

Destaquem... Facebook *tothom* modifica la gestió de la privacitat



En el número de setembre del +KDades, es va destacar l'avís, en forma d'últimàtum, que havia rebut Facebook de l'autoritat canadenca de protecció de dades. El 9 de desembre passat, Facebook va modificar la gestió de les opcions de privacitat. Podria semblar que els canvis anirien en la línia de restringir l'accés a la informació que s'aboca en aquest servei de xarxa social. Doncs res més lluny de la realitat: el canvi afavoreix encara més la difusió de la informació; això sí, donant més opcions per controlar la privacitat.

D'entrada, si llegim la guia sobre la privacitat a Facebook (per cert, si utilitzem el català com a idioma a Facebook, aquesta guia està en anglès), s'aconsella que **tothom** (la negreta també és a la guia) pugui accedir a la informació que permeti de localitzar-nos de la manera més senzilla, com ara: "datos básicos como la descripción del apartado "Acerca de mí", tus familiares y relaciones personales, la información laboral y educativa y los sitios web, así como el contenido que publicas, como los álbumes de fotos y las actualizaciones de estado". Ens recorden que la informació que pugui veure **tothom** és accessible a qualsevol internauta.

Evidentment, aquesta gestió de la privacitat de Facebook no segueix l'orientació del *privacy by default*, ja que d'entrada gairebé totes les informacions són accessibles per a **tothom**, incloses les de les aplicacions disponibles per defecte (a excepció de fotografies i vídeos, que estan restringides als amics dels nostres amics, que és el segon nivell de privacitat). Únicament algunes dades de contacte estan limitades per defecte als "meus amics", que és el tercer nivell estàndard de privacitat que preveu Facebook.

Cada vegada que introduïm informació podem decidir el grau de privacitat que volem, fins i tot en l'àmbit d'usuari o de grups d'usuaris, que seria el nivell personalitzat de privacitat. Ara bé, recordem que en la majoria de casos, per defecte, l'opció de privacitat serà **tothom**.

Esther Mitjans
Directora de l'Agència Catalana de Protecció de Dades

Parlem... del control d'indexació de continguts a Internet

En aquest document, identificarem quines són les vies disponibles per controlar la indexació de continguts que realitzen els cercadors a Internet de les pàgines o els llocs web, amb una especial referència a les dades de caràcter personal.

Les mesures que es poden adoptar per controlar o limitar l'esmentada indexació són fonamentalment de caràcter tècnic, tot i que també hi ha polítiques de tractament de dades que poden afavorir un major control dels responsables de les pàgines/dades a Internet. Aquest article, però, no revisa amb profunditat aquestes polítiques, basades en condicions d'ús, avisos legals o, fins i tot, legislació que s'hi refereix.

La necessitat d'aquesta anàlisi té l'origen en la problemàtica generada per la indexació de dades personals que fan cercadors com Google, en especial quan es tracta de publicacions oficials disponibles a Internet. La indexació d'aquests documents, que contenen dades de caràcter personal relacionades, en moltes ocasions, amb infraccions o resolucions judicials, poden generar perjudicis a les persones involucrades.

Tot i que el punt de partida és molt concret, la qüestió es pot abordar amb un abast més genèric, ja que inclouria qualsevol publicació de dades de caràcter personal a Internet, per exemple les que apareixen publicades als serveis de xarxes socials.

Continguts

Destaquem...	1
Parlem de...	1
Incidents de seguretat relacionats amb la protecció de dades	2
On anar...	2
Tecnologia i protecció de dades	2
Butlletí revisió vulnerabilitats	3
Enllacem amb...	3
Secció responsables de seguretat	3
Control d'indexació de continguts a Internet	4

+info

Incidents de seguretat relacionats amb la protecció de dades

Detenen una parella que robava dades amb el troià Zeus (novembre 2009)

La Policia Metropolitana de Londres ha detingut dues persones acusades de haver robat dades bancàries d'internautes utilitzant el troià Zeus, també conegut com a Zbot.

