INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Guías Legales

PROTECCIÓN DEL DERECHO AL HONOR, A LA INTIMIDAD Y A LA PROPIA IMAGEN EN INTERNET

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN
Área Jurídica de la Seguridad y las TIC

Los beneficios de las nuevas tecnologías de la información en el día a día son indudables, sin embargo también es cierto que éstas pueden ser empleadas de forma malintencionada por algunos sujetos pudiendo llegar a afectar a derechos fundamentales de ciudadanos legítimos y, de manera especial, al derecho a la intimidad y a la privacidad de éstos.

En esta guía se realizará un análisis exhaustivo sobre cómo actuar ante la publicación de una información o documento en Internet cuyo contenido atente contra el derecho a la intimidad y a la protección de datos de carácter personal de un ciudadano conforme a lo dispuesto en la legislación vigente.

De igual manera se analizará la responsabilidad de los proveedores de contenido y de acceso en el caso de una violación de dichos derechos.

El concepto de Privacidad

Previo al análisis, conviene definir y conocer el concepto de privacidad. El derecho a la intimidad y a la privacidad se encuentra regulado en el art. 18 de la Constitución Española de 1978 y ha sido desarrollado por el propio Tribunal Constitucional, estableciendo que la privacidad "*preserva un ámbito propio y reservado frente a la acción y conocimiento de los demás, el cual es necesario para mantener una calidad de vida mínima*[1]".

Legislación aplicable

Como se puede apreciar a continuación, existe un gran numero de leyes que tienen relación con la privacidad tanto a nivel comunicatario como nacional.

Desde el ámbito comunitario:

- La Directiva 95/46/CE, relativa a la Protección de Datos de Carácter Personal, modificada por Directiva 97/66/CE, de 15 de diciembre, con medidas más acordes a las necesidades reales de Europa en el ámbito de las telecomunicaciones y la privacidad.

- La Directiva 2002/58/CE, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas, más conocida como "Directiva sobre la Privacidad y las Comunicaciones Electrónicas", cuyo principal objeto es armonizar la normativa nacional en lo relativo a la protección de las libertades y los derechos fundamentales, la

[1] Sentencia del Tribunal Constitucional - Sala Segunda nº 231/1988, de 02 de Diciembre 1988.

intimidad y los datos de carácter personal en el ámbito de las telecomunicaciones.

- La Directiva 2006/24/CE sobre Conservación de Datos de Tráfico en las Comunicaciones, de reciente transposición a la legislación nacional por la Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.

En el plano nacional:

- El art. 18 de la Constitución Española de 1978, especialmente en relación a la protección de la intimidad en el ámbito de las nuevas tecnologías. Así el art. 18.4 CE dispone 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"*, dando así una regulación expresa desde la norma fundamental del Estado a la protección de la intimidad y la privacidad en el sector de las nuevas tecnologías.

- La Ley Orgánica 1/1982, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

- La Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico, recientemente modificada por la Ley 56/2007 de Medidas de Impulso de la Sociedad de la Información, la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.

Privacidad en Internet

El citado concepto de privacidad y la regulación descrita ofrecen una visón preliminar para el análisis de este concepto en el entorno de Internet. Existe gran cantidad de productos y servicios en la Red: buscadores, publicidad personalizada y contextualizada en los servicios de correo electrónico online (Gmail, Yahoo Mail!, Hotmail…), redes sociales, etc; que pueden implicar riesgos para la privacidad e intimidad de las personas. Así, respecto de la privacidad, merecen especial atención dos situaciones específicas:

- De una parte, *la responsabilidad del buscador*, al indexar sitios web con perfiles y datos de carácter personal de los integrantes de la red social.

- De otra parte, *la responsabilidad de la propia red social*, a la hora de disponer de los perfiles de sus integrantes, así como de la realización de publicidad personalizada y contextualizada con la información y los datos que el propio usuario ha introducido en la Red.

Desde el punto de vista de los *buscadores*, se debe tener en cuenta su posición como simples mediadores, por lo que su responsabilidad queda delimitada por lo dispuesto en el art. 17 de la LSSI-CE.

