

PRIVACY



31

Madrid, 4, 5 y 6 de  
de noviembre 2009

conferencia internacional  
de autoridades de  
protección de datos y  
privacidad

## **Destaquem...** els estàndards internacionals sobre protecció de dades personals i privacitat

El passat 5 de novembre de 2009, la 31a Conferència Internacional d'Autoritats de Protecció de Dades i Privacitat va acollir favorablement una proposta conjunta per a la redacció d'estàndards internacionals per a la protecció de la privacitat, en relació amb el tractament de dades de caràcter personal.

Es tracta d'un document consensuat entre una cinquantena d'autoritats de protecció de dades i privacitat, dels cinc continents. Té, per tant, la vocació de ser un instrument global per solucionar el problema que globalment genera la protecció de dades de caràcter personal.

Com a resolució de la Conferència, té el valor de marcar el posicionament que a nivell internacional tenen les autoritats en la matèria, i s'ha de valorar com una primera aproximació amb un model global de protecció de la privacitat, especialment pel que fa al tractament automatitzat de dades personals.

L'Agència Catalana de Protecció de Dades ha participat en el grup de treball coordinat per l'Agència Espanyola de Protecció de Dades. L'APDCAT va organitzar la primera reunió d'aquest grup de treball, que es va celebrar al Parlament de Catalunya al mes de gener de 2009, i hi ha seguit col·laborant al llarg de les reunions que han donat com a resultat el document adoptat per la Conferència.

El document en castellà es pot consultar a:

[https://www.agpd.es/portalweb/canaldocumentacion/common/estandares\\_resolucion\\_madrid.pdf](https://www.agpd.es/portalweb/canaldocumentacion/common/estandares_resolucion_madrid.pdf)

## **Parlem...** d'anonimat i identificació a les xarxes socials

Els serveis de xarxes socials a Internet tenen una evident manca de mecanismes fiables d'identificació. El fet que l'arquitectura d'Internet no incorpori una capa d'autenticació obliga que les solucions d'identificació electrònica les aportin els mecanismes que s'afegeixen a la xarxa com a serveis.

En l'àmbit de les xarxes socials, aquesta situació afavoreix fenòmens com la suplantació d'identitats, l'adopció de personalitats múltiples, el frau, l'extorsió, la vexació, etc.

Hi ha, per tant, un risc evident per a les dades de caràcter personal, és a dir, per a dades que identifiquen o fan identificables les persones físiques, ja siguin dades dels mateixos usuaris de les xarxes (usuaris actius) o bé de persones que, sense ser-ne (usuaris passius), també veuen publicada la seva informació personal amb total desconeixement d'aquesta circumstància.

Abordarem aquesta qüestió des d'una perspectiva general, analitzant les situacions típiques de risc i la necessitat d'establir mecanismes segurs d'identificació electrònica que siguin respectuosos i compatibles amb la privacitat i l'anonimat a Internet.

### Continguts

Destaquem...	1
Parlem de...	1
Tecnologia i protecció de dades	2
Incidents de seguretat relacionats amb la protecció de dades	3
On anar...	3
Butlletí revisió vulnerabilitats	4
Secció responsables de seguretat	5
Enllacem amb...	5
Anonimat i identificació a les xarxes socials	6

**+info**

## Tecnologia i protecció de dades

### Protecció de dades: Symantec llança Data Loss Prevention 10

Symantec Corporation va anunciar el llançament de Data Loss Prevention 10, una plataforma oberta de prevenció de pèrdua de dades (DLP) que permetrà a les empreses aplicar el xifrat i administració de drets empresarials (ERM) i s'integrarà amb altres solucions de Symantec.

Actualment, gairebé tothom pot compartir, accedir i difondre un volum il·limitat d'informació, del qual les organitzacions han arribat a dependre. Al mateix temps, la feina s'ha convertit en una activitat cada vegada més mòbil: gràcies a dispositius mòbils intel·ligents, a l'accés a Internet d'alta velocitat i a l'emmagatzemament portàtil, l'oficina pot ser en qualsevol lloc.

Com a conseqüència, les organitzacions tenen cada cop més dificultats per evitar la pèrdua de dades sensibles i, per tant, convé canviar l'enfocament i assegurar les dades mateixes, en lloc de la xarxa que les conté. Aquesta és la finalitat de Symantec Data Loss Prevention, que ofereix una solució unificada per descobrir, controlar i protegir les dades confidencials allà on s'emmagatzemin, o bé on s'utilitzin.