Es creu que utilitzaven aquest programa per infectar els usuaris d'Internet i recol·lectar-ne les dades personals i bancàries, per enviar-les als delinqüents. Els delinqüents van aconseguir milions de números de targetes de crèdit i contrasenyes per entrar a comptes de banca en línia, adreces de correu electrònic i xarxes socials.

Aquest troià va ser creat al 2007 i s'ha anat tornant més nociu amb el temps, ja que s'hi han afegit modes per evitar que els programes de seguretat el detectin i se n'han creat multitud de variants. L'any 2008, l'empresa de seguretat Symantec va detectar prop de 90.000 variants del troià Zeus.

Font: viruslist.com

Prop de 4.000 comptes d'usuaris de la xarxa social Tuenti han estat compromeses (desembre 2009)

Prop de 4.000 comptes d'usuaris actius de Tuenti s'han publicat a pàgines d'Internet.

Segons assenyala el responsable de comunicació de la xarxa social, Ícaro Moyano, aquest problema no ha estat originat per un forat de seguretat de Tuenti, sinó per un atac de pesca informàtica (*phising*) que s'ha fet des d'un lloc extern. Moyano destaca que des de la xarxa social s'ha actuat ràpidament i, en poc temps, s'ha aconseguit protegir els comptes i tancar les pàgines fraudulentes que recopilaven i distribuïen les contrasenyes. No obstant això, s'aconsella als usuaris afectats que comparteixen la contrasenya a Tuenti amb la del seu correu personal que en modifiquin aquesta última, per tal d'evitar problemes.

Tuenti té previst posar-se en contacte amb els afectats perquè puguin canviar les seves contrasenyes, que van ser inicialitzades com a mesura d'urgència.

Font: ITespresso.es

On anar...

Congressos i esdeveniments

Australasian Information Security Conferend (AISC 2010)

Del 18 al 21 de gener de 2010. Brisbane (Austràlia)
<http://conf.isi.qut.edu.au/aisc10/>

2010 Security Workshop Introduction

Del 20 al 22 de gener de 2010. Sophia Antipolis (França)
http://www.etsi.org/WebSite/NewsandEvents/2010SECURITYWS/2010_SECURITYWORKSHOP_HOME.aspx

Fourteenth International Conference Financial Cryptography and Data Security

Del 25 al 28 de gener de 2010. La Laguna, Tenerife
<http://fc10.ifca.ai/>

SPCC 2010 – Workshop on Security and Privacy in Cloud Computing

29 de gener de 2010. Brussel·les (Bèlgica)
<http://www.spcc2010.info/>

The 2010 Workshop on RFID Security (RFIDsec'10 Asia)

22 i 23 de febrer de 2010. Singapur
<http://rfidsec2010.i2r.a-star.edu.sg/>

Tecnologia i protecció de dades

Facebook és el paradís per als lladres d'identitat

El 46% dels usuaris d'aquesta xarxa social no va amb compte a preservar la intimitat de les seves dades personals. Sophos adverteix que gairebé la meitat dels usuaris de Facebook no es resisteix a l'hora de oferir informació personal a desconeguts.

Per dur a terme l'estudi esmentat, Sophos ha creat dos usuaris ficticis amb noms basats en anagrames de les paraules *false identity* i *stolen identity*, que han enviat 100 peticions d'amistat a usuaris triats a l'atzar i corresponents al seu grup d'edat. El primer d'aquests usuaris és una noia de 21 anys i el segon, una senyora de 56.

El 89% de les sol·licituds enviades al grup de 21 anys i el 57% de les enviades al grup de 56 van acceptar la sol·licitud d'amistat, sense fer cap pregunta. La majoria d'aquests usuaris van donar informació, com ara l'adreça de correu electrònic o la data de naixement.

<http://www.diarioti.com/gate/n.php?id=25330>

Seguretat de dades d'Oracle

El dia 3 de desembre, Oracle va organitzar un seminari web per donar a conèixer els seus productes vinculats a la protecció i la seguretat de les dades.

