para la norma fundamental secreta y sólo algunas, como es obvio, serán íntimas y privadas.

En esta misma línea el Proyecto de CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA establece que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y del secreto de sus comunicaciones (Artículo 7. Respeto a la vida privada y familiar)

La polémica está servida respecto del problema de los correos electrónicos de empleados, dependientes y funcionarios de empresas y Administraciones Públicas.

En este orden de cosas convendría distinguir dos supuestos bien diferenciados: El uso de la cuenta de correo electrónico que presta la empresa y la conexión desde la empresa a una cuenta personal de correo que el trabajador tenga abierta en la red. Mientras en el primer caso existen opiniones divididas sobre si se puede inspeccionar o no el contenido del correo electrónico, en el segundo no, ya que nos encontramos ante un acto privado autorizado por el empresario por lo que el mismo deberá respetar su privacidad.

Recientemente los medios de comunicación se han hecho eco del proyecto británico de autorizar a los empresarios la inspección rutinaria del correo electrónico que sus trabajadores envían desde el lugar de trabajo sin otro requisito que la previa advertencia a los mismos.

En el debate hay tres posiciones claramente diferenciadas, en primer lugar la de quienes defienden el derecho del empleador a rastrear el correo de sus trabajadores, en segundo lugar la de quienes limitan el derecho de inspección del empleador a la existencia de sospecha y a una apertura con garantías para el empleado y finalmente aquellos que defienden la tesis de la imposibilidad de inspección sistemática e indiscriminada de los correos electrónicos de los dependientes por atentar tanto al artículo 18.3 de la Constitución Española como al artículo 197 del Código penal.

A la hora de valorar estas posibles alternativas conviene no olvidar que la intimidad personal puede llegar a ceder en ciertos casos y en cualquiera de sus diversas expresiones ante exigencias públicas, pues no es un derecho de carácter absoluto, pese a que la CE, al enunciarlo, no haya establecido de modo expreso la reserva de intervención judicial que figura en las normas declarativas de la inviolabilidad del domicilio o del secreto de las comunicaciones (art. 18 núms. 2 y 3 CE); tal afectación del ámbito de la intimidad es posible sólo por decisión judicial, que habrá de prever que su ejecución sea respetuosa de la dignidad de la persona y no constitutiva, atendidas las circunstancias del caso, de trato degradante alguno (arts. 10.1 y 15 CE).[13]

El principio de respeto a la intimidad personal y a las comunicaciones privadas, frente a injerencias de las autoridades públicas, puede ceder, excepcionalmente, con el fin de proteger otros valores sociales que hayan de sobreponerse a los derechos individuales. Así el art. 8 Convenio de Roma 4 Nov. 1950 (protección de los derechos humanos y de las libertades fundamentales) señala la posibilidad de excepción cuando la injerencia esté prevista legalmente y se plasme en medidas necesarias en una sociedad democrática para la protección de intereses generales o colectivos como son, entre otros, la seguridad pública, la defensa del orden y la protección de los derechos y libertades de los demás ciudadanos. Consecuentemente con ese principio, el art. 18.3 CE prevé la salvedad de que por resolución judicial proceda adoptar excepciones a la garantía del secreto de las comunicaciones postales, telegráficas y telefónicas. En relación con esa posibilidad, la LO 4/1988 de 25 May. (reforma de la LECrim. en materia de delitos relacionados con bandas armadas o elementos terroristas o

[13] TC. TRIBUNAL CONSTITUCIONAL (Sala 1) 15/02/1989 Rubio Llorente

rebeldes) introdujo la redacción del art. 579 núms. 2 y 3 LECrim., conforme al cual es posible la intervención de las comunicaciones telefónicas de los procesados o personas de las que hubiere indicios de responsabilidad criminal, siempre que por esa intervención se pudiera obtener el descubrimiento o comprobación de hechos o circunstancias importantes de la causa y con la exigencia de que la intervención se acuerde por resolución motivada. Si se tienen en cuenta tales precauciones, con las aclaraciones que la jurisprudencia ha señalado, no se producirá violación de derechos o libertades fundamentales que invalidaría la eficacia de las pruebas, directa o indirectamente derivadas de tal violación [14].

