

Resumo executivo do “Estudo a privacidade dos datos persoales e a seguridade da información nas redes sociais online”



Edición: Febreiro 2009

A presente publicación pertence ao Instituto Nacional de Tecnoloxías da Comunicación (INTECO) e á Axencia Española de Protección de Datos (AEPD), está baixo unha licenza Recoñecemento-Non comercial 2.5 España de Creative Commons, e por iso está permitido copiar, distribuír e comunicar publicamente esta obra baixo as condicións seguintes:

- Recoñecemento: O contido deste informe pódese reproducir total ou parcialmente por terceiros, citando a súa procedencia e facendo referencia expresa tanto a INTECO e á AEPD como aos seus sitios web: www.inteco.es, www.agpd.es. Devandito recoñecemento non poderá en ningún caso suxerir que INTECO ou a AEPD prestan apoio a devandito terceiro ou apoian o uso que fai da súa obra.
- Uso Non Comercial: O material orixinal e os traballos derivados poden ser distribuídos, copiados e exhibidos mentres o seu uso non teña fins comerciais. Ao reutilizar ou distribuír a obra, ten que deixar ben claro os termos da licenza desta obra. Algunha destas condicións pode non aplicarse se se obtén o permiso de INTECO e AEPD como titulares dos dereitos de autor.

Nada nesta licenza menoscaba ou restrinxen os dereitos morais de INTECO e AEPD.

Texto completo da licencia:

<http://creativecommons.org/licenses/by-nc/2.5/es/>

RESUME EXECUTIVO

I Situación: definición das redes sociais

- As redes sociais online son servizos prestados a través de Internet que permiten ós usuarios xerar un perfil público, no que plasmar datos persoais e información dun mesmo, dispoñendo de ferramentas que permiten interactuar co resto de usuarios, afíns ou non, ó perfil publicado.
- O modelo de crecemento destas plataformas basease fundamentalmente nun proceso viral, no que un número inicial de participantes, mediante o envío de invitacións a través de correos ós seus coñecidos, ofrece a posibilidade de unirse o sitio web.
- Estos novos servizos configuranse como poderosos canais de comunicación e interacción, que permiten ós usuarios actuar como grupos segmentados: ocio, comunicación, profesionalización, etc.
- Un dos principais obxetivos da rede social alcanzase no momento no que os seus membros utilizan o medio online para convocar actos e accións que teñan efectos no mundo offline.
- A nivel mundial, as últimas estadísticas (3ª Oleada do Estudo Power to the people social media, Wave 3 de Universal McCann de marzo 2008) cifran o número de usuarios de redes sociais en 272 millóns, un 58% dos usuarios de Internet rexistrados en todo o mundo, o que supón un incremento do 21% respecto dos datos rexistrados en xuño do 2007.
- En España as fontes estadísticas son diversas, pero todas coinciden que no 2008 o número de usuarios españois de Internet que utiliza habitualmente redes sociais sitúase entre o 40% e o 50%¹. Dando a cifra dunha fonte concreta, tomaremos a que ofrece o estudo anteriormente citado: o 44,6% dos internautas españois ten un perfil nalgunha rede social. Desta forma, en España 7.850.000² usuarios habituais de Internet -maiores de 15 anos e con conexión no último mes- utilizan redes sociais.

¹ Por exemplo, un 50 % según Zed Dixital (O fenómeno das redes sociais. Percepción, usos e publicidade. Novembro 2008) ou un 45 %, según The Cocktail Analysis (Observatorio de evaluación de redes sociais: Ferramentas de comunicación on-line: As Redes Sociais. Novembro 2008).

² Calculouse aplicando a porcentaxe para España, dos datos do Estudo de Universal McCann a cifra de usuarios habituais de Internet obtida dos datos da Oleada XX de Red.es.

- Ademais, constatase que a porcentaxe de usuarios de redes sociais é máis alto entre os máis mozos e decrece coa idade: 7 de cada 10 son internautas menores de 35 anos.

II **Análise dos aspectos máis relevantes e problemática específica das redes sociais**

A notoriedade destes espazos sociais online non queda exenta de riscos ou posibles ataques malintencionados. É unha preocupación das organizacións nacionais, europeas e internacionais con competencias nas materias afectadas polo uso destas redes, que impulsaron a elaboración de normas e recomendacións³ dirixidas a garantir o acceso seguro dos usuarios –con especial atención ós colectivos de menores e incapaces -a estas novas posibilidades online.

