Capítulo 8

Internet y la protección de datos de carácter personal

1. Introducción

La llamada **Sociedad de la Información** viene determinada por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo. Internet tiene un impacto bastante pronunciado en el trabajo, el ocio, el entretenimiento, el conocimiento y otras áreas a nivel mundial. Gracias a la superautopista de la información, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea.

Pero la implantación de Internet y las nuevas tecnologías tropiezan en grandes ocasiones con la protección de los datos de carácter personal, por lo que es necesario generar en el ciudadano una cultura para la protección de sus datos en la Sociedad de la Información, ya que de ella dependerá que cada persona pueda hacer un uso seguro de Internet para lograr no solo un mejor nivel de vida, sino también un verdadero control sobre su información.

Con el fin de contribuir e ir generando dicha cultura de la protección de datos en el ámbito de la Sociedad de la Información a través de Internet, la Agencia de Protección de Datos nos expone una serie de recomendaciones en las que se analizan los principales riesgos que, hoy en día, aparecen en la Red y se enume-

ran algunas instrucciones para tratar de prevenir sus efectos, en los medios más utilizados como son el correo electrónico y las redes sociales.

2. EL CORREO ELECTRÓNICO

El correo electrónico (e-mail) es el servicio de comunicación que ha alcanzado un mayor nivel de desarrollo en Internet, tanto a nivel de comunicación privada como en el ámbito de las relaciones profesionales y comerciales.

Hay que tener en cuenta que la dirección de correo electrónico es la forma más común de registrar la identidad de una persona en Internet y puede servir de base para la acumulación de información en torno a la misma. Esta dirección se utiliza en múltiples lugares de la red y puede ser conseguida fácilmente sin nuestro conocimiento, utilizando, por ejemplo, instrucciones incluidas en los programas para transmitir la dirección de correo electrónico del cliente sin que este sea consciente de ello, o configuraciones de seguridad en los navegadores que permiten a un sitio Web conocer las direcciones de correo electrónico.

En este sentido, la inclusión de datos en directorios de personas accesibles al público en Internet, sin las adecuadas medidas de seguridad, supone exponer a los usuarios a que sus datos puedan ser recopilados sin su conocimiento y utilizados para otros fines. Existen programas específicamente diseñados para dicho fin, práctica que se conoce como cosecha de direcciones de correo electrónico, que son posteriormente utilizadas para el envío masivo de comunicaciones no solicitadas. Idéntica consecuencia puede suponer la participación por parte de los usuarios en cadenas de mensajes, sin adoptar precauciones como eliminar las direcciones de destinatarios que han sido incluidas en las sucesivas retransmisiones del mensaje, que suelen ser recopiladas por programas específicos o por el usuario que ha originado la cadena.

Esta práctica, permite la difusión de mensajes de correo electrónico de contenido normalmente engañoso, con la finalidad no declarada de obtener direcciones de correo electrónico para su uso posterior o de servir a intereses específicos del autor. Además de las consecuencias aquí descritas, suelen tener un alto grado de incidencia en el nivel de servicio de los sistemas gestores de correo electrónico.

Esta práctica se ha generalizado todavía más en las redes sociales ya sea mediante la recopilación masiva de amigos o la promoción de falsas citas. La

mayor parte de las técnicas de recopilación y uso de direcciones de correo electrónico se han trasladado a las redes sociales en las que la condición de teórico amigo de quien las realiza ofrece confianza e incrementa el riesgo.

Hay que considerar que todos los servicios aquí tratados no facilitan, de forma generalizada, el establecimiento fiable de la identidad de emisor y receptor. Tampoco se utilizan habitualmente mecanismos que garanticen la confidencialidad en el intercambio de la información. Por estos motivos, deben considerarse los riesgos de suplantación de la personalidad o violación del secreto de las comunicaciones a la hora de remitir por correo electrónico información de relevancia.