El producte ofereix una cobertura completa de les dades confidencials en els punts d'accés, a la xarxa i als sistemes d'emmagatzematge, tant si els usuaris són dins com fora de la xarxa corporativa.

<http://www.diarioti.com/gate/n.php?id=24688>

[http://www.symantec.com/content/en/uk/enterprise/media/theme/dlp/b-dlp\\_overview.pdf](http://www.symantec.com/content/en/uk/enterprise/media/theme/dlp/b-dlp_overview.pdf)

### LOPDGEST Sector Públic, gestió del cicle d'adaptació a la LOPD

LOPDGEST ha desenvolupat l'eina LOPD-GEST Sector Públic, una solució per a la gestió del cicle complet d'adequació a la Llei orgànica de protecció de dades.

Les principals funcions d'aquesta eina són les següents:

- Gestió d'entitats (control i tractament de fitxers).
- Gestió de fitxers (control del cicle dels arxius, recomanacions i informes dels nivells de seguretat).
- Gestió de mesures de seguretat (definició i control de les mesures de seguretat implantades a l'entitat responsable del fitxer).
- Gestió d'informes (generació de documentació tècnica, organitzativa i legal personalitzada).

- Gestió d'incidències (control de les incidències produïdes a l'organització, relacionades amb la integritat de les dades).
- Control de suports (administració dels sistemes que continguin dades de caràcter personal).
- Gestió dels drets ARCO (generació d'informes i control de peticions ARCO).
- Gestió d'auditories (compliment de les mesures establertes pel reglament de desenvolupament de la LOPD).
- Control de registres d'accés a documents no automatitzats.
- Gestió de registres d'accés als edificis (controls d'accés a les diferents seus de l'entitat responsable del fitxer).
- Gestió d'usuaris i privilegis (sistemes d'autorització per accedir i gestionar les aplicacions i els seus nivells d'accés).
- Quadre de comandament (control i visualització de l'estat de cada entitat en relació a la protecció de les dades, amb opció de generar informes de grau de compliment).

Font: Revista TCN, núm. 445 (del 4 al 10 de novembre de 2009)  
[www.lopdgest.com](http://www.lopdgest.com)

### 50 països acorden mesures comunes per protegir la privacitat a Internet

Els responsables de protecció de dades de 50 països han acordat, per unanimitat, un conjunt d'estàndards internacionals per protegir la privacitat de les persones i el tractament que fan les empreses i els organismes públics de les seves dades personals. El document s'ha aprovat en finalitzar la 31 Conferència Internacional de la Protecció de Dades i Privacitat.

Es tracta d'una proposta de mínims sobre principis, regles i drets que han d'aplicar tots els països. El text, que es coneix com la "Resolució de Madrid", no és vinculant però sí que tindrà un valor de referència immediat, especialment en països que no tenen una legislació pròpia.

Entre els principis bàsics que han de regir la recollida i l'ús de les dades personals s'hi assenyalen els següents: lleialtat, legalitat, proporcionalitat, qualitat, transparència i responsabilitat.

També s'ha destacat la necessitat que hi hagi autoritats de supervisió nacionals i cooperació internacional i s'ha consagrat el dret d'accés, rectificació, cancel·lació i oposició.

A la declaració, també es té en compte el deure de seguretat i confidencialitat en el tractament de les dades de caràcter personal, així com els requisits que s'han de complir per a la recollida, conservació, utilització,

revelació o supressió legítimes de les dades personals.

En referència a les transferències internacionals de dades personals, el text recorda que només es poden fer entre països que ofereixin com a mínim el nivell de seguretat previst en el document.

[http://www.elperiodico.com/default.asp?idpublicacio\\_PK=46&idioma=CAS&idnoticia\\_PK=659537&idseccio\\_PK=1012](http://www.elperiodico.com/default.asp?idpublicacio_PK=46&idioma=CAS&idnoticia_PK=659537&idseccio_PK=1012)

[https://www.agpd.es/portalweb/revista\\_prensa/revista\\_prensa/2009/notas\\_prensa/common/nov/061109\\_estandares\\_internacionales.pdf](https://www.agpd.es/portalweb/revista_prensa/revista_prensa/2009/notas_prensa/common/nov/061109_estandares_internacionales.pdf)

### L'AEPD presenta una eina gratuïta en línia per autoavaluar el compliment de la LOPD

L'eina presentada per l'AEPD ofereix respostes als dubtes dels qui habitualment tracten dades personals. Es tracta d'un autotest basat en preguntes amb múltiples respostes que, un cop finalitzat, genera un informe amb indicacions personalitzades i recursos que orienten sobre el compliment de la LOPD.