Partindo desas premisas, este capítulo ofrece un **análise en profundidade sobre as cuestións xurídicas máis relevantes que afectan directamente as redes sociais:**

Protección da honra, a intimidade persoal e familiar e a propia imaxe dos usuarios

O **dereito a honra** é aquel que ten toda persoa a súa boa imaxe, nome e reputación, de tal forma que calquer cidadán pode esixir que se respete a súa esfera persoal, con independencia das circunstancias particulares, sendo un dereito irrenunciable. O **dereito a intimidade** ten por obxecto a protección da esfera máis íntima da persoa, e encontrase estreitamente ligado a protección da dignidade do individuo. Por último, o **dereito a propia imaxe** pretende salvagardar un ámbito propio e reservado do individuo, aínda que no íntimo, fronte a acción e coñecemento dos demais.

En España, a protección destes dereitos encóntrase amparada na **Lei Orgánica 1/1982, do 5 de maio, de Protección Civil do Dereito a Honra, a Intimidade Persoal e Familiar e a Propia Imaxe**, donde o lexislador español desenrola a disposición constitucional recollida no artigo 18.1 CE. Sen embargo, non se regulan de forma expresa determinadas situacións que poden chegar a derivarse do uso das redes sociais

³ As principais iniciativas regulatorias proveñen do plano internacional, especialmente da Comisión Europea e do Grupo de Traballo do Artigo 29, que nos últimos meses fixo pública a súa intención de regular no menor prazo posible tódolos aspectos relacionados coa seguridade e protección dos usuarios das redes sociais, sitios web colaborativos, blog e demais medios de interacción de usuarios en Internet.

Así, o pasado 15-17 de outubro do 2008, celebrouse a 30 Conferencia Internacional de Autoridades de Protección de Datos e privacidade en Estrasburgo. Nela acordouse levar a cabo unha proposta de regulación normativa deste tipo de plataformas que cumpra cos seguintes requisitos: ser unha normativa mundial, legalmente esixible a calquier tipo de prestador, con independencia de dónde se encontre ubicado; que dote ós usuarios dunha serie de proteccions consideradas básicas a hora de desenrolar a súa actividade na Rede; que garante unha protección mínima e básica para os menores, usuarios nativos deste tipo de servizos e especialmente desprotexidos ante éstos, así como que os prestadores establezan unha serie de medidas tecnolóxicas encamiñadas a protección dos usuarios. Desta forma, o próximo mes de novembro do ano 2009 celebrarase en Madrid, a 31 Conferencia Internacional de Protección de Datos, na que se propondrá un primeiro borrador da regulación mundial na materia de protección de datos, para o seu posterior debate e aprobación a nivel internacional.

e sitios webs colaborativos. Esta ausencia de regulación explícita, unida a rápida evolución dos servizos da Sociedade da Información, pode conlevar situacións que poñan en entredito a defensa dos dereitos dos usuarios, a hora de facer efectiva a aplicación normativa. Entre as **posibles situacións de risco para a protección da intimidade**, cabe sinalar:

- No momento do rexistro da alta como usuario, na medida no que non sexa configurado correctamente o nivel da privacidade do perfil, así como polo feito de que sexa publicada información sensible dende o inicio da actividade na rede.
- No momento de participación na rede como usuario, no suposto que o grado de información, datos e imaxes publicados poidan ser excesivos e afectar a privacidade, tanto persoal como de terceiros.
 - Privacidade persoal: a pesar de que sexan os usuarios os que voluntariamente publican os seus datos, os efectos sobre a privacidade poden ter un alcance maior ó que consideran nun primeiro momento xa que estas plataformas dispoñen de potentes ferramentas de intercambio de información, a capacidade de procesamento e o análisis da información facilitada polos usuarios.
 - Privacidade de terceiros: e esencial que os usuarios teñan en conta que a publicación de contidos con información e datos respecto a terceiros non pode ser realizada si éstos non autorizaron expresamente a súa publicación, podendo solicitar a súa retirada de forma inmediata.

