

Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas



Edición: Febrero 2011

La "Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas" ha sido elaborada por el equipo del Observatorio de la Seguridad de la Información de INTECO:

Pablo Pérez San-José (dirección)

Cristina Gutiérrez Borge (coordinación)

Susana de la Fuente Rodríguez

Laura García Pérez

Eduardo Álvarez Alonso

El **Instituto Nacional de Tecnologías de la Comunicación (INTECO)**, sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional. Para ello, INTECO desarrollará actuaciones en las siguientes líneas: Seguridad Tecnológica, Accesibilidad, Calidad TIC y Formación.

El Observatorio de la Seguridad de la Información (<http://observatorio.inteco.es>) se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica, siendo un referente nacional e internacional al servicio de los ciudadanos, empresas, y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

La presente publicación pertenece al **Instituto Nacional de Tecnologías de la Comunicación (INTECO)** y está bajo una licencia Reconocimiento-No comercial 2.5 España de Creative Commons, y por ello esta permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento:** El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INTECO como a su sitio web: www.inteco.es. Dicho reconocimiento no podrá en ningún caso sugerir que INTECO presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial:** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INTECO como titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales de INTECO. <http://creativecommons.org/licenses/by-nc/2.5/es/>

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format). Se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección **Accesibilidad > Formación > Manuales y Guías** de la página <http://www.inteco.es>

Índice

1 WEB 2.0	4
1.1 Concepto.....	4
1.2 Tipología	5
1.3 La Web 2.0 en cifras.....	9
1.4 El papel de las tecnologías móviles en el futuro de la Web 2.0.....	12
2 WEB 2.0 EN EL DESARROLLO SOCIAL, PROFESIONAL Y EDUCATIVO.....	13
2.1 Ámbito Social	13
2.2 Ámbito Educativo.....	14
2.3 Ámbito Profesional	15
3 DERECHOS Y LIBERTADES A PROTEGER EN LA WEB 2.0.....	16
3.1 La libertad de expresión en la Web 2.0	16
3.2 La libertad de información en la Web 2.0.....	17
3.3 La intimidad, privacidad y propia imagen en la Web 2.0.....	17
3.4 La protección de datos en la Web 2.0	18
3.5 La propiedad intelectual en la Web 2.0	19
4 RIESGOS EN EL USO DE LA WEB 2.0.....	21
5 OBLIGACIONES Y RESPONSABILIDADES EN EL USO DE LA WEB 2.0	24
5.1 Responsabilidades de los diferentes actores	24
5.2 Preguntas frecuentes.....	27
6 RECOMENDACIONES PARA UN USO SEGURO Y RESPONSABLE DE LA WEB 2.0.....	29
6.1 Buenas prácticas de privacidad en la Web 2.0.....	29
6.2 Buenas prácticas de seguridad en la Web 2.0	31

A la vez que la Sociedad de la Información asiste a los nuevos logros en la Web 2.0, se producen nuevos desafíos en la seguridad y privacidad de los usuarios.

Así, la necesidad de una protección efectiva de los ciudadanos en el uso de dichas herramientas exige tanto un nuevo nivel de concienciación de los mismos respecto de los riesgos en el uso de dichos medios, como un mayor conocimiento de la normativa y un ejercicio efectivo de los derechos que se les reconocen.

Los internautas muestran preocupación por la seguridad y privacidad de sus datos en Internet, en especial en las redes sociales: cada vez son más los usuarios que limitan el acceso a su perfil únicamente a sus amigos o conocidos (el 66,2% en el tercer trimestre de 2010, frente al 60,6% en el mismo periodo de 2009)².

Para ello, la presente Guía ofrece una serie de pautas al lector que facilitan su aproximación a la Web 2.0, a los riesgos que pueden surgir y a las obligaciones de los diferentes participantes en este “juego” multidireccional, para asegurar el pleno disfrute de los usuarios en la experiencia de la colaboración digital.

1.2 TIPOLOGÍA

Las posibilidades de la Web 2.0 son casi ilimitadas, si bien el enfoque aportado en el presente documento se basa en el concepto de colaboración interactiva que es común a los distintos tipos de plataformas. Entre la diversidad de herramientas que surgen diariamente en la Web 2.0, las redes sociales, los blogs, las wikis o las herramientas de sindicación son las que mayor peso tienen entre los internautas³.

1.2.1 Redes sociales

Las redes sociales son espacios virtuales en los que cada usuario cuenta con un perfil público, que refleja datos personales, estado e información de uno mismo. A su vez dispone de herramientas que permiten interactuar y conocer al resto de usuarios, por ejemplo mediante la creación de grupos de interés.

El origen de las redes sociales se produce a mediados de los años 90, si bien en 2003 se produce el despegue de las mismas, con la creación de MySpace (portal cuyo enfoque principal estaba dirigido hacia grupos de música y fans) y Facebook (una red social creada en sus inicios para estudiantes universitarios y que hoy supera los 600 millones de usuarios⁴).

² Datos extraídos del *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles* (3^{er} trimestre 2010) http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_hogares_3T2010

³ Fuente: <http://www.focus.com/fyi/other/boom-social-sites/>

⁴ Información extraída de:

<http://www.facebooknoticias.com/2011/01/09/facebook-empieza-2011-con-600-millones-de-usuarios-registrados/>

Otras redes sociales destacadas hoy en día en España son Tuenti, Windows Live Messenger o LinkedIn y Xing en el ámbito profesional⁵.

Para conocer más acerca de la seguridad y privacidad en las redes sociales, pueden consultarse las publicaciones específicas del Observatorio de la Seguridad de la Información de INTECO⁶.

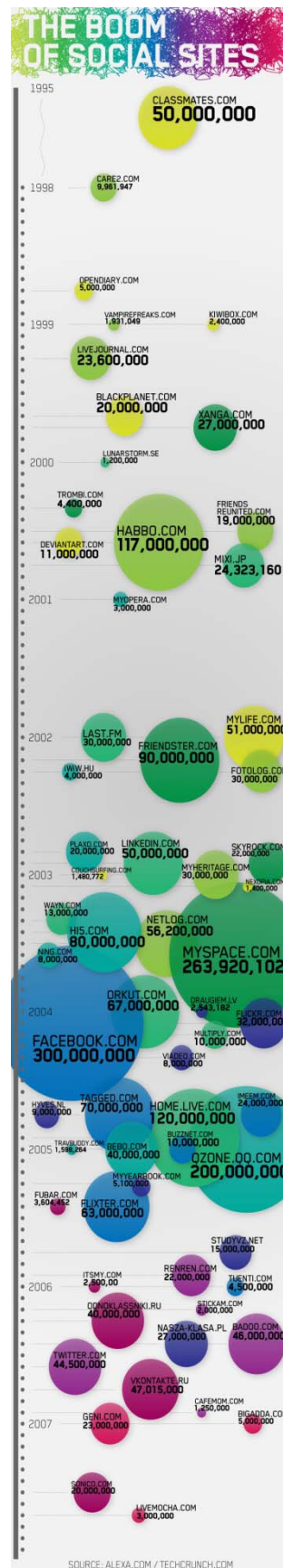
1.2.2 Blogs

Un blog es un sitio Web en el que el autor publica entradas o post, sobre temas de interés o como bitácora personal, y estos se almacenan cronológicamente. A su vez permite la inserción de comentarios (post) por parte de los lectores, convirtiéndose en una herramienta interactiva que constituye verdaderos foros de opinión.

El peso de la comunidad blog, la “blogosfera”, va aumentando en los aspectos social, cultural y político. La total independencia para escribir hace que los comentarios sean un indicador vivo de lo que realmente preocupa a la sociedad.

Los post generalmente contienen texto, pero gracias al podcasting (incorporación de archivos multimedia a los posts), también incluyen imágenes, sonido y vídeos. En la actualidad existen variantes del concepto original de blog, entre los que se encuentran el fotolog o el videolog.