Data Vault

Protegeix les dades d'una base de dades, per tal que els administradors no hi tinguin accés; protegeix la base de dades contra intrusos i canvis i facilita la separació de tasques. Es pot fer un control d'usuaris amb privilegis i també aplicar polítiques de seguretat.

Label Security

Fa un control d'accés basat en la sensibilitat de les dades i permet bloquejar una taula a nivell de registre. Les etiquetes que es poden crear per a la classificació de la informació són *Top Secret*, *Secret* i *Confidencial*; un cop creades les etiquetes, s'assigna a cada registre l'etiqueta que li correspongui.

Audit Vault

És un producte pensat sobretot per a quan hi ha diversos servidors de base de dades, encara que siguin d'altres proveïdors, i té com a objectiu principal l'anàlisi de les dades, per assegurar-ne la utilització correcta i per detectar anomalies i intrusos. En tenir un dipòsit únic i dedicat, l'impacte en l'entorn de producció és mínim.

Advance Security

Garanteix la seguretat a les connexions entre l'empresa i els clients o proveïdors. Permet xifrar a nivell de columna les dades de la base de dades. En resum, xifra parts de la base de dades i les seves comunicacions.

Secure Backup

Protegeix dades crítiques i les codifica, abans que s'eliminin de la base de dades. Permet fer còpies de seguretat amb més rapidesa. Respecte de les còpies de seguretat, xifra el resultat de la còpia de tal manera que si aquesta còpia s'intenta recuperar en un altre servidor no es pot llegir.

Data Masking

Anonimitza les dades de l'entorn de producció a la base de dades de l'entorn de test, mantenint-ne el tipus i el format, i canvia les dades per altres de molt semblants a les reals; té una llibreria de formats per poder fer aquesta anonimització. De forma automàtica, aquest producte garanteix la integritat referencial de les dades. El principal avantatge d'aquest producte és que permet compartir dades de producció de forma segura.

Butlletí revisió vulnerabilitats

Frau per Nadal

És ben sabut que els delinqüents aprofiten qualsevol esdeveniment d'una certa rellevància per, mitjançant tècniques d'enginyeria social¹, intentar enganyar els usuaris. Les dates nadalenes, amb l'anar i venir de postals de felicitació electrònica i l'ús intensiu de les compres en línia, suposen una major exposició al frau.

En arribar aquest període, no és estrany trobar campanyes fraudulentament a través del correu electrònic, que busquen infectar els ordinadors dels internautes. Amb aquesta finalitat, són molt recurrents les postals nadalenes que ens animen a seguir un enllaç per poder descarregar la felicitació que, naturalment, és algun tipus de programa maliciós (*malware*). En d'altres ocasions, l'enllaç porta a pàgines que suplanten serveis de correu o xarxes socials, per capturar les nostres contrasenyes.

Tampoc no hi pot faltar el PowerPoint manipulat, que intenta aprofitar les vulnerabilitats del programa per comprometre l'equip; vulnerabilitats ja corregides però que, per desconeixement dels usuaris pel que fa a la seva criticitat, segueixen sense solucionar-se amb els pedaços corresponents.

Els que hem esmentat són els més utilitzats, però els hams per enganyar els usuaris evolucionen constantment. L'any passat, per exemple, un dels més nous va ser el frau de la loteria de Nadal². I aquest any, de moment, la versió nadalena de Koobface³ s'endu la palma.

En qualsevol cas, l'objectiu d'aquests fraus és clar: d'una banda, capturar credencials d'accés a serveis de banca, comerç, correu i xarxes socials; de l'altra, controlar nombrosos ordinadors amb els quals constituir una xarxa *zombi* que desenvolupi altres activitats fraudulentament.

Cal, per tant, tenir certes precaucions a l'hora d'utilitzar el comerç en línia. La primera és bàsica: fer les compres des d'un ordinador segur. La segona passaria per comprovar que la pàgina és fiable, és a dir, verificar que es tracta d'un lloc legítim i, en cas que sigui un portal nou, assegurar-se que és una entitat de garantia.

Amb aquestes recomanacions i aplicant el sentit comú, podem gaudir d'unes celebracions tranquil·les, almenys pel que fa a la privacitat i seguretat del nostre equip!