Por último, e importante ter en conta que na gran maioría de ocasións, as redes sociais permiten ós motores de búsqueda de Internet indexar nas súas búsquedas os perfís dos usuarios, xunto coa información de contacto e de perfís amigos, o que pode supor outro risco para a protección da privacidade, ademais de dificultar o proceso de eliminación da súa información en Internet.

- No momento de darse de baixa da plataforma, no caso no que o usuario solicite dar de baixa o seu perfil, pero aínda así continúen datos publicados por éste, ou información persoal e imaxes propias publicadas nos perfís de outros usuarios.

Ademais existe en España, dende o punto de vista normativo, unha **protección especial para o caso de menores**, usuarios masivos deste tipo de servizos online, que lles otorga un estatus de protección mais elevado que ó resto de usuarios, xa que o consentimento para a disposición dos dereitos require da intervención dos seus pais ou titores legais.

Nos últimos anos o nivel de concienciación respecto a protección de dereito a intimidade e a protección de datos personais está sendo moito maior. Proba delo, e a publicación da

Lei 34/2002, do 11 de xullo, de Servizos da Sociedade da Información e de Comercio Electrónico (LSSI-CE) ó considerar a nova realidade social que supuxo o uso das TIC, en xeral, e Internet, en particular é dispor as bases normativas para unha regulación de Internet e os seus servizos de maneira completa, íntegra e efectiva.

Sen embargo, e como se recolle no Estudo, a adecuación práctica ó rápido desenvolvemento dos novos servizos que conleva a Sociedade da Información, entre os que se encontran as redes sociais, provoca situacións complexas para a aplicación e interpretación práctica da normativa. Por elo, *faise necesario emprender e desenvolver “tecnoloxía xurídica”, tomando como base actividades de I+D+i, que garante a protección dos usuarios sen que supoña un obstáculo para o desenvolvemento deste tipo de servizos.*

Protección de datos de carácter persoal

Este **dereito fundamental a protección de datos, regulado especificamente no artigo 18.4 da Constitución**, a diferenza do dereito a intimidade do art. 18.1 CE, con quen comparte o obxectivo de ofrecer unha eficaz protección constitucional da vida privada persoal e familiar, atribúe a súa titular un feixe de facultades que consiste na súa maior parte no poder xurídico de impoñer a terceiros a realización ou omisión de determinados comportamentos cuxa concreta regulación debe establecer a Lei. Desta forma, supón o “dereito a controlar o uso que se realice dos seus datos persoais, comprendendo, entre outros aspectos, a oposición do cidadán a que determinados datos persoais sexan utilizados para fins distintos de aquél lexítimo que xustificou a súa obtención”⁴.

Dada a gran cantidade de datos persoais que os usuarios publican nos seus perfís, éstos se convirten en auténticas “identidades dixitais” que facilitan un rápido coñecemento dos seus datos de contacto, preferencias e costumes.

A protección de datos de carácter persoal é un dereito amplamente desenvolvido legislativamente no ámbito comunitario e nacional. En España, a súa regulación lévese a cabo mediante **Lei Orgánica 15/1999, do 13 de decembro, de Protección de Datos de Carácter Persoal e por Real Decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento do Desenvolvemento da Lei Orgánica de Protección de Datos (RDLOPD)**. Ademais, existe un amplo desenvolvemento interpretativo por parte da Axencia Española de Protección de Datos (AEPD) que, mediante as súas resolucións, dou resposta os casos de vulneración de dereitos de protección de datos derivados do uso dos novos servizos que ofrece a Sociedade da Información, o que permite ós usuarios contar coa máxima garantía na protección dos seus dereitos persoais.

⁴ Extracto da Sentenza do Tribunal Constitucional 292/2000 donde se recoñece o Dereito a Protección de Datos, como un dereito fundamental absolutamente independente do Dereito á Honra, Intimidade e Propia Imaxe, outorgando así a protección de datos de carácter persoal, unha entidade absolutamente independente do resto de dereitos.