La evolución de este modelo da paso al *microblogging*. El máximo exponente de dicho fenómeno es Twitter, creado en 2006 y que en 2010 ha superado a Myspace en número de visitas⁷. Responder a la pregunta “Qué sucede” utilizando menos de 140 caracteres se ha convertido en el nuevo fenómeno de la Web social. La incorporación reciente de nuevas funcionalidades permite la evolución del microblogging. Ejemplo de ello es Foursquare, que incorpora el geoposicionamiento y los juegos sociales.



⁵ Fuente: http://www.iabspain.biz/General/Informe_Redes_Sociales_IAB_nov_09.pdf

⁶ Disponible en: <http://www.inteco.es/Seguridad/Observatorio>

⁷ Disponible en: http://blogs.wsj.com/digits/2010/09/28/tweet-this-milestone-twitter-passes-myspace/?mod=rss_WSJBlog&mod=

1.2.3 Wikis

Una wiki es una página web que permite a sus participantes cambiar o editar sus contenidos, haciendo de la propia página una plataforma fácil y accesible para que los diversos usuarios puedan aportar contenidos bajo un mismo documento online. Así, el portal crece gracias al trabajo de una comunidad de individuos con un interés en común.

El primer wiki fue creado en 1995 por Ward Cunningham, una enciclopedia sobre programación que, con el tiempo, se convertiría en un portal sobre el *extreme programming*⁸.

El máximo exponente de este modelo de comunicación en la Red es la *Wikipedia*, un compendio del conocimiento humano en permanente proceso de construcción, con ediciones en 271 idiomas y en el que participan a diario cientos de miles de usuarios.

1.2.4 Foros

Dentro de las herramientas colaborativas se incluyen los foros. Suelen existir como complemento a un sitio web permitiendo a los usuarios discutir y compartir información relevante respecto de la temática del sitio, de modo libre e informal, generando una comunidad con un interés común. También existen foros individuales especializados en temáticas concretas o generalistas.

Los foros surgen como evolución de los sistemas de noticias BBS⁹ (*Bulletin Board System*) y Usenet¹⁰ siendo uno de los primeros sistemas que permiten la participación del usuario en la Red. Si bien siguen siendo utilizados por millones de personas, su uso ha ido disminuyendo a lo largo de los últimos años en beneficio de sistemas más avanzados como las redes sociales, integrándose como herramientas complementarias en las mismas.

1.2.5 Sindicación de contenidos

El formato RSS (*Really Simple Syndication*) es un formato que permite reunir de forma automatizada las noticias u otros contenidos de las webs y blogs por los que se tiene un especial interés (y que se denominan *feeds*) en un programa al que se llama agregador o lector de RSS y consultarlas de manera rápida.



⁸ *Extreme Programming* (XP) es una metodología de proyectos de software, basada en la simplicidad y agilidad.

⁹ Un *Bulletin Board System* o BBS (Sistema de Tablón de Anuncios) es un software para redes de ordenadores que permite a los usuarios conectarse al sistema (a través de Internet o a través de una línea telefónica) y utilizando un programa terminal (o telnet si es a través de Internet), realizar funciones tales como descargar software y datos, leer noticias e intercambiar mensajes con otros usuarios.

¹⁰ Usenet es el acrónimo de *Users Network* (Red de usuarios), consistente en un sistema global de discusión en Internet, que evoluciona de las redes UUCP (*UNIX-to-UNIX Copy Protocol*) mediante el cual los usuarios pueden leer o enviar mensajes (denominados artículos) a distintos grupos de noticias ordenados de forma jerárquica.

Estos programas muestran los contenidos de distintas maneras, indicando los titulares ya leídos, y despliegan un aviso cuando se han actualizado los sitios web que se tienen agregados.

1.2.6 Bookmarking

El bookmarking también permite organizar las webs favoritas etiquetando los portales o noticias mediante palabras clave relevantes, denominadas etiquetas (*tags*).

Los usuarios pueden ver cuántas personas han usado una etiqueta y buscar todos los recursos a los que se ha asignado. También pueden conocer quién creó cada referencia y acceder a otras referencias del creador.

De esta forma, la comunidad de usuarios crea con el tiempo una estructura única de palabras clave para definir recursos, algo que ha venido en llamarse 'folksonomía'.

Sitios como del.icio.us o Digg permiten compartir enlaces favoritos con amigos y seguidores, presentando aquellos artículos que les parecen interesantes a fin de que otros usuarios puedan emitir su voto respecto de lo que se ha compartido. Algunas redes sociales incluyen esta herramienta para dar funcionalidad a su servicio.

1.2.7 Herramientas

Además de las principales plataformas descritas, existen multitud de herramientas centradas en la generación de contenidos. Dos de los ejemplos más representativos son YouTube y Flickr, con los que los usuarios pueden subir, compartir y ver vídeos y fotos.

Además, los usuarios pueden encontrar comunidades especializadas en música (iTunes, Spotify, Last.fm), videos (Vimeo, Dailymotion), mundos virtuales (Secondlife), juegos (World of Warcraft), aplicaciones ofimáticas (Google docs, Office live) o transmisiones en vivo (Justin.tv).

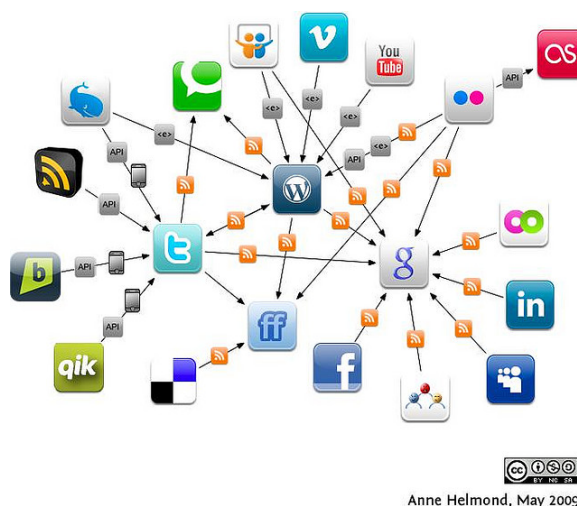


Ilustración 2: Una red interconectada

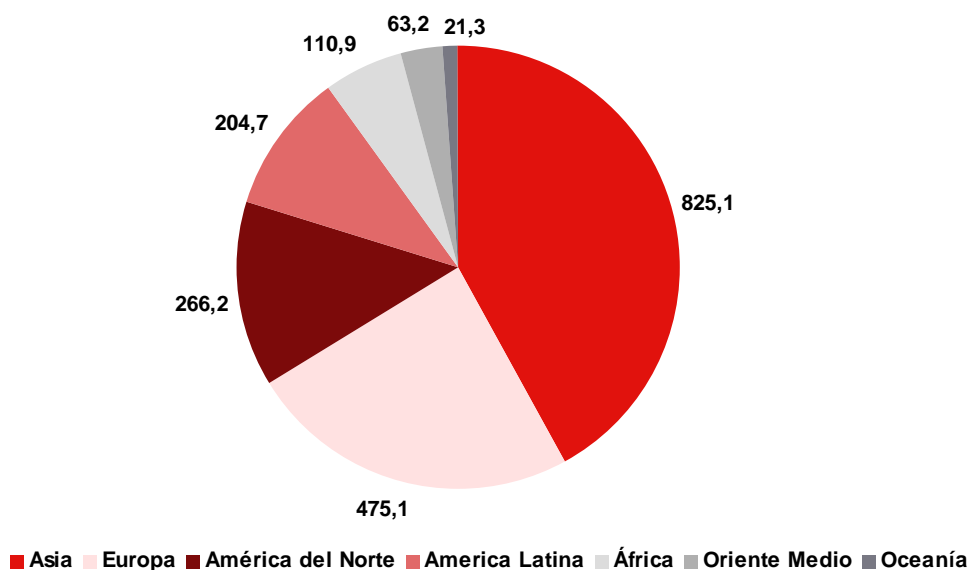
1.3 LA WEB 2.0 EN CIFRAS

La situación actual viene marcada por el vertiginoso y constante incremento de las cifras globales, propiciada por la popularidad de las plataformas y las funcionalidades que aportan las nuevas tecnologías. A continuación se dan las pinceladas para elaborar una imagen sobre la utilización de la Web 2.0 por los internautas a nivel mundial.¹¹

En Internet ...