Es frecuente que aparezcan, a menudo, avisos relativos a la aparición de un nuevo virus o gusano cuyo principal canal de distribución es el servicio de correo electrónico.

Uno de los formatos de inclusión de este tipo de piezas de software en los mensajes de correo son ficheros anexos modificados, cuya estructura esconde instrucciones para instalar nuevos programas o versiones modificadas de alguno preexistente, por lo que hay que procurar ser cuidadosos en su manejo, verificando siempre que su origen corresponde a una fuente de confianza y que disponemos de los adecuados medios de protección.

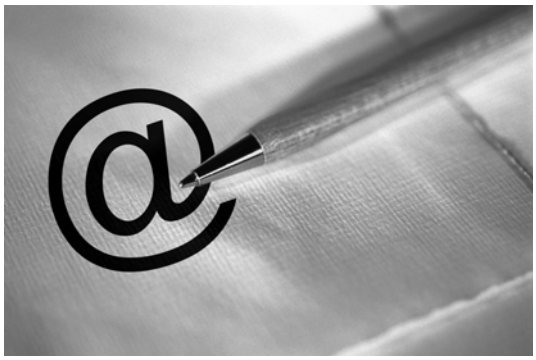
Por último, hay que hacer mención como riesgo asociado al correo electrónico el derivado de la difusión de mensajes de contenido engañoso o fraudulento, que son utilizados como vehículo de obtención de información sensible de los usuarios relacionados con otros servicios de Internet, como puedan ser la banca en línea.

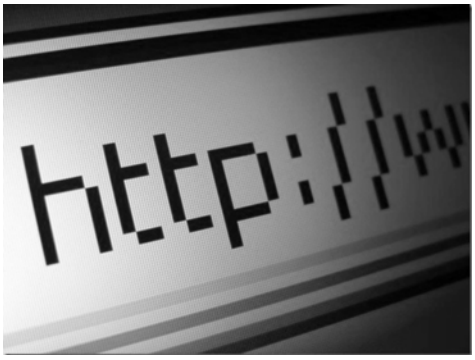
En todo caso, las recomendaciones relativas al uso del servicio de correo electrónico son las siguientes:

- Para acceder a su cuenta de correo electrónico, además de su código de usuario utilice una contraseña. La contraseña debe ser una combinación aleatoria de letras mayúsculas y minúsculas, números y símbolos. Debe cambiarla de forma periódica. La contraseña debería contar con un mínimo de ocho caracteres y cambiarse al menos en una ocasión al año.
- No utilice la opción de "Guardar contraseña" que, en ocasiones, se le ofrece para evitar reintroducirla en cada conexión.
- Si no quiere hacer pública su dirección de correo electrónico, configure su navegador para que no se la facilite a los servidores Web a los que accede.
- Conviene tener en cuenta, antes de proporcionarlos, que tanto nuestra dirección de correo electrónico como el resto de datos que proporcionamos para su inclusión en un directorio o lista de distribución, son susceptibles de ser utilizados sin nuestro conocimiento para fines diferentes de aquellos para los que fueron suministrados.
- Sea consciente de que cuando envía mensajes de correo a una variedad de destinatarios, está revelando las direcciones de correo electrónico de los mismos que figuran en los campos "Destinatario" o "Con Copia (CC)" a todos los receptores del mensaje. Para evitarlo, puede incluir los destinatarios del mensaje en el campo "Con Copia Oculta (CCO)" de tal forma que ninguno de los receptores podrá acceder a la dirección de correo electrónico del resto de los destinatarios.
- Configure su programa de correo en el nivel de seguridad máximo. Si es Vd. usuario de correo Web, decántese de ser posible por un proveedor de servicios que ofrezca análisis del contenido de los mensajes.
- Mantenga actualizado su programa cliente de correo electrónico, su navegador y su sistema operativo.
- No abra los mensajes que le ofrezcan dudas en cuanto a su origen o posible contenido sin asegurarse, al menos, que han sido analizados por su software antivirus.
- Active los filtros de correo no deseado de su programa de correo electrónico.
- Procure no utilizar para usos personales la dirección de correo electrónico que le haya sido proporcionada en el marco de su relación laboral.