Non entanto, tal e como se constatou durante as entrevistas os grupos de discusión realizados, e en materia de protección de datos donde acontece o maior número de situacións desfavorables para a protección dos dereitos dos usuarios, xa que as redes sociais fundamentan tódolos contidos nos perfís que os propios usuarios dan de alta e actualizan con asiduidade. Así, entre as **posibles situacións de risco para a protección de datos de carácter persoal**, e sen prexuízo das situacións citadas anteriormente pola súa relación co dereito a intimidade, encóntranse:

- Casos de phishing e pharming. Ambos fenómenos, moi explotados polos cibercriminosos para lograr a obtención de datos persoais dos usuarios de Internet, así como de datos de carácter sensible ou relativos a aspectos económicos (cartóns de crédito, PIN de usuarios, etcétera).
- Social Spammer e spam. O uso das redes sociais como plataformas para o envío de correos electrónicos non desexados.
- Indexación non autorizada por parte dos buscadores de Internet.
- Acceso ó perfil incontrolado. A maioría de redes sociais analizadas dispoñen dun perfil completo do usuario, ou polo menos de parte de éste, en formato público, de xeito que calquer usuario de Internet ou da rede social pode acceder a información de carácter persoal allea sen que o propietario dos datos teña que dar o seu consentimento expreso.
- Suplantación de identidade. Cada vez é mais frecuente que usuarios que nunca se rexistraron en redes sociais online, comprobren cómo no momento no que intentan acceder, a súa “identidade dixital” xa está sendo utilizada.
- Publicidade hipercontextualizada. Ésta aporta, a priori, unha vantaxe para os usuarios, xa que con ela evitan que se mostre durante a súa navegación contidos para eles irrelevantes ou ata ofensivos. Sen embargo, dende o punto de vista legal podería considerarse unha práctica ilegal, xa que para poder contextualizar a publicidade que se vai a mostrar a un usuario, teñense que examinar os seus datos e preferencias.
- A instalación e uso de “cookies” sen coñecemento do usuario. Outro posible risco relacionado coa participación do usuario na rede social radica na posibilidade de que o sitio web utilice cookies que permitan a plataforma coñecer cal e a actividade do usuario dentro da mesma. Mediante estas ferramentas, as redes sociais poden coñecer o lugar dende o que o usuario accede, o tempo de conexión, o dispositivo dende o que accede (fixo ou móvil), o sistema operativo utilizado, os sitios máis visitados dentro dunha páxina web, o número de clicks

realizados, e infinidade de datos respecto o desenvolvemento da vida do usuario dentro da rede.

Polo que respecta as medidas existentes en materia de protección de datos persoais para colectivos considerados especialmente vulnerables –menores e incapaces- cabe sinalar que, dende o punto de vista normativo, o Real Decreto 1720/2007 introduce unha importante especialidade no que respecta a prestación do consentimento por parte dos menores ó dispor que, para recabar os datos de calquer menor de 14 anos, é necesario contar co consentimento dos pais ou tutores.

Ademais, esta norma sinala de maneira expresa que para recabar o consentimento do menor debe utilizarse unha linguaxe sinxela e fácilmente comprensible para él, e que non se poida obter a partir deles información respecto ós seus familiares e achegados.

Protección da propiedade intelectual e industrial dos contidos

Estáse producindo un aumento no número de contidos protexidos polo dereito da propiedade intelectual que están sendo utilizados, compartidos e difundidos a través das redes sociais e sitios web colaborativos.

A protección céntrase, polo tanto, no **dereito que o autor ten sobre a súa creación literaria, artística ou científica**.

En España, a **Lei da Propiedade Intelectual** concede ós autores das obras dereitos en exclusiva sobre éstas, o que supón que calquer tratamento, reprodución, posta a disposición ou transmisión da obra deberá ser realizada coa autorización dos titulares dos dereitos. Tanto a normativa nacional como a comunitaria parten dun grao elevado de restricción dos dereitos de explotación, de forma que ninguén pode explotar dereitos de propiedade intelectual sen autorización pola parte do autor.

Non entanto, dentro das posibles vulneracións de dereitos en materia da propiedade intelectual e industrial, e tal e como se extraíu das entrevistas e dos grupos de discusión para analizar os aspectos xurídicos, é necesario diferenciar entre aquelas situacións nas que son os propios usuarios os que poñen en entredito a integridade e dereitos de propiedade intelectual dos autores e aquelas nas que son as redes sociais as que, a través das súas condicións xerais, poñen en risco os dereitos da propiedade intelectual dos usuarios.