- El número de usuarios de Internet supera los **2.000** millones en 2010¹².
- **225** millones de nuevos usuarios en el año 2010, de los cuales **162** millones pertenecen a países en vías de desarrollo.

Gráfico 1: Usuarios de la Red (Millones de usuarios)



Fuente: Internetworldstats¹³

¹¹ Los datos que aparecen en el presente capítulo se han extraído de: *Blogs y Microblogs en el entorno 2.0* – Marzo 2010. Esic, salvo que se indique explícitamente otra fuente, registrándose en la correspondiente nota al pie.

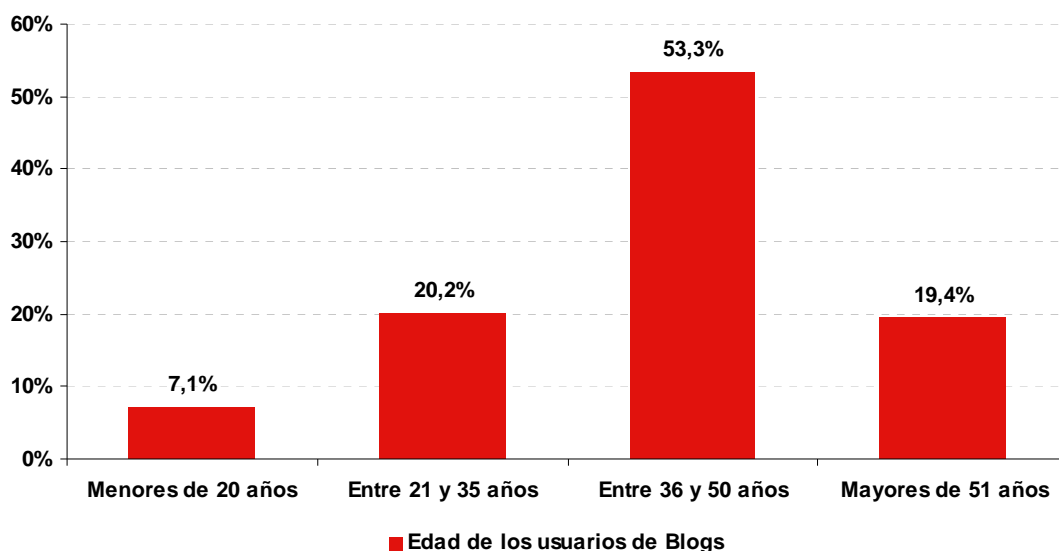
¹² Fuente: *El mundo en 2010: hechos y cifras de las Tecnologías de la Información y la Comunicación* - Unión Internacional de Telecomunicaciones (UIT) Disponible en: <http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf>

¹³ Disponible en: <http://www.internetworldstats.com/stats.htm>

En los blog

- **133** millones de blogs en Internet.
- **120.000** nuevos blogs al día
- **1.500.000** posts nuevos en blogs cada día.
- El **77%** de los internautas dice leer blogs cada día.

Gráfico 2: Distribución de los usuarios de blogs por franjas de edad



Fuente: Technorati¹⁴

En microblogging

- **150.000.000** usuarios en Twitter.
- **70** millones de tweets (comentarios) diarios¹⁵.
- **800** tweets por segundo.



¹⁴ Disponible en: <http://images.vizworld.com/wp-content/uploads/2010/07/the-internet.jpg>

¹⁵ Información extraída de: http://www.slideshare.net/raffikrikorian/twitter-by-the-numbers?from=ss_embed

En redes sociales

- **8 de cada 10** internautas pertenecen a una red social.
- **600.000.000** usuarios en Facebook.¹⁶
- **260.000.000.000** visitas al mes en esta red social.
- Más de **6.000.000** de visitas por minuto.



facebook

En otras herramientas 2.0...

- Más de **4 millones** de usuarios de Foursquare.
- **2.000.000** videos reproducidos al día en Youtube¹⁷.
- Cada minuto se suben **24** horas de video a Youtube¹⁸.



En cuanto a las amenazas existentes en la Web 2.0...

- Aproximadamente **1 de cada 4** comunicaciones sospechosas de ser fraudulentas en Internet se dirigen a redes sociales¹⁹.
- Facebook se convierte en la **cuarta** web más suplantada a nivel mundial²⁰.

¹⁶ Fuente: ComScore, WSJ Disponible en: <http://technorati.com/state-of-the-blogsphere/>

¹⁷ Datos de Website-monitoring.com 10/05/2010. Disponible en: <http://www.cleancutmedia.com/wp-content/uploads/2010/05/youtube-infographic-statistics.jpg>

¹⁸ Disponible en: <http://youtube-espanol.blogspot.com/2010/03/lo-logramos-un-dia-de-video-por-minuto.html>

¹⁹ Según datos por el Anti-Phishing Working Group (APWG) para el primer trimestre del 2010 y recogidos en el Estudio sobre el fraude a través de Internet 2º trimestre de 2010, disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_fraude_2T2010

²⁰ Fuente: <http://www.bitdefender.es/NW1659-es--Facebook-se-convierte-en-la-cuarta-empresa-m%C3%A1s-suplantada-en-los-ataques-de-phishing.html>

1.4 EL PAPEL DE LAS TECNOLOGÍAS MÓVILES EN EL FUTURO DE LA WEB 2.0

Las distintas plataformas y herramientas de la Web 2.0 están apostando por la integración de las tecnologías móviles y la difusión de un nuevo modelo de conexión a Internet.

Este modelo permitirá que el número de accesos y de actualizaciones de las páginas, los perfiles y las entradas de los usuarios en la Web 2.0 alcance límites cercanos al tiempo real, modificando el panorama actual de medios. A su vez la interoperabilidad entre las diferentes plataformas y el aumento y desarrollo de herramientas permitirán a los usuarios prescindir por completo de aplicaciones locales en favor de aplicaciones tanto móviles como en la nube.

Por tanto, la aparición de nuevos dispositivos móviles con más funcionalidades y la creación de plataformas como Android, iOS, Windows Phone 7 o WebOs, configuran la base necesaria para utilizar estos canales desde cualquier parte y con una simple conexión a Internet.

2. LA WEB 2.0 EN EL DESARROLLO SOCIAL, PROFESIONAL Y EDUCATIVO



2.1 ÁMBITO SOCIAL

A medida que el uso de la Web 2.0 se ha ido ampliando, los ciudadanos disponen de nuevas **posibilidades de participación en un contexto social**:

- El usuario se siente útil e integrado en un grupo, con el que se comunica y con el que comparte aficiones e inquietudes.
- Las personas se convierten en exploradores activos del conocimiento, según sus intereses, ganas y voluntad de aprendizaje, aumentando las capacidades de búsqueda, análisis y toma de decisiones.
- Se incrementa la importancia de las recomendaciones personales y profesionales, proporcionando, además de información ilimitada, una voz, una plataforma y el acceso a un mercado global.

La Web 2.0 pone a disposición del individuo una amalgama de herramientas que amplía las posibilidades de contacto con otras personas.

- Aplicaciones para crear y mantener sitios personales como las redes sociales o los blogs, o mediante la participación en páginas colaborativas como las wikis.
- Aplicaciones para publicar y difundir información: videos con YouTube, imágenes con Flickr, presentaciones con SlideShare.
- Aplicaciones para buscar y acceder a información actualizada: Google, Bing, GoogleReader, Google News, Twitter, buscadores especializados...
- Otras aplicaciones online como calendarios, herramientas de geolocalización, libros virtuales compartidos, noticias, ofimática online, plataformas de teleformación, pizarras digitales, etc.