En palabras de la propia Agencia Española de Protección de Datos *"… la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet se califica en la LSSI-CE como un servicio de intermediación. La Ley reconoce un interés legítimo en orden a la prestación del servicio, excluyendo inicialmente su responsabilidad…"*, *"…si bien les impone un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando, como puede suceder cuando se lesionen los derechos reconocidos por la normativa de protección de datos"*[2].

De todo ello cabe extraer que la LOPD sería de aplicación, a pesar de existir una exención, al menos inicial, de la responsabilidad de los buscadores en la labor de indexación de contenidos publicados en la Red. Esta exención se rompe en el caso de que de la indexación se derive una lesión de los derechos reconocidos por la

[2] Tomado de: http://www.inteco.es/Seguridad/Observatorio/area_juridica/Guias_Legales/guia_privacidad_internet

normativa vigente en materia de protección de datos.

Por otra parte, se encuentra la responsabilidad de la propia *red social* a la hora de disponer de los perfiles y otros datos de carácter personal facilitados por los propios usuarios y, tal como afirma la propia Agencia Española de Protección de Datos, *"… debe ser exigible, en primer lugar, a quienes la hacen accesible en la red*[3]". La actitud de la propia red social será jurídicamente reprochable dependiendo de las circunstancias, ya que la difusión de estos datos será lícita sólo cuando:

- Se derive del ejercicio de Derechos Fundamentales.
- Se lleve a cabo en cumplimiento de obligaciones legales.
- Se produzca con el consentimiento inequívoco del afectado, para lo que será necesario que la red social haya cumplido con la obligación, ya comentada en relación a los buscadores, respecto a la claridad y fácil comprensión de los avisos legales y políticas de privacidad.

Es por esto que resulta fundamental, de cara a proteger la privacidad de los integrantes de la red social, la lectura detallada de las *Condiciones Generales de Uso* de la misma, que deberán indicar de forma precisa el carácter personal que, en este caso, conforman el perfil de usuario y si éstos van a quedar disponibles en el propio sitio web, de tal forma que resulten indexados por cualquier buscador.

En líneas generales, para la lícita difusión de los datos de carácter personal contenidos en la red social, deberá recabarse el consentimiento inequívoco del afectado, así como que este consentimiento haya sido prestado conforme a los criterios suficientes de accesibilidad y claridad.

El consentimiento debe ser prestado siempre con anterioridad a la recogida de los datos, lo que es garantía de que el titular conoce la finalidad, sus derechos y los datos del Responsable del Fichero. La regla general establecida por la ley es la de solicitar a los titulares de los datos el *"consentimiento libre, específico, informado e inequívoco".*

Por tanto, nunca podrán solicitar el consentimiento para tratar los datos personales del usuario, sin que éste conozca con qué finalidad son tratados, cuál es la forma de ejercicio de sus derechos, quién es el Responsable del Fichero o que no se derive claramente de sus actos que deseaba prestar el consentimiento.

Otra de las características principales del consentimiento, que según lo dispuesto en el art. 6 de la LOPD debe cumplirse *"salvo disposición en contrario"*, es el hecho de que la aceptación por parte del afectado debe ser inequívoca, expresa o tácita, pero siempre una aceptación inequívoca.

[3] Declaración sobre Buscadores de Internet. Agencia Española de Protección de Datos. 1 de diciembre de 2007.

Intimidad en Internet

Como se ha señalado al comienzo de la guía, los beneficios de las TIC son indudables, sin embargo también es cierto que éstas pueden ser empleadas de forma malintencionada por algunos sujetos pudiendo llevarse a cabo actos que vulneren la intimidad de otros individuos.

En la Red, por su carácter universal, cabría la difusión a nivel global de cualquier información, documento, imagen o contenido audiovisual con la capacidad de difamar u ofender a un individuo o grupo de individuos, toda vez que se pueden ver incrementados dichos efectos por la velocidad e inmediatez de difusión que aquella ofrece. A esta situación se puede sumar la sensación de impunidad que aún interpretan algunos usuarios al considerar que nadie puede conocer qué acciones están realizando a través de sus equipos.

Si bien existen medios técnicos para anonimizar la navegación, los proveedores de acceso a Internet cuentan con la obligación de almacenar ciertos datos de acceso de los usuarios, de tal forma que en caso de necesidad, las autoridades competentes están cualificadas para tomar estos datos de forma que disponiendo de la información de hora de acceso y dirección IP[4] se pueda localizar al titular de la cuenta utilizada para una determinada conexión.