Ante estas situacións, as redes sociais, como medio da colaboración e loita contra a distribución non autorizada de contidos a través das súas plataformas, dispuxeron mecanismos automáticos para que os propios usuarios procedan a autorregulación dos contidos que desexen que existan na rede social. Para elo, permítese “denunciar” internamente contidos que non cumpran coas condicións de rexistro da plataforma ou

que atenten tanto contra os dereitos que ostentan os usuarios sobre as súas obras de propiedade intelectual, como contra os de terceiros.

Protección dos consumidores e usuarios

Teráanse en conta que unha das principais vantaxes que presenta este tipo de plataformas e a capacidade de obter beneficios económicos derivados da publicidade e das aplicacións internas desenvoladas polos propios usuarios da rede.

A facilidade coa que os usuarios poden anunciar ou ser receptores de anuncios de produtos e servizos é moi elevada se se compara co mundo físico, xa que xunto a sinxeleza coa que se poden comercializar produtos e servizos á distancia, as redes sociais contan cunha base de datos de usuarios (potenciais clientes), perfectamente segmentados por gustos e perfís, o que implica que as capacidades do éxito do procedemento comercial sexan moi altas.

Según se constatou a partires das entrevistas e os grupos de discusión realizados con usuarios e xuristas, o aumento da colaboración dos usuarios a hora de detectar e controlar o tipo de publicidade, así como os produtos e servizos comercializados a través da rede, permitiría unha autorregulación interna da plataforma dende o punto de vista comercial, que aumentaría o grao de seguridade dos usuarios.

Do mesmo modo, é esencial para un correcto desenvolamento da Sociedade da Información e polo tanto para que a venta de produtos e servizos a través de redes sociais sexa exitosa, que os potenciais clientes confíen plenamente no sitio web, para o que éste deberá garantir a tódolos potenciais clientes que observa e cumpre a normativa legal vixente, así como os requisitos tecnolóxicos necesarios.

III Propostas e recomendacións de actuación dirixidas ós axentes intervintes nas redes sociais

Tralo análise da información recabada durante a investigación cualitativa –redes sociais e plataformas colaborativas, servizos ISP ou provedores de acceso a Internet, fabricantes e provedores de servizos de seguridade informática, administracións e institucións públicas e usuarios e asociacións– fórmulanse unha serie de recomendacións ós diferentes axentes intervintes no proceso:

- **Dirixidas a industria**

Redes sociais e plataformas colaborativas: A proposta de recomendacións de carácter xeral dirixidas a este colectivo están enfocadas a adecuación dos seus servizos respecto da normativa europea e nacional, ó coñecemento das implicacións xurídico tecnolóxicas que conleva a realización de determinadas prácticas, a identificación do tipo de

ferramentas tecnolóxicas necesarias nos seus servizos, e a concienciación respecto da necesidade de incrementar as medidas de seguridade e protección dos usuarios.

Polo que respecta ás recomendacions específicas extraídas das entrevistas e dos grupos de discusión, cabe sinalar:

Recomendacions tecnolóxicas e de seguridade

1. Transparencia e facilidade do acceso a información
 - Resulta fundamental que este tipo de plataformas expoñan toda a información relativa os seus servizos de forma clara, de maneira que a linguaxe empregada nas súas condicións de uso e políticas de privacidade sexa absolutamente comprensible para calquer tipo de usuario.
 - É esencial que as redes sociais destaquen dentro das súas páxinas de inicio un apartado específico destinado a informar ós usuarios.
 - Recoméndase a creación de “microsites”⁵ con acceso directo dende a páxina principal da rede social, nos que se expoña información mediante “preguntas frecuentes” e contidos multimedia.
 - É esencial que as redes sociais manteñan a súa política de privacidade e condicións de uso sen cambios importantes e trascendentais para os usuarios.
2. Garantir ós usuarios o control absoluto do tratamento dos seus datos e información publicada na rede, poñendo ó seu dispor o maior número de ferramentas tecnolóxicas encamiñadas a facer efectivos os seus dereitos de forma automática, sinxela e rápida.
3. Establecer estándares de seguridade e privacidade, referidos a non indexación por defecto dos datos personais ou a especial protección dos datos sensibles.
4. Garantir a seguridade tecnolóxica da plataforma. Neste sentido, é vital a correcta elección por parte da plataforma dun prestador de servizos de Internet (Internet Service Provider o ISP) que conte cun elevado nivel de seguridade: servidores seguros, centros de respaldo e accesos seguros, entre outras medidas.
5. Eliminación da información despois dun tempo prudencial sen que o usuario entre na plataforma.