Todas ellas son herramientas que permiten una interacción y una comunicación entre personas que no se podría dar por otro medio, fomentando la cooperación y permitiendo crear un conjunto en base a las sucesivas aportaciones individuales.

2.2 ÁMBITO EDUCATIVO

La Web 2.0 ofrece una nueva **perspectiva a docentes, profesores e investigadores** de la pedagogía y educación, ya que las herramientas que proporciona actúan como complemento en la formación integral del alumnado.²¹

Mediante la creación de entornos participativos y colaborativos:

- Se habilitan espacios online para el almacenamiento, clasificación, publicación y/o difusión de contenidos textuales y audiovisuales, a los que los alumnos pueden acceder.
- Se desarrollan y mejoran las competencias digitales, desde la búsqueda y selección de información y su proceso para convertirla en conocimiento, hasta su publicación y transmisión por diversos medios.
- Se proporcionan entornos para el desarrollo de redes de centros y profesores donde reflexionar sobre los temas educativos, ayudarse, elaborar y compartir recursos.
- Aparecen nuevas herramientas de trabajo como *eBooks* o *tablets*, que permiten la interacción entre el profesor y el alumno en tiempo real.

Desde el **punto de vista del alumno**, utilizar las posibilidades que ofrece la llamada Web 2.0 permite al individuo utilizar un conjunto de nuevas herramientas y funcionalidades que pueden apoyarle en su educación, teniendo en cuenta que el alumno, sobre todo hablando de menores, es un auténtico ciudadano digital, que ve las TIC como parte de su vida diaria.

Las **plataformas educativas** son herramientas online que permiten a los profesores trabajar en equipo en todas las materias, pudiendo estructurar las clases en grupos de trabajo colaborativo entre sus estudiantes y entre investigadores.

Cabe distinguir varias categorías o modalidades de uso de dichos medios en diferentes situaciones de formación:

²¹ En la realización del presente apartado se han utilizado las siguientes fuentes:

- Orihuela, José Luis. (2007) Reseña de *La revolución de los Blogs. Cuando las Bitácoras se convirtieron en el medio de comunicación de la gente*. Universidad Oberta de Catalunya.

- Blogs y Wikis para la docencia. Formando Formadores *Hay talento 2009*.

- VV.AA. *Wikis e Innovación docente* Revista de Educación a Distancia.

- Sistemas de gestión de recursos didácticos: El profesor propone, como complemento a la clase presencial, una serie de actividades que el alumno deberá desarrollar empleando los recursos del medio.
- Blogs de profesores: grupos de docentes que comparten experiencias educativas, estrategias y recursos.
- Diarios de clase o tutoría: en los que se narra de manera cronológica la evolución de un grupo de alumnos, el grado de consecución de los objetivos establecidos, cuestiones metodológicas o aspectos de comportamiento y actitud relativos al alumnado.
- Cuadernos de trabajo individual: Son páginas dinámicas de autor. En el ámbito escolar sustituyen al cuaderno de clase, proporcionando el aliciente de poder ser visitadas en Internet y enriquecidas con las aportaciones de otros estudiantes y profesores.

2.3 ÁMBITO PROFESIONAL

La mayor parte de los blogs, wikis, foros y demás plataformas colaborativas que se encuentran en la Red son personales, si bien existe una tendencia creciente en las empresas a utilizarlas de forma corporativa.

Así, se encuentran **plataformas de uso interno**, a partir de las cuales las empresas comparten conocimientos dentro de la organización y con sus colaboradores; y **plataformas externas** que sirven como herramienta de comercialización y también de creación y mantenimiento de relaciones con sus clientes. En ambos casos, el papel de la dirección es fundamental, como promotor del uso de estos canales de forma abierta y multidireccional, para potenciar su efectividad.

El nuevo escenario de la web social supone una nueva realidad que afecta a las empresas en su conjunto aportándoles una serie de ventajas. Las principales son la posibilidad de crear mejores canales para compartir ideas, acceso más fácil, rápido y directo a expertos (tanto internos como externos) y menores costes de comunicaciones y operaciones²².

Otras ventajas son la capacidad de compartir toda la información vía plataformas web, la propagación inmediata de contenido e información, la innovación constante que se produce en la Red y el acceso en todo momento a la información desde cualquier lugar mediante dispositivos móviles.

²² Disponible en:

http://www.mckinseyquarterly.com/Business_Technology/BT_Strategy/How_companies_are_benefiting_from_Web_2.0_McKinsey_Global_Survey_Results_2432?pagenum=2#1

3. DERECHOS Y LIBERTADES A PROTEGER EN LA WEB 2.0

La Web 2.0 permite a los ciudadanos crear una fuente de información imparcial y diversa, aunque el anonimato que proporciona es utilizado en muchas ocasiones de manera inapropiada, sobrepasando los límites de los derechos individuales en detrimento de los derechos de otros.

A continuación, se tratan en profundidad los distintos bienes jurídicos afectados en la comunicación digital 2.0, aportando en la medida de lo posible ejemplos que facilitan la comprensión al lector²³.

3.1 LA LIBERTAD DE EXPRESIÓN EN LA WEB 2.0

El principal derecho que permite expresarse tanto en el ámbito de Internet como fuera de él es la **libertad de expresión**, recogido por la Constitución Española en su artículo 20 y que permite *expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción y comunicar o recibir libremente información veraz por cualquier medio de difusión*.



Dicho derecho legitima a los ciudadanos al realizar una labor participativa en las diversas plataformas.

Cualquier persona puede participar en foros, blogs, wikis o redes sociales, pero en sus participaciones debe mantener un respeto hacia los demás participantes y hacia terceros, no exento de ciertas dosis de sentido común.

²³ En la redacción del presente capítulo, se han tomado como base los siguientes documentos:

- Agencia Española de Protección de Datos (2010) "Estudio sobre la privacidad de los datos personales y la seguridad de http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf
- Derecho en Red (2009) "Guía Legal para bloggers y podcasters" http://www.derechoenred.com/blog/documentos/GUIA_LEGAL_BLOGGERS_POCASTERS.pdf
- Mata, Miguel Angel (2009) "Libertad de expresión en Internet" <http://www.miguelangelmata.com/2009/10/23/libertad-de-expresion-en-internet/>
- Maeztu, David (2008) "Prensa y Blogs: Aspectos legales, diferencias, similitudes y tratamiento jurisprudencial en España." <http://derechoynormas.blogspot.com/2008/04/prensa-y-blogs-aspectos-legales.html>
- Maeztu, David (2006) "Obligaciones jurídicas de los blogs (I): Obligaciones Tributarias" <http://derechoynormas.blogspot.com/2006/12/obligaciones-juridicas-de-los-blogs-i.html>

3.2 LA LIBERTAD DE INFORMACIÓN EN LA WEB 2.0

Unido a la libertad de expresión destaca de manera conexas un segundo derecho a la **libertad de información**. Sin embargo se diferencia del anterior en que presenta unos requisitos objetivos:

- Que la información sea veraz, es decir, que exige la existencia de una base en hechos objetivos y reales.
- Que la información tenga relevancia pública, careciendo de dicha relevancia los hechos que afectan a personas privadas en actuaciones o hechos cotidianos.

Estos elementos son claves en la diferenciación de la participación en la Web 2.0 con la prensa tradicional, dado que la posibilidad de encontrar referencias hacia personas de un entorno cercano sobre los que se comenta y opina no siempre se van a encontrar amparados por la libertad de información.

Comentar las intimidades de una persona “cercana” que no tiene el carácter de personaje público no quedaría amparado bajo la protección del derecho de libertad de información y, en función de los comentarios realizados, podría traspasar los límites del derecho a la libertad de expresión.