Para evitar ser objeto de este tipo de ataques, se recomienda llevar a cabo una labor de carácter preventivo. Las siguientes medidas[5] formarían parte de esa labor de cara a la protección de la intimidad en Internet:

- Leer detenidamente las Condiciones Generales, Avisos Legales y Políticas de Privacidad de aquellos sitios web que se utilizan.
- Registrarse únicamente en aquellos sitios web en los que se tenga confianza.
- Conocer que, en cualquier caso, se debe informar de forma previa, clara y de fácil comprensión sobre la finalidad para la que se recaban los datos de carácter personal, quién será el Responsable del Tratamiento y cuáles son los derechos de que se dispone.

[4] La dirección IP está formada por una serie numérica de cuatro grupos entre 0 y 255 separados por puntos y que identifica un ordenador conectado a Internet. Obviamente, este sistema no se utiliza para la navegación por las dificultades que supondría recordar esta serie de memoria. En su lugar, el DNS (Domain Name System o Sistema de Nombres de Dominio) traduce esos números a direcciones web, tal y como normalmente las utilizamos en los navegadores, que son fáciles de reconocer y recordar.

[5] http://www.inteco.es/Seguridad/Observatorio/area_juridica/Guias_Legales/guia_privacidad_internet

Ante un contenido difamatorio o que atente contra derechos en materia de protección de datos en Internet, ¿qué pautas de actuación se deben considerar?

En el caso de que sea localizado un contenido difamatorio o que atente o vulnere derechos en materia de protección de datos conviene tener en cuenta las siguientes premisas:

- En primer lugar, el propio usuario debe tomar conciencia de los actos que ejecuta a través de la Red, así como de la trascendencia y efectos que conlleva el remitir datos o informaciones, ya sean propios o de un tercero.

- En segundo lugar se debe tener en cuenta la responsabilidad no solo de los autores de un comentario o actividad que atenta contra la intimidad o la integridad personal, sino de los prestadores de servicios - webmaster de un foro, titulares de servicios audiovisuales, buscadorsw, etc- que son titulares del medio en el cual se publican, conforme a lo establecido en los arts. 13,14,15,16 y 17 de la Ley 34/2002 de los Servicios de la Sociedad de la Información y del Comercio Electrónico.

- Finalmente, si considera que sus datos de carácter personal se han podido filtrar o difundir sin su permiso, o que están siendo utilizados sin su autorización, realice la pertinente denuncia ante la Agencia Española de Protección de Datos - www.agpd.es .

De otro lado, las pautas de actuación más relevantes son las siguientes:

1. Búsqueda de todos aquellos foros, grupos, chats, blogs o páginas Web en Internet que contengan contenidos que atenten contra la persona. Para ello se llevará a cabo una exhaustiva búsqueda a través de Internet, mediante los principales buscadores, guardando capturas de pantalla de los mismos y haciendo una valoración jurídica de los hechos.

2. Consignación ante notario de todo el material localizado, con vistas a preconstituir prueba a aportar en un eventual procedimiento judicial. De esta manera se consigue otorgar a dichos hechos de fuerza probatoria plena.

3. Registro de los nombres de dominio pertinentes y realización de una página Web básica con la finalidad de mejorar y/o recuperar el posicionamiento de la persona que ha sufrido la difamación, incluyendo en ellos su currículo vítae, sirviéndole como medio de promoción personal o profesional.

4. Solicitud formal a los propietarios de las páginas Web que albergan dichos contenidos que retiren de inmediato los mismos, poniendo en su conocimiento que dicha información constituye un delito tipificado en el Código Penal (los comentarios de naturaleza injuriosa y calumniosa vertidos en Internet son

supuestos que recoge el Código Penal Español de 1995 en sus artículos 205 y 208).

5. Solicitud de bloqueo de la cache[6][7] a los buscadores más relevantes. Si es necesario, se ejercerán los derechos de acceso y cancelación de datos, y en caso de no obtener un resultado favorable se elevará la pertinente denuncia ante la Agencia Española de Protección de Datos.