⁵ Pequenas páxinas web, con contidos específicos que dependen dunha principal.

6. Respetar os dereitos de acceso e cancelación.

Recomendacións en materia de formación e concenciación

1. Desenrolo interno de espazos web dedicados a poñer ó dispor dos usuarios o máximo e o máis claro posible nivel de información respecto ó tratamento de datos personais, os sistemas publicitarios empregados na plataforma, as situacións de risco as que se poden enfrentar, así como das implicacións que poden derivarse da publicación de contidos na rede social.
2. Posta ó dispor dos usuarios da información relativa as medidas de seguridade que a plataforma implementou para actuar en caso de que se produza a vulneración de algún dos seus dereitos.
3. Tendo en conta que a gran maioría de usuarios das redes sociais xeralistas son menores de idade, resulta fundamental que as redes sociais e plataformas colaborativas, xunto coas autoridades públicas, asociacións e organizacións cuxa finalidade sexa a protección deste tipo de colectivos, leven a cabo iniciativas conxuntas encamiñadas a fomentar a formación entre os menores e titores respecto a seguridade dos usuarios, investigando as posibilidades tecnolóxicas existentes para lograr a identificación da idade dos usuarios do servizo.
4. Programas de voluntariado dentro da empresa para colaborar coas institucións escolares e centros de formación co fin de difundir a importancia da seguridade, así como para informar sobre as principais recomendacións a ter en conta no uso deste tipo de servizos.

Dirixidas a fabricantes e provedores de servizos de seguridade informática

Os fabricantes e provedores de seguridade deben ter en conta dous aspectos clave para lograr o máximo nivel de seguridade: a) a prevención do fraude online e b) a investigación e desenrolo en materia de seguridade tecnolóxica. Desta forma, recoméndase que fomenten no sector os seguintes aspectos:

1. Que as aplicacións comercializadas entre as redes sociais e plataformas colaborativas, así como entre os usuarios, fosen desenroladas, revisadas e avaliadas conforme os estándares de calidade e seguridade que garanten que a súa utilización é segura e respetuosa cos dereitos dos usuarios.
2. O fomento da interoperabilidade dos seus sistemas de seguridade.
3. A colaboración activa e directa coas Forzas e Corpos de Seguridade do Estado na investigación de novas situacións de risco para os usuarios.

4. A proactividade na detección de códigos maliciosos de programación que permitan buracos de seguridade nas plataformas, así como a elaboración de listados (Black Listed), nos que sexan incluídos tódolos nomes de dominio que contén con contidos non autorizados, ou no seu caso, que non superen os criterios de seguridade previamente establecidos.
5. O desenvolvemento de parches de seguridade e actualizacións.
6. O desenvolvemento de aplicacións remotas que permitan o control pleno por parte dos titulares dos contidos e das operacións realizadas polos menores a través de Internet.
7. O desenvolvemento de aplicacións que permitan as plataformas controlar a idade dos usuarios que intentan acceder ó servizo.
8. Incluír na descrición técnica dos produtos de software destinados ao tratamento de datos persoais a descrición técnica do nivel de seguridade, básico, medio ou alto que permitan alcanzar de acordo co Regulamento do desenvolvemento da LOPD.

Igualmente, recoméndase que os fabricantes de aplicacións software de seguridade, xunto coas administracións públicas competentes, fomenten o desenvolvemento das ferramentas encamiñadas a reducir a recepción de correos electrónicos non desexados (spam) a través das redes sociais e plataformas semellantes.

Dirixidas ós prestadores de servizos de acceso a Internet (ISP)

A proposta de recomendacións dirixidas a este colectivo inclúe:

1. A creación de plataformas de comunicación fidedigna e segura coas Forzas e Corpos de Seguridade do Estado, Ministerio Fiscal e Autoridades Xudiciais.
2. O apoio e asistencia plena as Forzas e Corpos de Seguridade do Estado.
3. Prestar información a tódolos usuarios e clientes directos sobre as medidas de seguridade que manteñen respecto ó servizo concreto.
4. Atender inmediatamente as reclamacións de bloqueo de servizos cando se reciban por calquer método que deixe constancia da identidade do remitente e se identifique de forma clara e concisa o emisor do mesmo.