3.3 LA INTIMIDAD, PRIVACIDAD Y PROPIA IMAGEN EN LA WEB 2.0

El **derecho al honor, a la propia imagen y a la intimidad personal** está recogido por la Constitución Española (artículo 18), y se desarrolla en la Ley Orgánica 1/1982, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

Es uno de los principales derechos que se pueden lesionar al participar en las plataformas de la Web 2.0, ya que implica interferir en el ámbito personal del individuo afectado a través de comentarios, informaciones u opiniones que representan **injurias o calumnias**, como:



- La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.
- La captación, reproducción o publicación de fotografías o películas de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en la propia ley.

- La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios o comerciales.
- La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona o menoscaben su fama.

Además, dentro de la parcela de intimidad de las personas, destaca el **secreto de las comunicaciones**, que implica que cualquier comunicación privada está protegida por la Ley. Es decir, interceptar mensajes ajenos o utilizar dispositivos para escuchar, transmitir, grabar o reproducir estas comunicaciones es una infracción legal, sancionada con multa.

Es frecuente la suplantación de la personalidad en los perfiles y páginas de las herramientas Web 2.0. El usuario malintencionado se registra en nombre de otro y publica comentarios, fotos, etc. que son falsos. Esta actividad está tipificada por el Código Penal español.

3.4 LA PROTECCIÓN DE DATOS EN LA WEB 2.0

El **derecho a la protección de datos** es un derecho fundamental, que emana directamente de la Constitución Española de 1978 (artículo 18.4) en consonancia con la normativa europea. La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) desarrolla este derecho en profundidad.

En la medida en que cada internauta puede ser protagonista, editar su página personal, participar en wikis, crear su web o mantener su blog, asume con ello una responsabilidad jurídica.

Respetar el derecho a la protección de datos de otras personas implica²⁴:

- *No publicar informaciones que no respondan a los requisitos de veracidad, interés público y respeto a la dignidad de las personas, y en particular a la juventud y la infancia.*
- *No difundir rumores o informaciones no contrastadas.*
- *Rectificar o retirar la información cuando lo solicite el afectado.*

²⁴ Fuente: Guía de recomendaciones en Internet AEPD. Disponible en:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_recomendaciones_internet_052009.pdf

- *Nunca publicar información que ponga en riesgo a la familia y en particular a los menores, amistades, vecinos, etc.*
- *Tener especial cuidado respecto a la publicación de información relativa a los lugares en que el usuario o un tercero se encuentra en todo momento, ya que podría suponer un grave riesgo para su integridad.*
- *No grabar ni publicar imágenes, videos o cualquier otro tipo de registro sin el consentimiento de los afectados.*
- *En el caso de los menores de 14 años, la LOPD obliga a los padres o tutores a prestar su consentimiento para el tratamiento de sus datos.*

En ocasiones, las plataformas disponen de todo o parte del perfil de usuario en formato público por defecto, por lo que cualquier usuario puede acceder a información de carácter personal ajena sin que el propietario real de los datos tenga que dar su consentimiento expreso.

3.5 LA PROPIEDAD INTELECTUAL EN LA WEB 2.0

La propiedad intelectual es el derecho que tienen las personas sobre las creaciones propias u obras, como reconoce el Real Decreto Legislativo 1/1996 de 12 abril por el que se aprueba la Ley de Propiedad Intelectual.

En el contexto de la Web 2.0, los usuarios podrán utilizar en plataformas colaborativas:

- Cualquier obra que hayan creado (siempre que no hayan cedido los derechos de explotación a otros).
- Obras con autorización de sus titulares de derechos, ya sea de forma directa o a través de cualquiera de las licencias existentes en la actualidad (*Creative Commons*, *GPL*, etc.).
- Obras caídas en el dominio público²⁵.
- Obras expuestas permanentemente en la vía pública (carteles, esculturas, etc.).
- Discursos o conferencias pronunciadas en público, siempre y cuando tenga una finalidad informativa (y no meramente comercial).



²⁵ Lo cual ocurre generalmente pasados 70 años desde la muerte del autor y 50 años desde la publicación, para las grabaciones sonoras o audiovisuales).

- Trabajos sobre temas de actualidad, en la medida descrita anteriormente.

Por tanto, según esta ley, **NO** se podrá utilizar en las plataformas 2.0:

- Obras y prestaciones protegidas por propiedad intelectual, salvo que cumplan alguna de las excepciones mencionadas anteriormente.

Siempre que se quiera utilizar alguna obra (textos, fotografías, vídeos, etc.) de Internet se debe acudir al aviso legal de la página donde se haya encontrado el contenido y observar si éste permite su reproducción.

4. RIESGOS EN EL USO DE LA WEB 2.0

Vistas las materias a proteger es necesario comprender que hay una serie de riesgos y que es importante conocer para poder adoptar unas medidas que garanticen la seguridad y privacidad y por tanto, el pleno disfrute en el entorno 2.0.

- **Riesgos de injurias y calumnias.**
- **Riesgos en las comunicaciones.**
- **Riesgos contra la privacidad.**
- **Riesgos contra la propiedad intelectual.**

Dentro de los riesgos existentes en las comunicaciones colaborativas, el **componente tecnológico** juega un papel fundamental. La capacidad actual del malware o código malicioso para aprovechar vulnerabilidades y fallos de seguridad de las plataformas colaborativas, multiplican los posibles efectos de sus ataques en la información de los perfiles y en los equipos y programas de los usuarios:

- **Infección y/o alteración de los equipos, aplicaciones y programas**, tanto del usuario como de su red de contactos.
- **Robo de información personal**, como nombres de usuarios y contraseñas, fotografías, aficiones, números de tarjetas..., información que puede ser utilizada con fines lucrativos o publicitarios.
- **Suplantación de la identidad del usuario**, bien creando cuentas falsas en nombre de otros usuarios, bien robando datos de acceso a los perfiles para sustituir al verdadero usuario.

A continuación, se incluyen algunas de las técnicas utilizadas para llevar a cabo los ataques de seguridad y privacidad en plataformas colaborativas.

- **Social Spammer y Scammer.** El uso de estas plataformas es una oportunidad para el envío de correos electrónicos no deseados, tanto si la finalidad es meramente publicitaria (spam), como si implica fraude o lucro indebido (scam).
- **Tabnabbing.** Esta técnica se basa en aprovechar el sistema de navegación por pestañas o *tabs*. Cuando el usuario va de una pestaña a otra, la que permanece en segundo plano se transforma en una página de acceso a servicios y plataformas (como Gmail, Youtube, Facebook, etc.). El usuario, al no percatarse, introduce los datos de acceso a estos servicios, y por tanto, está facilitando estos datos al propietario de la página falsa.

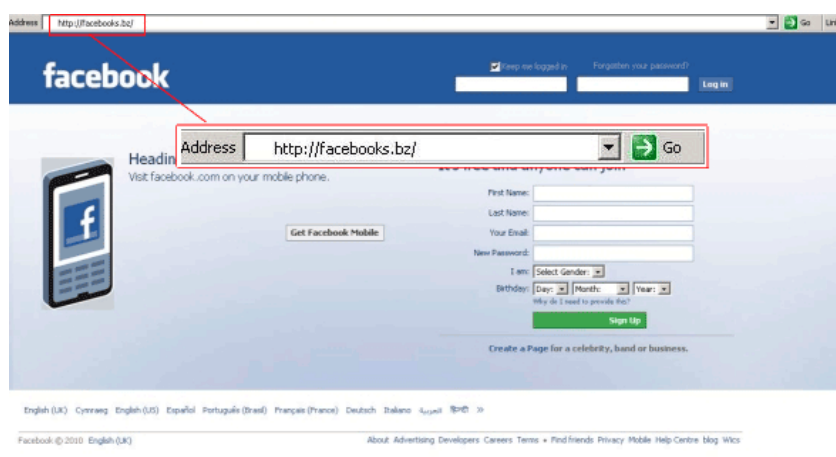


Ilustración 3: Ejemplo de tabnabbing

- Pharming.** Este ataque informático consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de la plataforma Web 2.0. Al escribir el nombre de la plataforma en la barra de direcciones, el navegador redirige automáticamente al usuario a otra dirección IP, donde se aloja una web falsa. Al intentar acceder al servicio, el usuario está facilitando sus datos de acceso al ciberatacante.