Tenga en cuenta que, en algunos casos, los mensajes de correos de esas cuentas pueden ser monitorizados por la entidad responsable de las mismas. En todo caso, solicite ser informado de las limitaciones de uso establecidas así como de la posibilidad de que sea monitorizado el contenido del buzón de correo asociado.

- Evite reenviar cadenas de mensajes.
- Si ha de remitir mensajes a un conjunto de usuarios conocido, utilice, si su programa cliente de correo lo permite, las direcciones de grupo.
- Lea cuidadosamente las condiciones del servicio que su proveedor de correo electrónico ha de poner a su disposición, haciendo especial hincapié en todo lo referido a la obtención y uso de sus datos de carácter personal, así como los medios de los que dispone para garantizar la privacidad de sus mensajes.
- Si va a enviar por Internet documentos privados, es conveniente utilizar sistemas que permitan el cifrado de su contenido.





3. REDES SOCIALES

En este ámbito, destacan las redes sociales, por su complejidad e incidencia en el derecho fundamental a la protección de datos las redes sociales. Se trata de un fenómeno que ha supuesto una verdadera revolución en Internet. A través de las redes sociales es posible compartir información personal y contactar con otros usuarios de la Red. En la práctica el funcionamiento de estos servicios comporta que cada usuario ponga a disposición de otros muchos, con los que no tiene porqué tener una relación de confianza, multitud de información personal. Generalmente en las redes sociales se denomina **amigo** a alguien que simplemente nos ha hecho llegar una tarjeta de presentación o que conforme a las reglas del portal "es amigo de un amigo". El empleo de expresiones del tipo "amigo", "tu muro", o "tu álbum de fotografías", ofrecen una falsa imagen de privacidad por lo que si no se conoce el funcionamiento de la red social acaba siendo público y disponible para cualquier persona. De hecho, si se utilizan las configuraciones por defecto, lo habitual es que la información sea completamente disponible para cualquier tercero, incluidos los buscadores.

El gran volumen de datos personales que se vuelca en la red social hace necesario plantear las siguientes recomendaciones a los usuarios:

- Aprender las posibilidades de configuración y uso que la red ofrezca.

- Disponer de un perfil registrado en el que no se publique información excesiva de su vida personal y familiar, así como recurrir al uso de seudónimos o nicks personales permitiéndoles disponer de una identidad digital.
- Tener especial cuidado al publicar contenidos audiovisuales y gráficos en sus perfiles, especialmente si se van a alojar imágenes relativas a terceras personas.
- No etiquete contenidos audiovisuales con la identidad real de sus protagonistas ni ofrezca datos de terceros en su espacio sin su consentimiento.
- Revisar y leer las condiciones generales de uso y la política de privacidad de la red social en el momento de registrarse.
- Ejercer sus derechos de acceso a los datos que utilice el portal y el derecho de cancelación, o el de cancelar la suscripción cuando se verifiquen cambios en las condiciones legales y políticas de privacidad con los que no se esté de acuerdo.
- Configurar adecuadamente el grado de privacidad del perfil de usuario en la red social, optando por el que resulte más conveniente.
- Aceptar únicamente a aquellas personas conocidas o con las que se mantiene alguna relación previa y no publicar en el perfil información de contacto que permita ubicarnos físicamente.
- Emplear diferentes nombres de usuario y contraseñas para entrar en las distintas redes sociales.
- Utilizar contraseñas de ocho caracteres o más utilizando tanto letras como números, mayúsculas y minúsculas, así como tener un buen sistema antivirus debidamente actualizado.