Font: INTECO

¹ L'enginyeria social és l'eina més utilitzada per dur a terme tota mena d'estafes i fraus sobre els usuaris més confiats, a través de l'engany. Consisteix a utilitzar un reclam per atraure l'atenció de l'usuari i aconseguir que actuï de la forma desitjada, per exemple convencent-lo de la necessitat que reenvii un correu a la seva llista d'adreces, que obri un arxiu que acaba de rebre i que conté un codi maliciós o que proporcioni els seus codis i les seves claus bancàries a una determinada pàgina web.

² Onada de correus fraudulents que aprofiten el sorteig de la Loteria de Nadal per dotar de major credibilitat el missatge. Els estafadors envien multitud de correus als comptes de correu electrònic, en què anuncien al receptor un premi concedit per una determinada entitat bancària i en faciliten un enllaç, en el qual l'usuari, per accedir al cobrament del suposat premi, ha d'introduir les seves credencials de banca en línia o el número de la targeta de crèdit.

³ El mètode d'infecció utilitza l'enginyeria social aplicada a les xarxes socials. En aquest cas, els falsos vídeos als quals s'accedeix si se segueix l'enllaç, publicat per algun dels nostres amics de Facebook, està infectat.

Enllacem amb...

http://europa.eu/legislation_summaries/information_society/index_es.htm

L'enllaç que hem triat aquest mes de no és un lloc web, sinó una part específica de la pàgina oficial de la Unió Europea <http://europa.eu>. Concretament, l'apartat d'aquest lloc web que recull una síntesi de legislació en matèria de societat de la informació.

És una pàgina de gran utilitat, perquè recull documents de diferents tipologies, orientats ja sigui a l'harmonització del marc regulador de les telecomunicacions o a garantir la protecció de les dades de caràcter personal, la seguretat a les xarxes i la lluita contra les activitats il·lícites.

D'una manera molt simple, en forma de llista organitzada per temes, podem accedir als documents més rellevants en matèria de societat de la informació. Així, posa a l'abast un gruix important de documentació relacionada amb: l'enfocament comunitari de la societat de la informació, el marc jurídic general, l'estratègia i2010 i els plans eEurope, Internet i activitats en línia, seguretat de la informació, protecció de dades, drets d'autor, comerç electrònic, radiofreqüències, sistemes de pagament, etc.

Secció responsables de seguretat

Nom i cognoms
Rubén Cortés Domingo

Lloc que ocupa
Cap de l'Àrea d'Operacions i Sistemes

Entitat
Consorci AOC

Aquesta àrea s'ocupa de gestionar els sistemes d'informació del Consorci AOC i de donar servei d'atenció als nostres usuaris.

Desenvolupes en exclusiva l'activitat de responsable de seguretat?

No, la tasca de responsable de seguretat és una més de les responsabilitats dins l'Àrea.

Quina és la principal dificultat que trobes per desenvolupar les funcions de responsable de seguretat?

La dificultat bàsica és la de poder gestionar, des de l'àmbit d'operacions i sistemes, totes aquelles aplicacions informàtiques que s'instal·len en els servidors del Consorci, tenint

en compte que han de complir els requeriments de seguretat i protecció de dades.

En relació a la protecció de dades, quina responsabilitat et requereix més dedicació?

Mantenir al dia les infraestructures i gestionar els accessos a la informació sensible en relació a la protecció de dades.

Mantens contacte amb l'APDCAT per resoldre qüestions o plantejar dubtes que et puguin sorgir en el dia a dia?

No directament; tenim contactes directes amb diferents empreses del sector de les TIC i de l'àmbit jurídic, però les consultes a les agències de protecció de dades es fan des de l'àrea d'assessoria jurídica.