El programa consta de dos nivells d'autoavaluació:

- El primer és un test bàsic per conèixer el nivell de compliment de la normativa de protecció de dades.
- El segon permet verificar fàcilment si es compleixen les mesures de seguretat exigibles en cada cas.

Per tant, aquest programa preveu dos perfils d'usuari diferents: per una banda, aquell usuari que per primera vegada entra en contacte amb la LOPD i busca saber si compleix amb la normativa; i per l'altra, l'usuari que en té un major coneixement i vol verificar el grau de compliment de les mesures de seguretat recollides en la normativa de protecció de dades.

El test és anònim i gratuït i estarà disponible, a partir del mes de desembre, a la pàgina web de l'AEPD.

[https://www.agpd.es/portalweb/revista\\_prensa/revista\\_prensa/2009/notas\\_prensa/common/no-051109\\_3\\_autotest\\_quia\\_proteccion\\_datos\\_empresas.pdf](https://www.agpd.es/portalweb/revista_prensa/revista_prensa/2009/notas_prensa/common/no-051109_3_autotest_quia_proteccion_datos_empresas.pdf)

## Incidents de seguretat relacionats amb la protecció de dades

### La FTC multa ChoicePoint per haver mantingut apagat el seu sistema de seguretat durant quatre mesos (octubre 2009)

La Comissió Federal de Comerç (FTC) dels EUA ha multat l'empresa de processament de dades ChoicePoint, per no haver protegit adequadament les dades confidencials dels seus clients.

La Comissió afirma que, l'abril de 2008, els sistemes de seguretat que protegien una base de dades de ChoicePoint es van desconectar sense que l'empresa se'n adonés i, fins quatre mesos després, no es va detectar l'error. En aquest temps, aprofitant que els sistemes de seguretat no funcionaven, un ciberdelinqüent va accedir a les bases de dades que processa aquesta empresa i va robar les dades personals de 13.750 persones.

La FTC va iniciar un procés penal contra l'empresa, amb l'acusació d'haver violat una ordre judicial de 2006 en què se li exigia la instal·lació d'un sistema de seguretat integral, per protegir les dades personals dels seus clients. Aquesta ordre es va dictar perquè el 2005 la manca de seguretat en els sistemes de l'empresa va permetre el robatori de les dades personals de 163.000 persones. En aquella ocasió, ChoicePoint va pagar una multa de 15 milions de dòlars.

Aquesta vegada, la FTC ha arribat a un acord amb ChoicePoint pel qual l'empresa haurà de pagar una multa de 275.000 dòlars per la seva negligència. A més, la Comissió ha exigint a l'empresa que, durant els propers dos anys, cada dos mesos es mantinguin reunions amb funcionaris del govern a fi de comprovar que els seus sistemes estan protegits adequadament.

Font: [www.viruslist.com](http://www.viruslist.com)

### Es perden les dades personals de 51.000 persones (octubre 2009)

Una cinta que contenia les dades personals de 51.000 clients de la companyia d'assegurances Zurich al Regne Unit s'ha perdut. S'ha confirmat que la cinta va desaparèixer durant un trasllat de rutina a un centre d'emmagatzematge de dades a Sud-àfrica, l'agost de 2008. Aquesta cinta també contenia dades de 550 persones de Sud-àfrica i Botswana.

La companyia ha escrit a tots els clients, informant-los que fins el moment no tenien proves que les seves dades s'haguessin destinat a usos fraudulents. Així mateix, a la carta s'explica als clients implicats quines precaucions tenen al seu abast.

La filial de Zurich al Regne Unit ha encarregat una investigació a la companyia d'auditoria KPMG, ha intensificat la seguretat al voltant del transport de les cintes i ha informat el

comissari d'Informació del Regne Unit.

Altres casos importants de pèrdua de dades que s'han produït al Regne Unit en els dos darrers anys han estat:

- Març de 2009: robatori d'un ordinador portàtil amb les dades de 109.000 persones, que tenien plans de pensions administrats pel Fons de Pensions del Regne Unit.

- Octubre de 2008: robatori d'un ordinador portàtil de l'empresa Deloitte, amb les dades sobre plans de pensions de més de 100.000 membres de la Xarxa de Ferrocarrils i de la Policia de Transport Britànica.

- Setembre de 2008: el Ministeri de Defensa va perdre dades de prop de 100.000 dels seus empleats.