En otro medio de comunicación como son las comunicaciones telefónicas, ya existe una línea jurisprudencial que permite esclarecer cuando se puede o no intervenir una línea telefónica, Así, son requisitos de las intervenciones telefónicas tanto para evitar la infracción del derecho al secreto de las comunicaciones constitucionalmente garantizado, como las que han de reunirse para que puedan ser acogidas como prueba: a) que esté prevista legalmente y que constituya una necesidad para la protección de intereses colectivos o generales como son la seguridad nacional y pública, la defensa del orden y la protección de derechos y libertades de los ciudadanos; b) de conformidad con la exigencia que expresa el art. 18.3 CE, ha de ser acordada en todo caso judicialmente y con una finalidad exclusiva de descubrir la existencia de delito y quienes sean las personas responsables del mismo; c) deben acotarse con precisión los teléfonos sobre los que recaiga la intervención, que habrán de ser los de las personas que puedan aparecer indiciariamente implicadas o de los que se sirvan habitualmente; d) la medida ha de ser excepcional en el sentido de que habrá de recurrirse a ella cuando no haya otro medio de investigación menos lesivo de los derechos individuales, proporcionada a la gravedad de los hechos cuya averiguación se pretende, temporalmente limitada sin que pueda admitirse intervenciones indefinidas o de duración excesiva, siendo inadmisible las que se encaminen a una averiguación indiscriminada de delitos, acordada en un procedimiento de investigación criminal o determinadora de su inicio, basarse imprescindiblemente en verdaderos indicios que permitan, aun cuando no sean datos exhaustivos, afirmar se cuenta con noticia racional de la existencia de delito, no bastando meras sospechas o conjeturas, y acordarse por resolución motivada que se refiera a las circunstancias concretas del caso en que la supresión de la protección constitucional se acuerde [15].

---

[14] TS. TRIBUNAL SUPREMO (Sala 2) 22/01/1996 Martin Canivell

[15] TS 2.ª SS 8 y 26 May., 26 Jun. 1997 y 20 Jun. 1998.

Como expone la sentencia del Tribunal Constitucional 114/1984 de 29 de noviembre, en su fundamento jurídico séptimo, el derecho fundamental a la libertad y secreto de las comunicaciones puede conculcarse tanto por la interceptación en sentido estricto —que suponga aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación del proceso de comunicación— como por el simple conocimiento antijurídico de lo comunicado —apertura de la correspondencia ajena guardada por el destinatario, por ejemplo—, porque la Constitución protege no sólo el proceso de comunicación, sino también el mensaje, en el caso de que éste se materialice en algún objeto físico, y el objeto del secreto abarca no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como por ejemplo la identidad subjetiva de los interlocutores o corresponsales.

Lo que indica la doctrina constitucional y del Tribunal de Estrasburgo es que no se pueden disociar sin merma relevante de garantías realidades tan sustancialmente integradas como son el mensaje y su proceso de transmisión.

El artículo 197 del Código Penal, que castiga a quien vulnere las comunicaciones personales. Este artículo cita el correo electrónico, una herramienta que no pudo prever la Constitución Española por su antigüedad, ni el Estatuto de los Trabajadores cuando reguló el registro de los efectos personales de los trabajadores.

El art. 18.3 de la Constitución Española consagró explícitamente el secreto de las comunicaciones, e implícitamente la libertad de las mismas, de lo que se deduce que la inmunidad constitucional no sólo previene la interceptación o captación en tiempo real, sino cualquier forma de conocimiento antijurídico del contenido del mensaje o de las circunstancias significativas de la comunicación, aunque se produzca fuera del contexto temporal de la conexión.

Por todo ello en nuestra opinión creemos que la protección constitucional de la intimidad cubre este vacío, de manera que:

1º.- Cuando el empleado verifique la conexión desde la empresa a una cuenta personal de correo que el trabajador tenga abierta en la red, el empresario no podrá tener acceso a la misma

2º.- Cuando es la empresa quien presta el correo como herramienta de trabajo, "y a esos únicos fines", se presenta un supuesto distinto, pero,

dado que no hay nada regulado, "ni en este caso" estaría justificado vulnerar la intimidad.