4. LA PROBLEMÁTICA DE LAS COMUNICACIONES COMERCIALES A TRAVÉS DEL CORREO ELECTRÓNICO

Las comunicaciones comerciales a través del correo electrónico son una de las herramientas de Marketing en Internet que mayores ventajas y beneficios aporta a las empresas, pero existen dudas sobre la forma en que estas han de realizarse para cumplir con toda la normativa aplicable. Por esa razón vamos a hablar de los conocidos "Spam o correo basura".

¿QUÉ ES EL SPAM?

Se denomina **Spam** o **correo basura** a todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo, se entiende por *Spam* cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico. Quienes se dedican a esta actividad reciben el nombre de **spammers.**

El bajo coste de los envíos vía Internet (mediante el correo electrónico) o mediante telefonía móvil (SMS y MMS), su posible anonimato, la velocidad con que llega a los destinatarios y las posibilidades en el volumen de las transmisiones, han permitido que esta práctica se realice de forma abusiva e indiscriminada.

El envío de mensajes comerciales sin el consentimiento previo está prohibido por la legislación española, tanto por la Ley 34/2002 de Servicios de la Socie-

dad de la Información como por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos.

La Ley de Servicios de la Sociedad de la Información, en su artículo 21.1 prohíbe de forma expresa el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. Es decir, se desautorizan las comunicaciones dirigidas a la promoción directa o indirecta de los bienes y servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, si bien esta prohibición encuentra la excepción en el segundo párrafo del artículo, que autoriza el envío cuando exista una relación contractual previa y se refiera a productos similares. De este modo, el envío de comunicaciones comerciales no solicitadas puede constituir una infracción leve o grave de la LSSI.

Según esta ley las empresas a la hora de realizar comunicaciones electrónicas con personas físicas y/o jurídicas deberán:

- **Informar al usuario** previamente a la obtención de sus datos de:
  - Existencia de un fichero o tratamiento de datos.
  - Finalidad de la recogida de los datos.
  - Identificación del responsable del fichero.
  - Posibilidad de ejercitar sus derechos de acceso, modificación, cancelación y oposición.
- **Consentimiento del usuario.** En todo caso, las empresas que deseen realizar comunicaciones comerciales con los usuarios, deberán contar

con su consentimiento. A la vista de la diferencia de criterios, en cuanto al tipo de consentimiento requerido por la normativa aplicable, será recomendable contar con el consentimiento expreso del usuario, utilizando para ello medios como el correo electrónico de confirmación.

- **Revocabilidad del consentimiento.** Las empresas están obligadas, en todo supuesto, a facilitar un procedimiento sencillo y gratuito, a través del cual el usuario puede revocar su consentimiento para recibir comunicaciones comerciales, así como darse de baja de este servicio.
- **Identificación de la publicidad** y de las **ofertas promocionales.** En este caso habrá que atender a las previsiones realizadas por la LSSI, identificando el mensaje con la palabra publicidad al inicio del mismo, así como informando al usuario de manera clara y precisa sobre las condiciones de las ofertas promocionales.

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, establece una excepción al principio del consentimiento expreso del usuario "conocido como el principio de "opt in" recogido por la LSSI, motivo por el cual, la Ley española fue modificada por la Ley 32/2003 de 3 de Noviembre, General de Telecomunicaciones. Concretamente esta Directiva establece lo siguiente:

- Principio del consentimiento previo del usuario. Este principio se encuentra ya recogido por la legislación española en materia de comunicaciones comerciales, tanto en la LOPD, como en la LSSI.
- Excepción al principio del consentimiento previo conocido como "opt in". El art. 13.2 de la Directiva establece que cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o servicio, esa misma persona física o jurídica podrá utilizar los datos para la venta directa de sus propios productos y servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, de manera sencilla y gratuita, la posibilidad de oponerse a recibir dichas comunicaciones. Esta previsión ha sido recogida por el Art. 21.2 de la LSSI, tras modificación por Ley 32/2003, de 3 de Noviembre, General de Telecomunicaciones.