- Novembre de 2007: la HM Revenue and Customs (HMRC) britànica va perdre dos discs d'ordinador amb la base de dades de prestacions per a fills, que abasta 7,25 milions de famílies i que incloïa les dades personals de 25 milions de persones.

Font: BBC News

### Detingudes dues persones per l'estafa de 2.690 euros mitjançant la banca electrònica (novembre 2009)

Agents de la Policia Nacional van detenir dues persones a Castelló, com a presumptes integrants d'una organització dedicada a les estafes a través d'Internet.

La investigació va començar a mitjans d'octubre d'aquest any, quan la Comissaria del Cos Nacional de Policia de Marbella va rebre la denúncia de dues transferències fraudulentes realitzades utilitzant banca electrònica.

Segons les fonts, aquests grups organitzats tenen una estructura complexa i inicien el frau aconseguint les claus secretes d'accés a la banca electrònica de les víctimes i accedint, així, als seus comptes bancaris. Un cop hi han accedit, n'obtenen els diners fent transferències als comptes destí, amb la col·laboració dels titulars d'aquests comptes.

Un dels detinguts va ser presumptament captat per aquests grups mitjançant un correu electrònic, que ofería una feina com a agent de logística. Habitualment, a partir d'aquí s'estableix una comunicació entre ambdues parts mitjançant el correu electrònic, en què l'organització indica al col·laborador que ha d'obrir un compte al seu nom i facilitar els codis d'accés i el codi IBAN. Més tard, ha d'acudir a l'entitat bancària, retirar els diners, cobrar la seva comissió i remetre la resta dels diners a l'estranger.

Font: ABC.es

## On anar...

### Congressos i esdeveniments

#### International Conference on Information Security and Cryptology (ICISC '09)

Del 2 al 4 de desembre de 2009. Seul (Corea)  
<http://www.icisc.org/>

#### First IEEE International Workshop on Information Forensics and Security

Del 6 al 9 de desembre de 2009. Londres (Gran Bretanya)  
<http://www.wifs09.org/>

#### 8th International Information and Telecommunication Technologies Symposium I2TS 2009

Del 9 a l'11 de desembre de 2009. Florianópolis, Santa Catarina State (Brasil)  
<http://www.i2ts.org/>

#### Iberic Web Application Security conference (IBWAS09)

10 i 11 de desembre de 2009. Escuela Universitaria de Ingeniería Técnica de Telecomunicación, UPM, Madrid  
<http://www.ibwas.com/>

#### The Second International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems (MPIIS-2009)

Del 10 al 12 de desembre de 2009. Jeju Island (Corea)  
<http://www.ftgr.org/MPIIS2009/>

#### The 8th International Conference on Cryptology and Network Security (CANS '09)

Del 12 al 14 de desembre de 2009. Kanazawa (Japó)  
<http://www.rcis.aist.go.jp/cans2009/>

#### The 2009 International Conference on Information and Communications Security

Del 14 al 17 de desembre de 2009. Beijing (Xina)  
<http://www.icics2009.org/>

#### International Conference on Information Systems Security (ICISS 2009)

Del 14 al 18 de desembre de 2009. Kolkata (Índia)  
<http://www.eecs.umich.edu/iciss09/>

#### International Conference on Ubiquitous Information Technologies & Applications (ICUT)

Del 20 al 22 de desembre. Fukoka (Japó)  
<http://www.icut2009.org/index.php>

#### Fourteenth International Conference Financial Cryptography and Data Security

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

# Butlletí revisió vulnerabilitats

## Últims virus amb més activitat

### Trojan.W32/Pfinet (Perillositat: 1 - Mínima)

Troia per a la plataforma Windows, que instal·la una eina d'intrusió (*rootkit*) en el sistema compromès i utilitza un disc virtual encriptat per emmagatzemar els seus components.

### Downloader.W32/Bredolab.Q @ Altres (Perillositat: 1 - Mínima)

Troia que descarrega altres codis maliciosos i intenta connectar-se a determinats llocs web.

### Trojan.W32/Mdrop.CHZ (Perillositat: 1 - Mínima)

Troia per a la plataforma Windows, que modifica el registre per carregar-se en iniciar el sistema.

### Trojan.W32/Agent.LNS (Perillositat: 1 - Mínima)

Troia per a la plataforma Windows, que té la capacitat d'accedir a Internet i comunicar-se amb servidors remots a través del protocol HTTP.

### Trojan.W32/Bredolab.H (Perillositat: 1 - Mínima)

Troia que intenta comunicar-se amb diversos servidors corresponents a diferents dominis d'Internet.