Sin perjuicio de ello y dado que el empresario no puede inmiscuirse en el correo electrónico ni en datos incorporados al contenido sustancial del derecho fundamental al secreto de las comunicaciones sin la preceptiva licencia judicial, podrá instar la correspondiente autorización judicial tomando, si lo estima oportuno, las medidas cautelares que, ajustándose a la legalidad, eviten la destrucción de las pruebas que acrediten la posible utilización indebida del correo o la conducta delictiva o desleal del empleado.

III

El comercio electrónico.-[16]

El comercio electrónico se basa en gran medida en los llamados contratos electrónicos.

En este tipo de contratos las condiciones no siempre están mutuamente negociadas. De hecho en un porcentaje muy alto nos encontramos ante condiciones generales de contratación unilateralmente redactadas por una de las partes que propone a la otra parte, la adhesión sin más a dichas condiciones.

Por ejemplo, un sistema de contratación muy empleado en Internet se basa en contratos llamados click-wrap —textos que aparecen forzosamente

---

[16] La irrupción de las nuevas tecnologías de la información y, en general, el fenómeno globalizador, han configurado lo que se ha dado en llamar la *nueva economía*. En ella, la contratación electrónica juega, sin duda, un papel esencial. A este respecto, pueden señalarse algunas publicaciones de interés:

- Oliver Cuello, R.: El comercio electrónico: perspectiva tributaria Actualidad informática Aranzadi, nº 33, octubre de 1999
- Sardina Ventosa, F.: La contratación electrónica del seguro de vida, Dykinson. Madrid, 2000.
- Carrascosa López, V., Del pozo Arranz, M.A.; y Rodríguez de Castro, E.P.: La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos, Comares. Granada, 1997.
- Martínez Nadal, A.: Comercio electrónico, firma digital y autoridades de certificación, Dykinson. Madrid, 1998.
- Martínez Nadal, A: Medios de pago en el comercio electrónico, Actualidad informática Aranzadi, nº 37, octubre de 2000
- Paz, E.: Cómo exportar, importar y hacer negocios a través de Internet Editorial Gestión 2000.Madrid, 2000.
- Barriuso Ruiz C.: La contratación electrónica. Aspecto legal del comercio electrónico, de loscontratos informáticos y del negocio jurídico por medios electrónicos, Dykinson. Madrid, 1998.
- Mougayar, W.:Nuevos mercados digitales. Comercio en Internet , Fundación Universidad – Empresa, Madrid. 1998.
- Oliver Cuello, R.: Tributación del Comercio Electrónico, . Tirant lo Blanch. Valencia, 1999.
- Álvarez-Cienfuegos Súarez, J.M.: Banca electrónica. LA LEY, 1997-3.

en la pantalla del ordenador en algún momento de la transacción—. Dichos documentos aparecen en la pantalla del ordenador indicando las condiciones y cláusulas del contrato, de manera que quien propone su condicionado requiere que el consumidor acepte dichas condiciones antes de proceder a la siguiente pantalla.

Nos encontramos sin duda ante una fuente inagotable de conflictos.

La Ley de condiciones generales de contratación -Ley 13-4-1998, núm. 7/1998- tiene por objeto -según indica el preámbulo de su exposición de motivos- la transposición de la Directiva 93/13/CEE, del Consejo, de 5 de abril de 1993, sobre cláusulas abusivas en los contratos celebrados con consumidores, así como la regulación de las condiciones generales de la contratación, y se dicta en virtud de los títulos competenciales que la Constitución Española atribuye en exclusiva al Estado en el artículo 149.1.6.ª y 8.ª, por afectar a la legislación mercantil y civil.

Se ha optado por llevar a cabo la incorporación de la Directiva citada mediante una Ley de Condiciones Generales de la Contratación, que al mismo tiempo, a través de su disposición adicional primera, modifique el marco jurídico preexistente de protección al consumidor, constituido por la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

La protección de la igualdad de los contratantes es presupuesto necesario de la justicia de los contenidos contractuales y constituye uno de los imperativos de la política jurídica en el ámbito de la actividad económica. Por ello la Ley pretende proteger los legítimos intereses de los consumidores y usuarios, pero también de cualquiera que contrate con una persona que utilice condiciones generales en su actividad contractual.