En todo caso conviene conocer que las acciones cometidas a través de la Red son perseguibles de igual forma que sus correspondientes en el mundo real y que es importante denunciar cualquier hecho o suceso que atente contra nuestra integridad o intimidad, a través de cualquier medio.

Posibles acciones legales

Ante la publicación de contenidos difamatorios u otras acciones que atenten contra el derecho a la intimidad en Internet, existe la posibilidad de ejercer acciones de naturaleza penal o civil.

La acción penal supone obtener, en su caso, una condena de privación de libertad o de multa en los términos que establece la Ley, mientras que la vía civil implica una satisfacción de carácter económico a favor del ofendido.

Se recomienda ejercitar la vía penal, ya que pueden dilucidarse las cuestiones civiles, en compensación por los daños causados al ofendido, la denominada “responsabilidad civil”, que se suma a las pertinentes penas de multa o privación de libertad, que en el caso de las calumnias son de prisión de seis meses a dos años o multa de doce a veinticuatro meses, y de multa de seis a catorce meses en el caso de las injurias, teniendo en cuenta que en ambos casos media publicidad.

Además se puede solicitar la compensación económica a favor del ofendido en concepto de daños producidos, tanto por parte del presunto autor como del responsable, que en su caso, y respetando siempre lo explicado en el apartado referido a la responsabilidad establecida en el art.212 del Código Penal, podrá, en su caso, pedir la responsabilidad subsidiaria del medio de comunicación.

[6] Es el tipo de memoria que se encuentra en el procesador del ordenador y cuya función es almacenar información de uso muy frecuente y por lo tanto, necesita tener un acceso rápido y constante a la misma.
[7] Conjunto de datos duplicados de otros originales, con la propiedad de que los datos originales son costosos de acceder, normalmente en tiempo, respecto a la copia en el caché. Cuando se accede por primera vez a un dato, se hace una copia en el caché; los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso medio al dato sea menor.

La injuria y calumnia

El Código Penal Español define en su artículo 205 la **calumnia** como *"la imputación de un delito o falta con conocimiento de su falsedad o con temerario desprecio a la verdad"*. Por su parte, el art. 208 califica las **injurias** como aquellas *"acciones o expresiones que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación"*. En caso de que este tipo de acciones típicas sean consideradas como graves, serán consideradas como delito y no como falta.

*En el caso de la calumnia***,** el autor debe publicar los contenidos con conocimiento de que son falsos y de que suponen una agresión para la persona víctima de la calumnia. Esta expresión supone el requisito de que el autor tenga conocimiento doloso de que el hecho que se imputa es falso y en definitiva como una actitud en la que no se ha guardado la más mínima cautela o precaución respecto de los posibles derechos de terceros o de los posibles daños que pudieran producirse.

Tal y como establece el art. 211 del Código Penal, el delito se comete a través de medios de difusión y con publicidad, lo que incluye Internet, por lo que se considerará realizada con publicidad.

Las penas previstas para este tipo de delitos son de multa de 6 meses a 2 años o multa de 6 meses a 24 meses en caso de ser considerado grave, y en otro caso, con multa de 4 a 10 meses.

*Por lo que respecta a la injuria***,** la vía penal se cierra a todas las injurias que no revistan el carácter de graves, al menos en el concepto de delitos. La referencia que se contiene a la injuria en el número 2º del artículo 620, no ha de entenderse, necesariamente, como una penalización de las injurias leves a título de falta.

La injuria se va a considerar grave cuando el hecho o expresión implique un hecho o valoración que pueda ser considerado como grave, *"en el conjunto de la sociedad"*, es decir, no por la valoración del propio juez o ni siquiera por la del ámbito social en el que este se mueva, sino en el ámbito de los valores de la sociedad de la actualidad.

Las penas previstas para este tipo de delitos son de multa de 3 a 6 meses, y cuando los hechos ocurren con publicidad, como en el caso de que los contenidos calumniosos sean difundidos a través de Internet, con multa de 6 a 14 meses.

La publicidad: circunstáncia agravatoria

La publicidad en lo que respecta a la cuantificación de la pena en los delitos de injurias y calumnias es de vital importancia ya que conlleva un aumento considerable de las penas.