### Trojan.W32/VbInject.R (Perillositat: 1 - Mínima)

Troia que s'instal·la perquè s'executi en cada reinici.

### Downloader.W32/AutoRun.AIUN @ Altres (Perillositat: 1 - Mínima)

Troia que s'instal·la perquè s'executi en cada inici del sistema compromès i descarrega altres codis maliciosos.

### Trojan.W32/Inject.KQ (Perillositat: 1 - Mínima)

Troia que s'instal·la en el sistema compromès perquè s'executi en cada inici del sistema.

### Trojan.W32/Dloadr.CWR (Perillositat: 1 - Mínima)

Troia que s'instal·la perquè s'executi en cada reinici del sistema i que disposa de funcionalitat per a comunicar-se amb un servidor remot, mitjançant HTTP.

### Worm.W32/SillyFDC.BDD @ Altres (Perillositat: 1 - Mínima)

Cuc per a sistemes Windows, que es propaga a totes les unitats del sistema.

### Trojan.W32/Banker.EUW (Perillositat: 1 - Mínima)

Troia per a la plataforma Windows, que roba informació de l'usuari i l'envia a un servidor remot a través del protocol HTTP.

### Backdoor.W32/Agent.IQZZ @ MM Altres (Perillositat: 1 - Mínima)

Porta del darrere (*backdoor*) per a la plataforma Windows, que arriba al sistema com a adjunt d'un correu enviat de forma massiva, com a correu brossa (*spam*).

### Trojan.W32/Agent.LRA (Perillositat: 1 - Mínima)

Troia per a la plataforma Windows, que roba informació de l'equip infectat i l'envia a un servidor HTTP remot.

### Backdoor.W32/Clicker.EYE @ Altres (Perillositat: 1 - Mínima)

Porta del darrere (*backdoor*) per a plataforma Windows, que es connecta a Internet per descarregar més programari maliciós.

### SpyWare.W32/Zbot.CCS @ Altres (Perillositat: 1 - Mínima)

Programa espia per a la plataforma Windows, que cerca informació sensible a l'equip infectat, la recull, l'envia a un servidor remot i es connecta a altres llocs web per descarregar nous programes maliciosos. Acostuma a arribar al sistema com a adjunt d'un correu enviat de forma massiva, com a correu brossa (*spam*).



Virus más detectados (ult. 24h)	
Número	Incidències
<a href="#">Bredolab.AM</a>	(36,9%)
<a href="#">Netsky.Q</a>	(25,0%)
<a href="#">MIME Overflow</a>	(15,4%)
<a href="#">Netsky.P</a>	(12,3%)
<a href="#">Zbot.P</a>	(6,1%)
<a href="#">Zbot.ACSP</a>	(1,1%)
<a href="#">Cutwail.K</a>	(0,5%)
Muestra: 45.509.720 Detecciones: 72.064 (0,2%)	

Font: INTECO

## Secció responsables de seguretat

Nom i cognoms  
**Dolors Jiménez López**

Lloc que ocupa  
**Responsable de Qualitat dels Sistemes d'Informació  
Àrea TIC — Direcció de Serveis**

Des de quan  
**Novembre 2006**

Entitat  
**Departament d'Educació**

### En quin àmbit desenvolupes la teva activitat com a responsable de seguretat?

*El Departament d'Educació és l'òrgan de l'Administració de la Generalitat de Catalunya que té encomanada la proposta i l'execució de les directrius del Govern en matèria de política educativa en tots els àmbits de l'ensenyament, llevat de l'universitari.*

*El meu àmbit principal d'actuació, en aquests moments, se centra en impulsar i implantar el marc de referència que ha de permetre revisar i adequar les actuacions del Departament a les exigències marcades per la Llei orgànica de protecció de dades de caràcter personal i el Reglament que la desenvolupa.*

### Desenvolupes en exclusiva l'activitat de responsable de seguretat?

*Tot i que l'àmbit de la qualitat dels sistemes d'informació és conceptualment més ampli, la meua dedicació als aspectes de revisió i definició de mesures organitzatives i tècniques que proporcionen una efectiva protecció als tractaments de dades personals, i la revisió de les polítiques de seguretat associades als entorns de tractaments*

*de dades propis del Departament, centren de forma exclusiva la meua activitat.*

*Afortunadament, per al primer dels aspectes al Departament s'ha constituït el Grup de Treball LOPD. Aquest grup està format per un representant de cada unitat directiva i/o significativa del Departament. Es mantenen reunions de forma periòdica, en les quals es consensuen i coordinen propostes d'actuació en relació a la normativa vigent en matèria de protecció de dades.*