Además de suponer una infracción a la Ley de Servicios de la Sociedad de la Información, la práctica del Spam puede significar una vulneración del derecho a la intimidad y el incumplimiento de la legislación sobre protección de datos, ya

que hay que tener en cuenta que la dirección de correo electrónico puede ser considerada como dato de carácter personal.

A continuación les plantearemos una de las muchas preguntas que se hacen la mayoría de los empresarios respecto al envío de información comercial para darse a conocer como un ejemplo a lo expuesto anteriormente.

Ejemplo

¿Podría una nueva empresa que quiere darse a conocer en el mercado, enviar publicidad comercial a las direcciones de e-mail de otras empresas publicadas en las páginas amarillas?

Desde el punto de vista de la normativa vigente, se deben identificar como Spam todas aquellas comunicaciones electrónicas del tipo que fueren (correo electrónico de Internet, mensajes cortos de telefonía móvil "SMS", etc.) que el usuario recibe sin haber otorgado su consentimiento para ello, con las siguientes precisiones:

- Una comunicación electrónica no constituirá infracción en el caso de existir una relación contractual previa, y siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los emplee para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.
- Toda comunicación electrónica recibida sin consentimiento (y no existiendo una relación contractual previa), independientemente de su carácter comercial o no, es Spam. Sin embargo, la LSSICE solo regula comunicaciones electrónicas comerciales.
- No obstante, cuando los destinatarios de las comunicaciones no comerciales son personas físicas, podría aplicarse la LOPD (tratamiento sin consentimiento).
- Queda, por tanto, una situación de Spam no recogida por la legislación española (tampoco por la directiva), cuando los destinatarios sean personas jurídicas y la comunicación electrónica no sea comercial. Existen numerosos Spam que no tienen carácter comercial, como aquel cuyo contenido son chistes, bromas, cadenas de favores y virus informáticos, por ejemplo, si bien en los casos constitutivos de delito existe la jurisdicción ordinaria.

Se hace notar también que, en el caso en que los receptores de las comunicaciones comerciales sean personas jurídicas, la Agencia Española de Protección de Datos ostenta las competencias sancionadoras, ya que la LSSICE no hace distinción entre persona jurídica/física para los receptores de las comunicaciones electrónicas.

Se le informa que el envío de comunicaciones comerciales no deseadas por cualquier medio electrónico (e-mail. SMS, etc.) es considerado Spam por la Ley de la Sociedad de los Servicios de Información (LSSI) y podría ser objeto de sanción.

¿QUÉ MEDIDAS SE HAN DE TOMAR PARA EVITAR EL SPAM?

La dirección de correo electrónico es el medio más utilizado para registrar la identidad de una persona en Internet y suele servir de base para la acumulación de información en torno a la misma. En muchas ocasiones, contiene información acerca de la persona como el apellido, la empresa donde trabaja o el país de residencia. Esta dirección puede utilizarse en múltiples lugares de la red y puede ser conseguida fácilmente sin nuestro conocimiento, por lo que es necesario seguir una serie de normas para salvaguardar nuestra privacidad.

- **Ser cuidadoso al facilitar la dirección de correo.**

  Facilitar únicamente la dirección de correo a aquellas personas y organizaciones en las que confía y que quiera comunicar.

- **Utilizar dos o más direcciones de correo electrónico.**

  Utilice una dirección para aquellos casos en los que no se confíe o conozca lo suficiente al destinatario, y otra dirección personal que sea conocida únicamente por sus amigos o por sus contactos profesionales.

  Lo mismo se recomienda a la hora de utilizar servicios de mensajería instantánea.

- **Elegir una dirección de correo poco identificable.**

  Para crear una dirección de correo electrónico y reducir el envío de Spam, sería conveniente no introducir campos que sean potencialmente identificables por el spammer.