Tanto el phishing como el pharming están muy explotados por los delincuentes para lograr la obtención de datos personales de los usuarios de Internet, así como datos de carácter sensible o relativos a aspectos económicos (tarjetas de crédito, PIN de usuarios, etc.).

- Clickjacking.** En este caso, al hacer *click* en “Me gusta” (botones para compartir opiniones sobre un contenido), se actualizan en el estado del usuario frases que redirigen hacia webs de spam o malware. También se pueden encontrar mensajes que enlazan hacia webs fraudulentas, como en el siguiente ejemplo en Twitter:

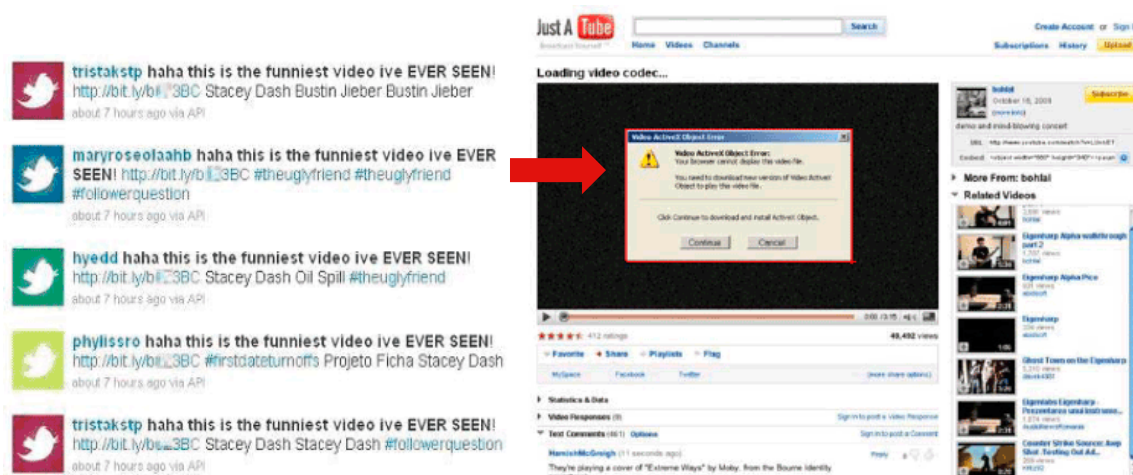


Ilustración 4: Ejemplo de clickjacking en Twitter

En este sentido, en Twitter se está extendiendo el uso de acortadores de URL (dadas las limitaciones de caracteres por mensaje) que enlazan a páginas web maliciosas.

- **Gusanos.** Los gusanos constituyen una de las amenazas con mayor repercusión, ya que disponen de variantes diseñadas para diferentes plataformas Web 2.0, como es el caso del gusano Koobface y sus variantes para las principales redes sociales. Este tipo de malware utiliza cuentas de usuarios ya comprometidas para propagarse, colocando enlaces infectados en los que fácilmente pinchan los contactos del usuario víctima.
- **Instalación y uso de cookies²⁶ sin conocimiento del usuario.** Otro riesgo relacionado con la participación del usuario en las plataformas radica en la posibilidad de que el sitio web utilice cookies que permitan a la plataforma conocer cuál es la actividad del usuario dentro de la misma. Mediante estas herramientas pueden conocer el lugar desde el que el usuario accede, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil), el sistema operativo utilizado, los sitios más visitados dentro de una página web, el número de *clicks* realizados, e infinidad de datos respecto al desarrollo de la vida del usuario dentro de la Red.

²⁶ Una cookie es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página.

5. OBLIGACIONES Y RESPONSABILIDADES EN EL USO DE LA WEB 2.0

La evolución de la Red ha permitido un cambio desde un modelo en el que el internauta ocupaba un papel pasivo como mero lector, a un papel activo y protagonista.

En la Web 2.0, no resulta necesario tener un conocimiento experto las aplicaciones y servicios, ya que están pensados para ser fáciles e intuitivos. Basta con registrarse para acceder a un conjunto de programas y servicios que permiten participar en las nuevas plataformas y mantener una interacción en tiempo real con otros usuarios de la Red.

En esta actividad se identifican varios roles: usuarios, administradores, moderadores y prestadores de servicios. **La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico (LSSICE)** identifica a los diferentes actores en esta actividad y establece el régimen de responsabilidad civil al que están sujetos.

5.1 RESPONSABILIDADES DE LOS DIFERENTES ACTORES

5.1.1 Usuarios

Quiénes son:

Los usuarios de la Web 2.0 son aquellos internautas que participan en la misma, bien editando y publicando comentarios, subiendo videos, imágenes, etc. o bien comentando lo publicado por otros. En definitiva, navegando activamente en cualquiera de las plataformas que componen este universo social.

El hecho de registrarse como usuario de cualquier herramienta o plataforma implica la adhesión a unas condiciones establecidas por el prestador del servicio.

Obligaciones:

Los usuarios pueden subir todo tipo de contenidos a su sitio, pero siempre haciendo un uso responsable de la libertad de expresión.

Exceden a las funciones del usuario y, por tanto, son conductas ilícitas:

- Cometer el delito de injurias o calumnias al realizar una falsa imputación de un delito a otra persona o manifestar expresiones que atenten contra el derecho al honor, a la propia imagen y a la intimidad personal.
- Incurrir en violaciones a la Ley de Propiedad Intelectual (Derechos de Autor) al publicar cualquier obra protegida que no cuente con la expresa autorización del titular o no se haga un uso correcto del derecho de cita, ya sea sobre textos (artículos, libros, notas, etc.), o contenidos multimedia (música, audio, video, software, etc.).

- Violar derechos de marca, de diseño, secretos comerciales o violar derechos industriales (como patentes).
- Atentar contra el derecho a la protección de datos publicando información privada de terceros (publicar un correo electrónico personal).
- Cometer delitos de pornografía infantil al publicar cualquier representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales.

Responsabilidades:

La responsabilidad será en todo caso de la persona que cometa el hecho delictivo. Sin embargo, dicha responsabilidad puede ampliarse a otras personas por la falta de una vigilancia correcta de la plataforma como se verá en el apartado siguiente.

Por ejemplo, publicar un vídeo de otra persona, la cual no ha otorgado su consentimiento expreso para que se realizara esta difusión e incluso para que se grabara ese vídeo, supone un atentado contra su honor y su intimidad personal.

5.1.2 Administradores y moderadores

Quiénes son:

- Los administradores (propietarios de la página o no), son los encargados de la gestión de la página, y cuentan con las opciones necesarias para editar y eliminar contenidos. Pueden ejercer de moderadores en caso de ausencia de estos.
- Los moderadores controlan el tono y contenido de la información que se escribe en la plataforma, tratando de mantener un ambiente cordial y agradable para todos los usuarios del mismo. Para ello, pueden modificar o eliminar comentarios ajenos, retirar temporalmente un mensaje, o cerrar y eliminar discusiones, además de otros mecanismos designados por la plataforma.

Obligaciones:

Tienen la obligación de velar por el correcto uso de la plataforma a fin de que no se cometan hechos delictivos en la misma. Según la legislación española, es necesaria la existencia de una moderación de contenidos, ya que aún cuando el comentario es anónimo, el medio debe asumir el comentario y hacerlo propio.

Responsabilidades:

Sus responsabilidades vienen derivadas de las labores de gestión, así como de control y supervisión, bien a priori, bien a posteriori una vez que se ha insertado un comentario.

Un reciente cambio jurisprudencial ha agravado dicha responsabilidad a la responsabilidad como autor, con lo que son sancionables tanto el autor del comentario como el responsable del foro, página web, plataforma colaborativa, etc., según el artículo 28 del Código Penal.