Se pretende así distinguir lo que son cláusulas abusivas de lo que son condiciones generales de la contratación.

Una cláusula es condición general cuando está predispuesta e incorporada a una pluralidad de contratos exclusivamente por una de las partes, y no tiene por qué ser abusiva. Cláusula abusiva es la que en contra de las exigencias de la buena fe causa en detrimento del consumidor un desequilibrio importante e injustificado de las obligaciones contractuales y puede tener o no el carácter de condición general, ya que también puede darse en contratos particulares cuando no existe negociación individual de sus cláusulas, esto es, en contratos de adhesión particulares.

Las condiciones generales de la contratación se pueden dar tanto en las relaciones de profesionales entre sí como de éstos con los consumidores. En uno y otro caso, se exige que las condiciones generales formen parte del contrato, sean conocidas o -en ciertos casos de contratación no escrita- exista posibilidad real de ser conocidas, y que se redacten de forma transparente, con claridad, concreción y sencillez. Pero, además, se exige, cuando se contrata con un consumidor, que no sean abusivas.

El concepto de cláusula contractual abusiva tiene así su ámbito propio en la relación con los consumidores. Y puede darse tanto en condiciones generales como en cláusulas predispuestas para un contrato particular al que el consumidor se limita a adherirse. Es decir, siempre que no ha existido negociación individual.

La Ley define las condiciones generales de la contratación como aquellas cláusulas predispuestas cuya incorporación al contrato sea impuesta por una de las partes, con independencia de la autoría material de las mismas, de su apariencia externa, de su extensión y de cualesquiera otras circunstancias, habiendo sido redactadas con la finalidad de ser incorporadas a una pluralidad de contratos (art. 1.1).

El concepto de condición general de la contratación está basado en la predisposición e incorporación unilateral de las mismas al contrato. En su formulación se han tenido en cuenta orientaciones jurisprudenciales anteriores, las aportaciones doctrinales sobre la materia y los criterios utilizados por el Derecho comparado.

¿Hay motivos para la desconfianza? Probablemente los haya cuando las condiciones sean abusivas y desorbitantes, sin embargo no debe haberlos si los pactos sean respetuosos con la legalidad [17].

---

[17] «Disposición adicional primera. **Cláusulas abusivas.**

A los efectos previstos en el artículo 10 bis, tendrán el carácter de abusivas al menos las cláusulas o estipulaciones siguientes:

I. Vinculación del contrato a la voluntad del profesional.

1.ª Las cláusulas que reserven al profesional que contrata con el consumidor un plazo excesivamente largo o insuficientemente determinado para aceptar o rechazar una oferta contractual o satisfacer la prestación debida, así como las que prevean la prórroga automática de un contrato de duración determinada si el consumidor no se manifiesta en contra, fijando una fecha límite que no permita de manera efectiva al consumidor manifestar su voluntad de no prorrogarlo.

2.ª La reserva a favor del profesional de facultades de interpretación o modificación unilateral del contrato sin motivos válidos especificados en el mismo, así como la de resolver anticipadamente un contrato con plazo determinado si al consumidor no se le reconoce la misma facultad o la de resolver en un plazo desproporcionadamente breve o sin previa notificación con antelación razonable un contrato por tiempo indefinido, salvo por incumplimiento del contrato o por motivos graves que alteren las circunstancias que motivaron la celebración del mismo.

En los contratos referidos a servicios financieros lo establecido en el párrafo anterior se entenderá sin perjuicio de las cláusulas por las que el prestador de servicios se reserve la facultad de modificar sin previo aviso el tipo de interés adeudado por el consumidor o al consumidor, así como el importe de otros gastos relacionados con los servicios financieros, cuando aquéllos se encuentren adaptados a un índice, siempre que se trate de índices legales y se describa el modo de variación del tipo, o en otros casos de razón válida, a condición de que el profesional esté obligado a informar de ello en el más breve plazo a los otros contratantes y éstos puedan resolver inmediatamente el contrato. Igualmente podrán modificarse unilateralmente las condiciones de un contrato de duración indeterminada, siempre que el prestador de servicios financieros esté obligado a informar al consumidor con antelación razonable y éste tenga la facultad de resolver el contrato, o, en su caso, rescindir unilateralmente, sin previo aviso en el supuesto de razón válida, a condición de que el profesional informe de ello inmediatamente a los demás contratantes.