Control de la indexació de continguts a Internet

Ramon Miralles. Coordinador d'Auditoria i Seguretat de la Informació
Agència Catalana de Protecció de Dades

Punt de partida

Els cercadors d'Internet constitueixen una de les eines més potents i utilitzades a Internet. Són essencials per a l'accés a la informació publicada a la xarxa, així com per al mateix desenvolupament i creixement d'Internet, i representen un enorme estalvi de temps per als usuaris. La quantitat d'informació disponible a Internet seria difícilment accessible, si no fos per aquestes eines que faciliten, mitjançant recerques molts simples (comunament basades en paraules), la recerca a tots els llocs web.

Pel nivell de profunditat que ens interessa tractar en aquest article podem dir que, com a principi general, l'activitat dels cercadors o indexadors es pot dividir en tres grans funcions:

- Localització de llocs webs (URL o adreces de servidors web) i indexació dels seus continguts. Processen la informació que troben, simplificant podríem dir que paraula a paraula, i la inclouen en una base de dades amb la referència del lloc web on es troba.
- Emmagatzematge, en alguns casos, de la pàgina indexada en els seus mateixos sistemes, que és el que s'anomena memòria cau (*cache*).
- I, per últim, posen a disposició dels usuaris una interfície de cerca, que permet introduir una o diverses paraules per fer la consulta. Així, s'obté com a resultat la llista de totes les pàgines que contenen les paraules utilitzades a la cerca i, a partir de la llista, es pot accedir a la pàgina en qüestió (la llista conté, habitualment, un títol i unes quantes línies de resum de la pàgina).

El mecanisme i la política d'indexació impliquen que, amb caràcter general, s'indexa tot el contingut que es troba al servidor web, sempre que el seu contingut sigui un fitxer individual (poden ser de diferents formats: html, pdf, rtf, word, excel, powerpoint, etc.).

La indexació també pot afectar imatges. En aquest cas, s'utilitzen com a criteri d'indexació tant el títol de la imatge que hagi introduït l'administrador de contingut del lloc web com altres marques en les pàgines web, que vinculen descripcions textuales a imatges.

Cercadors i dades personals

Segons el mecanisme descrit, el que s'anomena robot d'indexació no distingeix els tipus

d'informació que està tractant, ja que a efectes del robot es tracta de paraules que no vénen qualificades o tipificades. Per tant, no aplica cap tipus "d'intel·ligència" al procés d'indexació i, a priori, no sap si aquella paraula que està indexant és una dada personal o no; però és evident que un percentatge important de les paraules tractades (indexades) seran dades personals, i l'exemple més clar el tenim en els cognoms.

A partir d'un cognom, els cercadors permeten localitzar totes les pàgines web on apareix. Si el nom es combina amb un segon cognom i un nom de pila, es redueix el nombre de pàgines que coincideixen amb la recerca; així, amb successives recerques i afegint noves paraules (llocs geogràfics, dates, professions, etc.), es poden arribar a trobar les pàgines que contenen informació respecte d'una persona concreta, de manera que amb certa facilitat es pot obtenir una relació de tota la informació que se'n publica a Internet.

La cerca de dades personals mitjançant els cercadors és una pràctica absolutament implantada entre els usuaris d'Internet. Per exemple, aquest procés d'obtenció d'informació de caràcter personal, utilitzant el cercador Google, rep el nom de *googling* i l'utilitzen tant les empreses com particulars per obtenir informació de persones concretes.

Control d'indexació

Per minimitzar o controlar les amenaces que suposa l'activitat dels cercadors per a la privacitat, quant a les possibilitats de recerca que proporcionen als usuaris d'Internet, podem identificar 3 nivells d'actuació dels proveïdors d'informació a la xarxa. Cada nivell superior implica una major complexitat d'implantació tècnica i, en alguns casos, unes inversions econòmiques superiors:

- Nivell de protocol.** Tal i com ja s'ha exposat anteriorment, els cercadors utilitzen robots d'indexació, que són els elements de programari que analitzen l'estructura del lloc web (segueixen tots els enllaços que troben a partir d'una URL) i recullen i tracten la informació publicada, per a la seva posterior presentació mitjançant la interfície de cerca del buscador.