Es una buena práctica que el administrador de un foro incluya en su página una política de publicación, para evitar entradas inapropiadas de los usuarios, así como la posibilidad de que otros usuarios denuncien estas situaciones y se pueda realizar un control posterior más efectivo.

5.1.3 Empresas prestadoras de servicios de intermediación en Internet

Quiénes son:

Los prestadores de servicios de alojamiento de páginas web, servicios web 2.0, servicios de alojamiento de datos, los proveedores de acceso, los operadores de telecomunicaciones.

Obligaciones:

- Informar a los clientes sobre los principales datos como prestadores de servicios (identificación y correo electrónico), los servicios prestados y los términos de la prestación, la política de protección de datos, así como los medios técnicos que aumenten la seguridad de los usuarios.
- Colaborar con los organismos públicos para ejecuciones que no puedan realizarse sin su ayuda.

Responsabilidades:

- Son responsables de los contenidos si tienen conocimiento efectivo de que la actividad o la información a la que remiten es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización.
- Son responsables en cuanto a los datos de carácter personal que se tratan en los buscadores de perfiles o en las campañas de publicidad personalizada.

A la hora de crear un blog o página personal, cualquier individuo puede optar por utilizar páginas o herramientas ya existentes en la Red y que ofrecen este servicio (por ejemplo, Wordpress o Myspace), o puede acudir a una empresa de hospedaje y crear un dominio propio. En ambos casos, las empresas que ofrecen los servicios están dentro de esta categoría.

5.2 PREGUNTAS FRECUENTES

Si crea un dominio propio para alojar una página personal en la que otros usuarios pueden comentar ¿es responsable de los comentarios establecidos por estos otros usuarios?

Hasta que se identifique al verdadero autor del comentario, la jurisprudencia puede aplicar la responsabilidad en cascada al propietario de la página personal. En este sentido, la inclusión o no de publicidad en la página (y por tanto, la generación de un lucro) determina la responsabilidad del propietario:

- Si tiene publicidad: el propietario es considerado prestador de servicios estando su responsabilidad limitada a lo dispuesto en el artículo 16 de la LSSICE.
- Si no tiene publicidad: se aplica el Código Penal para asignar la responsabilidad correspondiente al propietario, pudiendo considerarle como medio tradicional o como cooperador necesario.

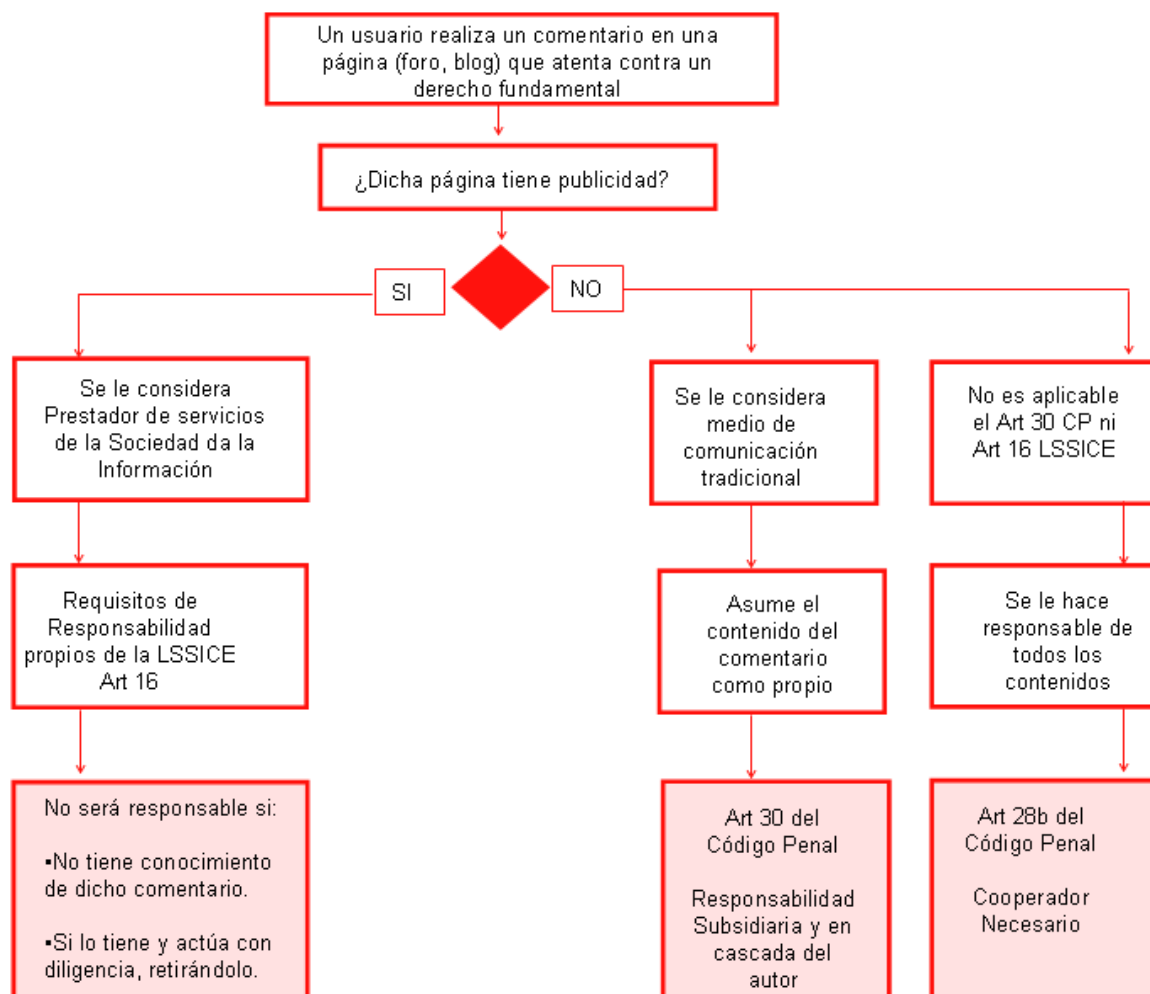


Ilustración 5: esquema de la responsabilidad del propietario de una página en la Web 2.0

¿Se puede pedir al propietario de la página a que identifique al autor de los comentarios?

Si un lector identifica en una página un comentario erróneo o difamatorio contra su persona, puede solicitar al propietario de la página que identifique al autor del comentario mediante los datos de que se dispongan, generalmente la dirección IP.

De acuerdo con el criterio de la Agencia Española de Protección de Datos, actualmente se considera que la dirección IP es un dato de carácter personal por lo que sólo se comunicará cuando lo requieran los jueces o tribunales. Por ello, se recomienda conservar esos datos de tal forma que no se destruyan y poderlos ofrecer al juzgado si así se requieren.

¿Puede exigirse una rectificación o réplica por parte del autor del comentario en caso de que se haya atentado contra el honor, la propia imagen y la intimidad personal?

Si, puede exigirse al autor y de forma ascendente, al propietario de la página, a que remedien el daño cometido al afectado.

El derecho de rectificación ampara a los particulares por informaciones erróneas o incompletas y establece que la rectificación debe dirigirse al director del medio o propietario de la página. El derecho de réplica ampara las opiniones erróneas, aunque no está materializado formalmente en el ordenamiento español.

¿Se puede cerrar una página personal si se infringe algún derecho?

La CE en su artículo 20.5 prohíbe el secuestro de publicaciones, grabaciones y otros medios de información si no es realizado en virtud de resolución judicial. Sin embargo el Proyecto de Ley de Economía Sostenible, en proceso de aprobación en el Senado²⁷, en su disposición final segunda modifica el procedimiento judicial actual.

Según esta Ley se establece una Comisión de Propiedad Intelectual que, en aquellos casos en que considera que se infringe el derecho de propiedad intelectual, puede solicitar al Juez que el proveedor del servicio proporcione los datos de un cliente determinado para su identificación. Esta Comisión también puede emitir resoluciones de cierre de publicaciones siendo necesaria la autorización de un Juez para ejecutar dichas resoluciones.