Dirixidas as administracións e institucións públicas

Como garantes dos dereitos dos cidadáns as recomendacións que se propoñen as autoridades catalóganse dende o:

Punto de vista normativo:

Polo que respecta a protección de datos pessoais, entre as propostas cabe citar:

- As autoridades competentes deben promover a elaboración de informes, recomendacións e dictámes públicos.
- Seguridade xurídica global: que se fomente o establecemento internacional, o menos ó nivel comunitario, dos principios normativos básicos.
- Deberán instrumentarse e reforzarse as sancións para aquelas plataformas ou usuarios que compartan ou obteñan información de forma ilegal.
- Recoméndase as autoridades traballar en favor dun dereito internacional homoxéneo en materia de protección de datos pessoais, honra, intimidade e propia imaxe.

Propiedade Intelectual:

- Fomentar, e no seu caso dispor como obligatorio, que este tipo de plataformas fagan públicas e destaquen con especial énfasis que ditos contidos pasarán a ser propiedade da plataforma.
- Recoméndase que as autoridades competentes promocionen, dende o punto de vista normativo, acordos directos entre a industria audiovisual e musical e as grandes plataformas de difusión de contidos.
- Recoméndase a obriga de todo prestador de servizos da Sociedade da Información a que dispoñan de medios automatizados, gratuitos, sinxelos e eficaces para que os titulares de obras de propiedade intelectual poidan denunciar a retirada de contidos.
- Que se garante a xusta remuneración dos titulares dos dereitos.

Consumidores e Usuarios

- Recoméndase ó lexislador que se delimite claramente que autoridade é competente para atender as reclamacións dos consumidores ou usuarios.
- Promover mecanismos eficaces e eficientes respecto a posibilidade de bloquear o acceso a plataforma online.

Punto de vista executivo e administrativo:

- Formación específica en Dereito Tecnolóxico destinada a xuíces, maxistrados, forenses, fiscais e secretarios xudiciais.
- Dotar ás brigadas tecnolóxicas das Forzas e Corpos de seguridade do Estado, tanto estatais e autonómicas, como internacionais, de ferramentas tecnolóxicas que lles permitan investigar, manter a cadea de custodia das probas electrónicas e bloquear situacións que pudesen ser susceptibles de delitos e/ou perxudiciais para os usuarios de redes sociais.
- Desenrolo e articulación de procedementos xudiciais rápidos.

Punto de vista formativo e divulgativo:

- Realizar campañas de concienciación sobre os riscos da difusión de datos personais nas redes sociais.
- Levar a cabo xornadas de formación e programas de difusión relativos a seguridade.

Incluir nos plans oficiais de estudo o coñecemento de aspectos relacionados coa seguridade das tecnoloxías da información e a protección de datos personais fomentando a formación específica neste campo.

- Levar a cabo accións de sensibilización e fomento da seguridade en Internet a través dos propios medios 2.0.

Dirixidas ós usuarios e asociacións

A proposta de recomendacións dirixidas a este colectivo fórmase coa intención de que poidan coñecer os beneficios que este tipo de servizos online poden aportar as súas vidas, pero sen descoidar o coñecemento sobre a existencia de situacións desfavorables, que poidan ser facilmente evitables.

Éstas propostas estrutúranse atendendo a protección de datos personais, honra, intimidade e propia imaxe, a propiedade intelectual, recomendacións de carácter tecnolóxico e de seguridade e a protección dos menores.

1. Recoméndase a tódolos usuarios recurrir o uso de pseudónimos ou nicks persoais cos que operan a través de Internet, permitíndolles dispor dunha auténtica “identidade dixital”, que non poña en entredito a seguridade da súa vida persoal e profesional. Desta forma, unicamente será coñecido polo seu círculo de contactos que coñecen o nick que emprega en Internet.