Cuando se habla de publicidad se hace referencia a toda aquella comunicación injuriosa o calumniosa que sea realizada a través de medios de comunicación de difusión masiva.

El artículo penal no cierra la posibilidad a las nuevas tecnologías y deja abierto el amplio abanico que conllevan los nuevos medios de comunicación, en especial Internet, que supone quizás el medio de comunicación más rápido y efectivo que existe, y por tanto los tipos penales de injuria y calumnia aplican perfectamente en el ámbito digital.

Responsabilidad

Del mismo modo se establece la responsabilidad solidaria del medio a través del que la calumnia o la injuria fue difundida, tal y como establece el art. 212 del Código Penal:

Art. 212. Código Penal. "En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria."

Mediante este artículo penal, una vez se comunica el presunto delito al propietario y al responsable del sitio web (webmaster) y éstos no proceden a la retirada de los contenidos, el Juez podría entender que está cometiéndose una colaboración a la hora de llevar a cabo el ilícito penal.

Necesidad de querella

Otro aspecto común a injurias y calumnias es la necesidad de interposición de querella por parte del ofendido según el artículo 215 del Código Penal.

La querella no es más que la declaración que una persona efectúa por escrito para poner en conocimiento del Juez unos hechos que cree que presentan las características de delito.

A través de la querella, el querellante solicita la apertura de una causa criminal en la que se investigará la comisión de un posible delito, y se constituirá como parte acusadora en el mismo.

Revelacion de secretos relativos a la vida intima

El vigente Código Penal establece en su artículo 197 el delito de descubrimiento y violación de revelación de secretos relativos a la vida íntima, que estipula:

Artículo 197 del Código Penal.

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 difunden, 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 descrita 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 al 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.

En el caso de que sea una 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 arriba descritas, 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.

Así mismo, como causa de agravación de la pena, el Código Penal establece que el que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

A su vez, el profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Dichas penas tambíen serán aplicables al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.

Para proceder por los delitos arriba previstos será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal, excepto cuando el inputado sea la autoridad o funcionario público, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

Lo anterior es importante toda vez que ya hay un precedente jurisprudencial en España al respecto: El juzgado de lo Penal número 11 de Barcelona ha condenado a dos años y dos meses de cárcel a un hombre por haber entregado a la cuñada de un compañero de trabajo las copias de varios correos electrónicos extraídos del ordenador de éste, algunos de ellos de contenido íntimo.

El titular del juzgado consideró que el procesado cometió un delito de revelación de secretos relativos a la vida íntima, aunque no consideró probado que fuera el propio procesado quien extrajera la información del ordenador de su compañero.

La sentencia, que es susceptible de ser recurrida ante la Audiencia de Barcelona, establece una multa de 3.240 euros y el pago de una indemnización de 4.000 euros para el perjudicado.

El juez da poca importancia al tipo de información desvelada en los correos, porque sostiene que la intimidad se vulneró en el momento en que se accedió al correo

electrónico del perjudicado, independientemente del contenido de los mismos.

Protección de datos

Por último, es necesario remitirse a la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), toda vez que el título VII de la misma establece las infracciones y sanciones que la Agencia Española de Protección de Datos (AEPD) puede interponer. Dichas sanciones puden variar desde infracciones leves hasta muy graves. Así:

Son infracciones leves:

a. No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b. No proporcionar la información que solicite la Agencia Española de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c. No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d. Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e. Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

Son infracciones graves:

a. Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o Diario oficial correspondiente.

b. Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c. Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d. Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e. El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f. Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g. La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h. Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i. No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquel a tales efectos.

j. La obstrucción al ejercicio de la función inspectora.

k. No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia Española de Protección de Datos.

l. Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

Son infracciones muy graves:

a. La recogida de datos en forma engañosa y fraudulenta.

b. La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c. Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d. No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia Española de Protección de Datos o por las personas titulares del derecho de acceso.

e. La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos.

f. Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g. La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h. No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i. No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Por lo tanto, en el caso de que una publicación tenga contenidos que violen la

intimidad de una persona, ésta esta facultada, adicionalmente a las acciones penales pertinentes, a presentar –anónimamente si lo desea- la respectiva denuncia ante la AEPD (la cual también puede investigar de oficio).