²⁷ A fecha de publicación de esta guía

6

RECOMENDACIONES PARA UN USO SEGURO Y RESPONSABLE DE LA WEB 2.0

6.1 BUENAS PRÁCTICAS DE PRIVACIDAD EN LA WEB 2.0

Vistos los posibles riesgos de la Web 2.0, se proporcionan a continuación una serie de pautas de privacidad, dirigidas a cada colectivo implicado.

6.1.1 Usuarios

En la Web 2.0 los usuarios deben respetar unas normas de privacidad, tanto en lo relativo a datos propios, como si la información que difunden es de terceros.

- Los usuarios deben proteger su información. Por ello, es necesario leer las políticas de privacidad, estableciendo unos límites sobre quién puede o no acceder a la información publicada.
- Una buena práctica es recurrir al uso de seudónimos o *nicks* personales permitiéndole disponer así de una “identidad digital”.
- No se debe publicar información excesiva de la vida personal y familiar, esto es, información que no se difundiría en entornos no tan cercanos.
- Es necesario tener especial cuidado al publicar contenidos audiovisuales y gráficos, especialmente si son imágenes relativas a terceras personas.
- Antes de publicar una foto es recomendable considerar si es adecuado colgarla o si dicha acción puede traer consecuencias, involucrando a gente del trabajo, colegio, universidad o del entorno cercano o personal.
- Si se desea utilizar o reproducir cualquier obra en la Red (gráfica o no), se debe acudir al aviso legal de la página web donde se encuentre y ver las condiciones de reproducción de la misma.
- Acudir a la Agencia de Protección de Datos, AEPD (www.agpd.es), para ejercer los derechos que otorga la LOPD en relación a la protección de los datos de carácter personal. En el sitio de la AEPD se puede descargar un modelo de reclamación.



6.1.2 Administradores y moderadores

En este grupo, las pautas de privacidad están relacionadas con la protección de datos e informaciones de carácter personal de los usuarios, así como con la defensa de la legalidad por parte de los usuarios de la plataforma que gestionan.

- Según se establece en la LOPD, toda persona que trate datos de carácter personal (asociados a buscadores, a perfiles, etc.) debe cumplir unas obligaciones y atender a los afectados de dicho tratamiento. Entre otras, debe haber un titular que realice un tratamiento de datos:
 - Debe inscribir el fichero en el Registro de la AEPD y adecuar los ficheros a la normativa vigente (LOPD y Reglamento de desarrollo).
 - Está obligado a informar a los usuarios sobre la Política de Privacidad de la página web, así como de la finalidad para la que se recaban datos de carácter personal, el Responsable del Tratamiento y los derechos de que dispone el usuario.
 - Debe recabar el consentimiento inequívoco del afectado para difundir los datos de este.
 - Permite a los usuarios el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición.
- Es importante ejercer de una forma efectiva las labores de supervisión y control, sobre los participantes y sus informaciones. Ante comentarios o informaciones incorrectas o ilícitas, mediar en el debate y/o eliminar los comentarios.
- Hay que implementar medidas tecnológicas que permitan conocer la edad de los usuarios, tales como: el uso de certificados reconocidos de firma electrónica o de aplicaciones que detecten el tipo de sitio web visitado y los servicios más demandados.
- Es un deber colaborar con las Fuerzas y Cuerpos de Seguridad del Estado para identificar usuarios que cometen hechos ilícitos.

6.1.3 Empresas que prestan servicios de intermediación de la sociedad de la información

Los datos que los usuarios introducen en la Red son almacenados por parte de los prestadores de servicios de intermediación de la sociedad de la información (buscadores, formularios de registro, utilización de datos cruzados, etc.). Las actuaciones en materia de privacidad deben encaminarse al adecuado tratamiento de datos personales de usuarios de las plataformas.

- Al igual que en el caso de los Administradores, cumplir las obligaciones que establece la LOPD en relación al tratamiento de datos de carácter personal.

- Además, la ley prohíbe enviar "comunicaciones publicitarias" por correo electrónico u otro medio de comunicación electrónica "que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios".
- No retener datos de carácter personal de forma excesiva o injustificada, salvo que esta actuación responda a una colaboración con las Fuerzas y Cuerpos de Seguridad del Estado.
- Por último, deberán facilitar información a sus usuarios acerca de las posibles responsabilidades en que puedan incurrir por la vulneración de derechos de propiedad intelectual e industrial.

6.2 BUENAS PRÁCTICAS DE SEGURIDAD EN LA WEB 2.0

Las amenazas de seguridad en la Web 2.0 tienen un potencial de expansión superior al de otros medios, debido a su propia estructura en red. Por ello, todos los actores deben seguir unas pautas de seguridad.

6.2.1 Usuarios

Los usuarios son los principales perjudicados por los ataques de malware, que pueden afectar tanto a la información contenida en las plataformas colaborativas, como a sus propios equipos y dispositivos. Para evitarlo, se recomienda:

- Mantener actualizado el equipo, tanto el sistema operativo como cualquier aplicación que tenga instalada. Ello es fundamental dado que un navegador actualizado incorporara filtros de bloqueo frente a nuevas amenazas e intrusiones no deseadas.
- Utilizar contraseñas seguras para acceder a los diferentes perfiles.
- Comprobar la legitimidad de los sitios web a los que se quiere acceder, vigilando las URLs en la ventana del navegador.
- Durante la navegación, sólo se deben descargar ficheros o aplicaciones de fuentes confiables, a fin de evitar códigos maliciosos o malware. Se recomienda igualmente analizar con un antivirus los elementos descargados antes de ejecutarlos.

6.2.2 Administradores y moderadores

Se recomienda a estos actores de las plataformas de la Web 2.0:

- Disponer internamente de herramientas encaminadas a reducir los casos de suplantación de identidad de usuarios dentro de la Red, permitiendo a los legítimos titulares de los servicios que puedan autenticar su verdadera identidad,

para así recuperar y bloquear el acceso al usuario que ilegítimamente utilizó el perfil del otro.

- Integrar sistemas que detecten el nivel de seguridad de las contraseñas elegidas por los usuarios en el momento de registro, indicándole si es o no segura e informándole de los mínimos recomendables.

6.2.3 Empresas que prestan servicios de intermediación de la sociedad de la Información

Los prestadores de servicios de la sociedad de la información ligados a las plataformas colaborativas deben tener en cuenta que estos servicios se basan en grandes bases de datos, con datos personales de los usuarios que las utilizan. Por ello, deben:

- Garantizar que la Red es segura frente a posibles ataques de terceros y, que impide, o al menos reduce, la posibilidad de éxito de éstos.
- Es vital la correcta elección por parte de la plataforma, de un prestador de servicios de Internet (*Internet Service Provider* o ISP) que cuente con un nivel de seguridad alto.

En este sentido, se recomienda que el ISP garantice en todo momento, al menos, los siguientes aspectos:

- Los servicios prestados por los ISP a este tipo de plataformas se centrarán en servidores seguros, centros de respaldo, accesos seguros, etc.
- En los servidores y en la propia aplicación se deben utilizar herramientas destinadas a detectar, evitar y bloquear códigos maliciosos. En este sentido, se recomienda el fomento de acuerdos estratégicos con empresas de seguridad.
- Emplear aplicaciones de seguridad encaminadas a garantizar, o en su caso minimizar, la posibilidad de recepción de mensajes comerciales no deseados a través de la plataforma (spam/scam).
- A su vez deben informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.



inteco



Instituto Nacional
de Tecnologías
de la Comunicación



OBSERVATORIO
inteco

Web

<http://observatorio.inteco.es>



Canal Twitter del Observatorio de la Seguridad de la Información:

<http://twitter.com/ObservaINTECO>

BLOG

Blog del Observatorio de la Seguridad de la Información:

<http://www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad/>



observatorio@inteco.es