3.ª La vinculación incondicionada del consumidor al contrato aun cuando el profesional no hubiera cumplido con sus obligaciones, o la imposición de una indemnización desproporcionadamente alta, al consumidor que no cumpla sus obligaciones.

4.ª La supeditación a una condición cuya realización dependa únicamente de la voluntad del profesional para el cumplimiento de las prestaciones, cuando al consumidor se le haya exigido un compromiso firme.

5.ª La consignación de fechas de entrega meramente indicativas condicionadas a la voluntad del profesional.

6.ª La exclusión o limitación de la obligación del profesional de respetar los acuerdos o compromisos adquiridos por sus mandatarios o representantes o supeditar sus compromisos al cumplimiento de determinadas formalidades.

7.ª La estipulación del precio en el momento de la entrega del bien o servicio, o la facultad del profesional para aumentar el precio final sobre el convenido, sin que en ambos casos existan razones objetivas o sin reconocer al consumidor el derecho a rescindir el contrato si el precio final resultare muy superior al inicialmente estipulado.

Lo establecido en el párrafo anterior se entenderá sin perjuicio de la adaptación de precios a un índice, siempre que sean legales y que en ellos se describa explícitamente el modo de variación del precio.

8.ª La concesión al profesional del derecho a determinar si el bien o servicio se ajusta a lo estipulado en el contrato.

II. Privación de derechos básicos del consumidor.

9.ª La exclusión o limitación de forma inadecuada de los derechos legales del consumidor por incumplimiento total o parcial o cumplimiento defectuoso del profesional.

En particular las cláusulas que modifiquen, en perjuicio del consumidor, las normas legales sobre vicios ocultos, salvo que se limiten a reemplazar la obligación de saneamiento por la de reparación o sustitución de la cosa objeto del contrato, siempre que no conlleve dicha reparación o sustitución gasto alguno para el consumidor y no excluyan o limiten los derechos de éste a la indemnización de los daños y perjuicios ocasionados por los vicios y al saneamiento conforme a las normas legales en el caso de que la reparación o sustitución no fueran posibles o resultasen insatisfactorias.

10. La exclusión o limitación de responsabilidad del profesional en el cumplimiento del contrato, por los daños o por la muerte o lesiones causados al consumidor debidos a una acción u omisión por parte de aquél, o la liberación de responsabilidad por cesión del contrato a tercero, sin consentimiento del deudor, si puede engendrar merma de las garantías de éste.

11. La privación o restricción al consumidor de las facultades de compensación de créditos, así como de la de retención o consignación.

12. La limitación o exclusión de forma inadecuada de la facultad del consumidor de resolver el contrato por incumplimiento del profesional.

13. La imposición de renuncias a la entrega de documento acreditativo de la operación.

14. La imposición de renuncias o limitación de los derechos del consumidor.

III. Falta de reciprocidad.

15. La imposición de obligaciones al consumidor para el cumplimiento de todos sus deberes y contraprestaciones, aun cuando el profesional no hubiere cumplido los suyos.

16. La retención de cantidades abonadas por el consumidor por renuncia, sin contemplar la indemnización por una cantidad equivalente si renuncia el profesional.

17. La autorización al profesional para rescindir el contrato discrecionalmente, si al consumidor no se le reconoce la misma facultad, o la posibilidad de que aquél se quede con las cantidades abonadas en concepto de prestaciones aún no efectuadas cuando sea él mismo quien rescinda el contrato.

IV. Sobre garantías.

Dado el continuo desarrollo de las telecomunicaciones, es muy difícil elaborar un inventario permanentemente actualizado de formas de contratación electrónica. Sin embargo, cualquiera que sea el medio empleado, el consumidor debe ser informado convenientemente de sus derechos y quien propone la transacción deberá respetar la legalidad respecto de las condiciones generales de contratación, evitando en todo momento que puedan resultar abusivas. Tanto la información adecuada,

---

18. La imposición de garantías desproporcionadas al riesgo asumido. Se presumirá que no existe desproporción en los contratos de financiación o de garantías pactadas por entidades financieras que se ajusten a su normativa específica.