Per controlar l'activitat d'aquests robots quan accedeixen a un web, hi ha el "Robots Exclusion Protocol" i el "Robots META tag". Ambdós mecanismes permeten als administradors de la pàgina web indicar al robot d'indexació quines parts del lloc web no ha d'indexar, o fins i tot quines pàgines individuals no s'han d'indexar.

Cal tenir present que és un protocol que els cercadors poden decidir no utilitzar (ja que és

una convenció d'adopció voluntària) i, per tant, poden ignorar les instruccions d'accés per indexació contingudes al fitxers *robots.txt*. En aquest supòsit, l'opció seria impedir l'accés dels servidors del cercador en qüestió al nostre lloc web, és a dir, a nivell de limitació de trànsit IP. Però aquesta és una mesura que pot arribar a tenir efectes no desitjats (impedir que determinats usuaris puguin accedir a la nostra pàgina, per exemple) i amb una gestió de manteniment complexa, per la qual cosa se n'ha de reservar l'ús per a situacions extremes.

Els cercadors més utilitzats són respectuosos amb el que preveu el REP i, per tant, per tenir un alt control sobre la indexació externa n'hi hauria prou de procurar d'implementar-lo en el lloc web.

En el cas de cercadors que emmagatzemen també les pàgines que indexen, com es el cas de Google, el mateix cercador proporciona eines i informació sobre com evitar que les pàgines es guardin en memòria cau, de manera que s'obliga que l'accés sempre es faci a la pàgina original situada en el servidor que ha estat indexat.

Aquest tipus de solució té una implantació senzilla i de baix cost, està molt documentada i cercadors com Google proporcionen molta informació i eines específiques per controlar la profunditat i l'abast dels seus processos d'indexació de pàgines.

- b. **Nivell tecnològic.** Tal i com ja s'ha explicat a l'inici d'aquest document, els cercadors indexen fitxers en diferents tipus de formats, que s'han anat ampliant des dels inicis. Així doncs, una manera de limitar de forma considerable, o gairebé d'evitar, la indexació de continguts dels llocs web, és fer un canvi tecnològic: deixar d'utilitzar fitxers i passar a solucions tècniques basades en informació estructurada, és a dir, utilitzar bases de dades per accedir a la informació i per emmagatzemar-la.

Si la informació està continguda en bases de dades, els robots d'indexació no hi poden accedir si no coneixen la interfície d'interrogació (criteris de recerca), de manera que a la pràctica l'ús de bases de dades impedeix que els robots puguin accedir a la informació. En aquest cas, el contingut de la base de dades no es podria trobar mitjançant la interfície de cerca, ja que no hauria passat abans pel procés d'indexació.

Es poden produir algunes excepcions a aquest mecanisme quan el lloc web, tot i tenir continguda la informació en bases de dades, crea pàgines fixes (fitxers) amb informació extreta de la base de dades, a fi de reduir el temps de presentació de la informació (creació de pàgines en memòria cau, a partir de bases de dades). En aquest cas, si el robot del cercador troba la ruta on hi ha aquestes pàgines

d'informació, podrà arribar a indexar-les i a facilitar-ne l'accés mitjançant els seus serveis de consulta.

Atès que aquesta solució pot implicar un canvi tecnològic, s'han de valorar els costos que pot implicar, tant quant a llicenciament de programari com respecte de la necessitat d'una major capacitat de processament del maquinari i els desenvolupaments d'aplicació que puguin ser necessaris.

- c. **Nivell d'aplicació.** Si la informació es difon mitjançant bases de dades, es poden preveure altres actuacions que permetin un control més acurat sobre les dades personals que es publiquen:

- *En la fase d'edició de la informació:* si en el procés d'elaboració de la informació, els operadors que introdueixen les dades disposen de funcions d'aplicació orientades a marcar les dades de caràcter personal (metadades), després es poden dur a terme procediments de dissociació (fer anònimes les dades) o, si cal, generar fitxers estàtics amb la informació. D'aquelles parts de la informació que es volen protegir de la indexació, se'n poden generar imatges en comptes de text; això també complica tractaments posteriors de la informació per part de tercers que capturin les dades.
- *En les aplicacions de recerca del mateix sistema,* limitant els criteris d'accés per evitar consultes creuades o consultes massa àmplies. Aquestes solucions potencien la privacitat del sistema, sense limitar la capacitat d'accés a la informació, i fan més selectiva la recerca d'informació.
- *En la interfície de presentació de la informació:* totes aquestes mesures poden complementar-se amb mecanismes que evitin que es pugui obtenir de forma senzilla informació del sistema per al seu tractament posterior. Per exemple, evitar que s'arribin a generar fitxers sencers d'informació o bé obligant a una navegació que dificulti capturar la informació de forma massiva (ús de paginació), limitant el "copiar" i "enganxar", etc.