- **No publicar la dirección de correo.**

  No se debe anunciar la dirección de correo en buscadores, directorios de contactos, foros o páginas Web. Cuando envíe correos en los que aparezcan muchas direcciones, envíelas usando copia oculta. Si es necesario facilitar la dirección de correo en alguna Web, escriba "at" o "arroba" en lugar de @. Asimismo, si reenvía un correo, elimine las direcciones de los anteriores destinatarios.

- **Leer detenidamente las Políticas de Privacidad y las Condiciones de Cancelación.**

  Si se va a suscribir a un servicio *online* o a contratar un producto, revise la política de privacidad. No dude en ejercer los derechos de acceso y cancelación sobre sus datos ante estas empresas.

- **Sensibilizar a los niños sobre la utilización del correo y la mensajería instantánea.**

  Los niños son objetivos ideales para promocionar información sobre la composición y las prácticas de consumo del hogar. Además, los correos pueden tener contenidos no aptos para los niños.

¿QUÉ MEDIDAS DEBEMOS TOMAR SI YA RECIBIMOS SPAM?

Una vez que se empieza a recibir Spam, es casi imposible detenerlo completamente sin recurrir a un cambio de dirección de correo electrónico.

De todas formas, se recogen una serie de recomendaciones que pueden ser aplicados para reducir la proliferación del correo basura.

- **No es conveniente contestar al Spam.**

  Responder a dichos correos informa al remitente de que la dirección está activa, lo que puede animar tanto a ese como a otros spammers a enviar todavía más mensajes. La mayoría de los spammers provienen de fuera de nuestras fronteras, por lo que solo se debe responder a aquellos correos electrónicos de los que se conozca el remitente y se confíe en él.

  Es conveniente desactivar la opción que envía un acuse de recibo al remitente de los mensajes leídos del sistema de correo electrónico. Si un spammer recibe dicho acuse sabrá que la dirección está activa, y lo más probable es que le envíe más Spam.

- **No haga clic sobre los anuncios de los correos basura.**

  Si entramos en las páginas Web de los spammers podemos demostrar que nuestra cuenta de correo está activa, con lo que puede convertirse en un objetivo para nuevos envíos. Por otra parte, los gráficos e imágenes incluidos en los correos basura pueden proporcionar al spammer no solo la información de que el mensaje ha sido recibido, sino también datos de carácter personal como la dirección IP.

- **Utilice filtros de correo.**

- **Programas de filtrado de correo electrónico.**

  Los programas de gestión de correo electrónico, así como muchas páginas Web de correo, ofrecen la posibilidad de activar filtros que separan

el correo no deseado del Spam. Estos filtros reciben instrucciones para definir que tipo de correos se quieren recibir y cuales son considerados como Spam.

- **Filtros basados en ISP.**

  Muchos proveedores de Internet ofrecen soluciones que pueden llegar a ser muy efectivas a la hora de bloquear el Spam. Utilizan combinaciones de listas negras y escaneado de contenidos para limitar la cantidad de Spam que llega a las direcciones. El principal inconveniente es que, en ocasiones, bloquean correos legítimos, y además suelen ser servicios de pago. Para más información, consulte con su proveedor.

- **Mantenga al día su sistema.**

  Los ordenadores personales requieren de un mantenimiento. La mayoría de las compañías de software distribuyen actualizaciones y parches de sus productos que corrigen los problemas detectados en sus programas.

  Por otra parte, los usuarios deberían utilizar programas antivirus para protegerse contra estos perniciosos programas, capaces de destruir todos los archivos de un ordenador, y que cada vez son más utilizados por los spammers.

  Asimismo, es muy recomendable la instalación de un cortafuego para monitorizar lo que ocurre en el ordenador.

1. ¿Qué es el Spam?

2. Enumere las medidas que deben tomarse, si recibimos Spam.

3. ¿Qué es el "op it"?

4. ¿Qué normas españolas prohíben el envío de mensajes con fines comerciales?

Ejercicios de Repaso y Autoevaluación