19. La imposición de la carga de la prueba en perjuicio del consumidor en los casos en que debería corresponder a la otra parte contratante.

V. Otras.

20. Las declaraciones de recepción o conformidad sobre hechos ficticios, y las declaraciones de adhesión del consumidor a cláusulas de las cuales no ha tenido la oportunidad de tomar conocimiento real antes de la celebración del contrato.

21. La transmisión al consumidor de las consecuencias económicas de errores administrativos o de gestión que no le sean imputables.

22. La imposición al consumidor de los gastos de documentación y tramitación que por Ley imperativa corresponda al profesional. En particular, en la primera venta de viviendas, la estipulación de que el comprador ha de cargar con los gastos derivados de la preparación de la titulación que por su naturaleza correspondan al vendedor (obra nueva, propiedad horizontal, hipotecas para financiar su construcción o su división y cancelación).

23. La imposición al consumidor de bienes y servicios complementarios o accesorios no solicitados.

24. Los incrementos de precio por servicios accesorios, financiación, aplazamientos, recargos, indemnización o penalizaciones que no correspondan a prestaciones adicionales susceptibles de ser aceptados o rechazados en cada caso expresados con la debida claridad o separación.

25. La negativa expresa al cumplimiento de las obligaciones o prestaciones propias del productor o suministrador, con reenvío automático a procedimientos administrativos o judiciales de reclamación.

26. La sumisión a arbitrajes distintos del de consumo, salvo que se trate de órganos de arbitraje institucionales creados por normas legales para un sector o un supuesto específico.

27. La previsión de pactos de sumisión expresa a Juez o Tribunal distinto del que corresponda al domicilio del consumidor, al lugar del cumplimiento de la obligación o aquél en que se encuentre el bien si fuera inmueble, así como los de renuncia o transacción respecto al derecho del consumidor a la elección de fedatario competente según la Ley para autorizar el documento público en que inicial o ulteriormente haya de formalizarse el contrato.

28. La sumisión del contrato a un Derecho extranjero con respecto al lugar donde el consumidor emita su declaración negocial o donde el profesional desarrolle la actividad dirigida a la promoción de contratos de igual o similar naturaleza.

29. La imposición de condiciones de crédito que para los descubiertos en cuenta corriente superen los límites que se contienen en el artículo 19.4 de la Ley 7/1995, de 23 de marzo, de Crédito al Consumo.

Las cláusulas abusivas referidas a la modificación unilateral de los contratos y resolución anticipada de los de duración indefinida, y al incremento del precio de bienes y servicios, no se aplicarán a los contratos relativos a valores, con independencia de su forma de representación, instrumentos financieros y otros productos y servicios cuyo precio esté vinculado a una cotización, índice bursátil, o un tipo del mercado financiero que el profesional no controle, ni a los contratos de compraventa de divisas, cheques de viaje, o giros postales internacionales en divisas.

Se entenderá por profesional, a los efectos de esta disposición adicional, la persona física o jurídica que actúa dentro de su actividad profesional, ya sea pública o privada».

como el equilibrio en la reciprocidad de las prestaciones posibilitarán pasos decisivos para provocar la confianza entre las partes intervinientes en el comercio electrónico.

Firma electrónica.-[18]

La firma electrónica se configura como una alternativa que pretende llevar seguridad al tráfico de la contratación en Internet.