Aplicar mètode

Tot i que les solucions són eminentment tècniques, és convenient preveure de forma paral·lela uns certs procediments organitzatius i de mètode de treball, a fi que el control de la indexació impacti al mínim en les possibilitats de cerca de la informació que publiquem.

1. Analitzar la informació. Abans de prendre decisions sobre quines limitacions d'indexació cal implantar al sistema de publicació, cal analitzar en quin tipus de docu-

ments o registres poden aparèixer, o no, dades de caràcter personal.

2. Una vegada analitzada la informació, cal verificar si és possible identificar tècnicament els diferents tipus de documents i agrupar-los, per tal de definir els controls d'indexació.
3. Quan sigui possible agrupar la informació d'acord amb el nivell de contingut de dades de caràcter personal, es podran aplicar els nivells de control d'indexació identificats en aquest document. La implantació d'aquests nivells tècnics es fa de manera gradual.
4. Implantar unes determinades pràctiques d'edició de documents també pot afavorir una major protecció de les dades personals (per exemple, la no inclusió de noms i cognoms en els títols dels documents o fitxers que es publiquin).
5. Incloure condicions d'ús que limitin, almenys formalment, l'ús de la informació obtinguda al lloc web per a finalitats diferents de les que originen la publicació.

Documents de referència

Cal assenyalar que els diferents documents que fan referència a la problemàtica dels cercadors ho fan des de la preocupació que tenen les autoritats de control i, en general, les entitats preocupades per la privacitat, respecte de l'ús que pugin fer els administradors dels cercadors, de les dades de navegació i trànsit que emmagatzemen als efectes de prestar serveis de valor afegit als usuaris.

La majoria de documents que es relacionen a continuació tracten la problemàtica dels cercadors, principalment des d'aquesta perspectiva (tractament posterior dels *logs*, retenció de dades, oferiment de serveis en funció de les recerques, etc.).

Resolution on Privacy Protection and Search Engines

28th International Data Protection and Privacy Commissioners Conference. Londres, Regne Unit (2 i 3 de novembre de 2006)

Common Position on Privacy Protection and Search Engines

*Internacional Working Group on Data Protection and Telecommunications (grup de Berlín)
Primera adopció al 23th Meeting in Hong Kong SAR, China (15 d'abril de 1998) i revisada a la 39a edició del Meeting (6 i 7 d'abril, a Washington DC)*

Dictamen 3/99 relativo a la información del sector público y protección de datos personales

Grup de Protecció de les Persones pel que fa al Tractament de Dades Personals (grup de l'art. 29). De fet, aquest és el document que, en parts concretes, més s'apropa a les qüestions plantejades en aquest informe.

Privacidad en Internet: Enfoque comunitario integrado en la protección de datos en línea (21/11/2000)

Document de treball del Grup de Protecció de les Persones pel que fa al Tractament de Dades Personals (grup de l'art. 29). El capítol 5 d'aquest extens document és el que té alguns punts de connexió amb aquest informe.

Decisioni su ricorso. Reti telematiche e Internet – Motori di ricerca e provvedimenti di Autorità indipendente: le misure necessarie a garantire il c.d. (diritto all'oblio)

Garante per la protezione dei dati personali (Itàlia). El més important d'aquesta resolució del Garante és el concepte del dret a l'oblit, és a dir que tot i que les publicacions oficials tenen la funció de fer públics certs esdeveniments, aquests no tenen perquè estar disponibles "eternament" a Internet.