2. Recoméndase ós usuarios ter especial coidado a hora de publicar contidos audiovisuais e gráficos nos seus perfís, dado que neste caso poden estar poñendo en risco a privacidade e intimidade de persoas do seu entorno.
3. Recoméndase revisar e ler, tanto no momento previo ó rexistro de usuario, como posteriormente, as condicións xerais de uso e a política de privacidade que a plataforma pon a súa disposición nos seus sitios web.
4. Recoméndase configurar adecuadamente o grado de privacidade do perfil de usuario na rede social, de tal forma que éste non sexa completamente público, senon que únicamente teñan acceso a información publicada no perfil aquelas persoas que fosen catalogadas como “amigos” ou “contactos directos” previamente polo usuario.
5. Recoméndase aceptar como contacto únicamente a aquelas persoas coñecidas ou coas que mantén algunha relación previa, non aceptando de forma compulsiva tódalas solicitudes de contacto que recibe e investigando sempre que fose posible e necesario, quen e a persoa que solicita o seu contacto a través da rede social.
6. Recoméndase non publicar no perfil de usuario información de contacto físico, que permita a calquer persoa coñecer dónde vive, dónde traballa ou estuda diariamente ou os lugares de ocio que adoita frecuentar.
7. Ós usuarios de ferramentas de microblogging⁶ recoméndase ter especial coidado respecto a publicación de información relativa ós lugares no que se encontra en todo momento.
8. Recoméndase utilizar e publicar únicamente contidos respecto os que se conte cos dereitos de propiedade intelectual suficientes. No caso contrario, o usuario estará cometendo un ilícito civil protexible por parte dos tribunales nacionais.
9. Recoméndase os usuarios empregar diferentes nomes de usuario e contrasinais para entrar nas distintas redes sociais das que sexa membro.
10. Recoméndase utilizar contrasinais cunha extensión mínima de 8 caracteres, alfanuméricos e con uso de maiúsculas e minúsculas.
11. Recoméndase a tódolos usuarios dispor nos seus equipos de software antivirus instalado e debidamente actualizado.

⁶ Este tipo de plataformas basean o seu servizo na actualización constante dos perfís de usuarios. Máis información: Capítulo 3 deste Estudo.

12. Os menores non deberán revelar datos pessoais excesivos. Nunca deberán suministrar os datos a descoñecidos.
13. Débese ler toda a información concernente a páxina web. Nela explícase quenes son os titulares da mesma e a finalidade para a que se solicitan os datos.
14. Se o usuario é menor de catorce anos, necesítase tamén o consentimento dos pais ou titores. Nestes casos, sempre que se soliciten datos por parte dunha rede social debe preguntarse ós pais ou titores para ver si eles aproban a suscripción ou non.
15. Non deben comunicarse a terceiros os nomes de usuario e contrasinais, nin compartilos entre amigos ou compañeiros de clase. Estos datos son privados e non deben ser comunicados a terceiros e/ou descoñecidos.
16. Sempre que se teña calquer dúbida respecto a algunha situación que derive do uso das redes sociais e ferramentas colaborativas, debe preguntarse ós pais ou titores.
17. Débese manter o ordenador nunha zoa común da casa.
18. Débense establecer regras sobre o uso de Internet na casa.
19. Os pais deben coñecer o funcionamento e as posibilidades deste tipo de plataformas, tanto positivas como negativas.
20. Activar o control parental e as ferramentas de control da plataforma, así como establecer o correo do pai ou titor como correo de contacto secundario.
21. Asegurarse de que os controis de verificación da idade están implementados.
22. Asegurar a correcta instalación do bloqueador de contidos.
23. Concienciar e informar ós menores sobre aspectos relativos a seguridade.
24. Explicar ós menores que nunca deben quedar con persoas que coñeceran no mundo online e que si o fan debe ser sempre en compañía dos seus pais ou titores.
25. Asegurarse de que os menores coñecen os riscos e implicacións de aloxar contidos como vídeos e fotografías, así como o uso de cámaras web a través das redes sociais.
26. Controlar o perfil de usuario do menor.

27. Asegurarse de que o menor só accede ás páxinas recomendadas para a súa idade.

28. Asegurarse de que os menores non utilizan o seu nome completo



<http://www.inteco.es>

<http://www.agpd.es>

<http://observatorio.inteco.es>