«Firma electrónica» es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.[19]

El Real Decreto-ley 17-9-1999, núm. 14/1999 (BOE 18-9-1999, núm. 224, pág. 33593) persigue –conforme declara su preámbulo- , respetando el

---

- Martínez Nadal, A.: Comercio electrónico, firma digital y autoridades de certificación, Dykinson. Madrid, 1998.
- Martínez Nadal, A.: Comentarios de urgencia al urgentemente aprobado Real Decreto-Ley 14/1999 de 17 de septiembre, sobre firma electrónica. LA LEY, 1999-6.
- Félix, Muñoz, J.: La firma electrónica en las declaraciones tributarias. LA LEY, 1999-3.
- Oliver Lalana, A.D.La equiparación de los efectos probatorios de los documentos electrónicos y escritos ante la futura regulación de la firma electrónica. LA LEY, 1999-3.
- Galindo, F.: Firma electrónica e instituciones de confianza: algunas precisiones. LA LEY, 1998-6.
- Galindo, F.: Los proveedores de servicios de certificación. LA LEY, 1998-3.
- Galindo, F.:: Los servicios de fiabilidad de las comunicaciones electrónicas. LA LEY, 1997-1.
- Álvarez Cienfuegos Suárez, J.M. : Las obligaciones concertadas por medios informáticos y la documentación electrónica de los actos jurídicos. LA LEY, 1992-4, 1012

[19] A su vez el Real Decreto-ley 17-9-1999, núm. 14/1999 (BOE 18-9-1999, núm. 224, pág. 33593) denine la «Firma electrónica avanzada» como la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

contenido de la posición común respecto de la Directiva sobre firma electrónica, establecer una regulación clara del uso de ésta, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación. De igual modo, este Real Decreto-ley determina el registro en el que habrán de inscribirse los prestadores de servicios de certificación y el régimen de inspección administrativa de su actividad, regula la expedición y la pérdida de eficacia de los certificados y tipifica las infracciones y las sanciones que se prevén para garantizar su cumplimiento.

El Real Decreto-ley determina el registro en el que habrán de inscribirse los prestadores de servicios de certificación y el régimen de inspección administrativa de su actividad, regula la expedición y la pérdida de eficacia de los certificados y tipifica las infracciones y las sanciones que se prevén para garantizar su cumplimiento.

El artículo 14 del Real Decreto de firma electrónica establece algunos principios en materia de **las responsabilidades por daños y perjuicios** de los prestadores de servicios de certificación, diciendo que los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone este Real Decreto Ley o **actúen con negligencia**.

La norma que comentamos desplaza la carga de la prueba sobre el prestador de servicios cuando establece que, en todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia. En consecuencia, al perjudicado corresponderá la carga de la prueba a la hora de acreditar el daño y la relación de causalidad entre la actividad del prestador del servicio y el daño, correspondiendo a este último acreditar que no incurrió en culpa si quiere exonerar su responsabilidad.

El prestador de servicios de certificación sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

El Real Decreto establece que la responsabilidad será exigible conforme a las normas generales sobre la culpa contractual y extracontractual, según proceda, con las especialidades previstas en su artículo 14.

Naturalmente cuando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros.

Lo dispuesto en artículo 14, se entiende sin perjuicio de lo establecido en la legislación sobre protección de los consumidores y usuarios.

El artículo 11 determina las condiciones exigibles a los prestadores de servicios de certificación estableciendo el elenco de obligaciones de los prestadores de servicios de certificación.

Entre ellas establece en su apartado g) la necesidad de disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en este Real Decreto-ley y, en particular, para afrontar el riesgo de la responsabilidad por daños y perjuicios. Para ello, habrán de garantizar su responsabilidad frente a los usuarios de sus servicios y terceros afectados por éstos. **La garantía a constituir podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un** [redacted] Inicialmente, la garantía cubrirá, al menos, el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada prestador de servicios de certificación. Teniendo en cuenta la evolución del mercado, el Gobierno, por Real Decreto, podrá reducir el citado porcentaje, hasta el 2 por 100.

Llamamos la atención sobre el hecho de que la garantía a constituir podrá verificarse mediante en un afianzamiento mercantil prestado por una entidad de crédito o en un [redacted] Es decir, no está estableciendo un único sistema de garantía sino que otorga la opción para realizarla por dos sistemas: entidad de crédito o entidad aseguradora.

En caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de los certificados que emita el prestador de servicios de certificación, la garantía a constituir, cubrirá, al menos, su responsabilidad por un importe de 1.000.000.000 de pesetas (6.010.121,04 euros). El Gobierno, por Real Decreto, podrá modificar el referido importe.