Para ejercer sus derechos en materia de protección de datos, basta con rellenar el modelo disponible en el sitio web de la AEPD (www.agpd.es), acompañado de una copia del DNI. El procedimiento de ejercicio de los derechos deberá ser gratuito y sencillo, entendiéndose como tal que el envío de un *fax* no incumple con el requisito de gratuidad.

No obstante, los sitios web suelen tener un procedimiento interno para el ejercicio de derechos. En estos casos, conviene seguir las indicaciones señaladas. El procedimiento resultará más rápido y sencillo.

En el caso de ejercer los derechos de acceso, oposición, cancelación y rectificación, es necesario que el Responsable del Fichero cumpla con los plazos establecidos. En caso contrario el usuario quedará habilitado para presentar una denuncia ante la Agencia Española de Protección de Datos mediante el formulario disponible en la página web www.agpd.es.

La retención de datos por parte de los operadores de telecomunicaciones y prestadores de servicios de la Sociedad de la Información tiene como única finalidad poder luchar de forma más efectiva contra los delitos graves, delincuencia organizada y terrorismo, por lo que en ningún momento éstos pueden justificar el almacenamiento excesivo o injustificado de datos de los usuarios y relativos a los mismos.

Los correos electrónicos de los usuarios en ningún caso pueden ser abiertos o rastreados, ni por una persona física, ni por un equipo informático. Únicamente se podrá “filtrar” cuando sea con finalidades relativas a la seguridad.

En el caso de que la imagen de un usuario aparezca en una plataforma de difusión de contenidos, éste deberá solicitar al propietario de la web que proceda a su retirada, por no existir autorización expresa para mostrarla, solicitando en su caso a los buscadores que lo hayan indexado que retiren dichos contenidos de sus búsquedas.

En caso de que no sean eliminados, deberá iniciarse un procedimiento ante la AEPD solicitándo la retirada inmediata de las imágenes.

Por último, se podrán iniciar las actuaciones judiciales pertinentes ante los Tribunales Civiles y, en su caso, denunciar ante la Agencia Española de Protección de Datos el incumplimiento de la normativa de protección de datos de carácter personal. En todo caso, es recomendable preconstituir prueba mediante depósito notarial de todos los contenidos mostrados a través de la web.

La obligación del propietario de la página web

La responsabilidad civil solidaria alcanzaría al propietario de la página web en la que se publicó la información y que en principio es el que debe controlar los comentarios que se realizan en sus foros o en su sitio web y mostrar la diligencia debida respecto a la retirada de los contenidos ilícitos. No obstante una vez ha sido retirada de forma automática cuando se le ha solicitado o bien vía correo electrónico, burofax o telefónicamente a los responsables del sitio web, su responsabilidad finaliza.

Para el establecimiento de la responsabilidad del art. 212 tendrá que tenerse en consideración, lo estipulado en la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico, que regula la responsabilidad de los prestadores de servicio de la sociedad de la información.

La Ley define, por su parte, como prestador de servicios de la sociedad de la información a "*toda persona física o jurídica que presta un servicio de la sociedad de la información, incluyéndose todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario*".

Este concepto se extiende a todo servicio que suponga para el prestador de servicios una actividad económica directa, o indirecta (ej: remuneración por publicidad inserta en la página), se puede encontrar dentro de estos:

- La contratación de bienes o servicios por vía electrónica.
- La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
- La gestión de compras en la Red por grupos de personas.
- El envío de comunicaciones comerciales.
- El suministro de información por vía telemática.
- El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la Red, tanto el programa deseado como el momento de su suministro y recepción.

El artículo 16 de la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico establece el régimen de responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos, como seria en el caso que nos ocupa, indicando que dichos prestadores de servicios *no* tendrán ningún tipo de responsabilidad cuando 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, o si tienen conocimiento efectivo, actúen con diligencia

para retirar los datos o hacer imposible el acceso a ellos.

La propia ley define el conocimiento efectivo cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

El apartado j del anexo de definiciones de la LSSI define competente:

"… *como todo órgano jurisdiccional o administrativo, ya sea de la Administración general del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas*…"

Enlaces de interés

www.agpd.es

http://www.policia.es/bit/index.htm

http://www.internautas.org/