*En relació al segon aspecte, i conjuntament amb les àrees que tenen competències tecnològiques, s'avalua el nivell de compliment legal en matèria de seguretat i es revisen i planifiquen actuacions, per tal de sincronitzar els requeriments legals no assolits a les solucions tècniques disponibles.*

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

*El compliment de la garantia del dret a l'educació, i el seu caràcter de servei públic, obliga el Departament i els centres i serveis educatius a desenvolupar una activitat que implica el tractament sistemàtic de grans volums de dades de caràcter personal. El caràcter de les dades tractades, en molts casos especialment protegides, requereix condicions específiques en relació a les mesures de seguretat que en garanteixin la confidencialitat i una adequada formació i conscienciació del personal que intervé en alguna fase d'aquest tractament.*

*Un dels reptes que hem d'afrontar és l'abast territorial i la necessitat d'un treball conjunt amb centres i serveis educatius, per definir un marc de referència bàsic en matèria de protecció de dades que els permeti adaptar-se a les seves particularitats. És especialment en l'àmbit educatiu on la protecció de dades és una necessitat per al lliure desenvolupament de la personalitat, en una etapa de formació del caràcter i dels valors personals.*

*Un altre dels reptes pendents és la revisió sistemàtica i continuada dels procediments administratius en base a judicis de proporcionalitat, idoneïtat i necessitat, i l'efectiva incorporació dels aspectes de seguretat i privacitat en el moment del disseny de les solucions organitzatives i tecnològiques.*

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

*Donar suport i assessorament a les unitats que ho demanen. Quan les persones adquireixen consciència de les implicacions, afectacions i no compliments en què es pot incórrer pel fet de no haver-ho "pensat abans", demanen un assessorament i un suport continuat.*

*Per a una implantació efectiva i eficaç, l'assessorament personalitzat esdevé un element clau. Per sort, les bones pràctiques s'estenen ràpidament.*

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

*Sí, estem en contacte permanent amb l'APDCAT. Sempre n'hem obtingut una col·laboració excel·lent. Les vostres aportacions i reflexions sempre ens ajuden a interpretar correctament aquells aspectes que ens plantegen més dubtes.*

*Des d'aquí, aprofito per felicitar l'Agència per la iniciativa d'editar aquest butlletí, en el qual podem visualitzar les diferents alternatives i formes de treballar de la resta d'organismes.*

## Enllacem amb...

<http://www.csae.map.es/>

El Consell Superior d'Administració Electrònica és un òrgan col·legiat, actualment adscrit al Ministeri de la Presidència. S'encarrega de preparar, elaborar, desenvolupar i aplicar la política i estratègia del Govern de l'Estat en matèria de tecnologies de la informació, així com d'impulsar i implantar l'administració electrònica a l'Administració General de l'Estat.

A la seva pàgina hi trobarem informació sobre les seves funcions. A la secció que descriu les accions que duu a terme en les seves diferents àrees d'actuació, cal destacar la part dedicada a política de seguretat a les administracions públiques.

Hi ha, també, un apartat dedicat a informes estadístics en relació a l'ús de les TIC a les administracions públiques, així com tot un recull documental de molt interès en matèria de tecnologies de la informació i la seguretat.

Per la seva rellevància actual, resulta d'especial interès la secció dedicada al desenvolupament de l'administració electrònica així com la secció "Productes", on es poden consultar els projectes de Reial decret dels esquemes nacionals de seguretat i interoperabilitat, previstos a la Llei 11/2007 (versions de juliol de 2009).

## Anonimat i identificació a les xarxes socials

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

Voldria començar fent una reflexió de caràcter general sobre l'evolució de les tecnologies de la informació i la comunicació (TIC) en els últims 40 anys, per remarcar-ne un element clau: el fet que la millora tant de les infraestructures com dels dispositius, així com també del programari, ha estat sempre marcada per un apropament de les tecnologies a les persones.

A la sessió inaugural de la 31a Conferència Internacional d'Autoritats de Protecció de Dades i Privacitat, celebrada aquest mes de novembre a Madrid, Martin Cooper (considerat un dels inventors del telèfon mòbil, 1973) va posar l'exemple de l'evolució dels serveis de telefonia: partint d'una telefonia fixa que posava en comunicació llocs físics, units per un cable al costat del qual havien de romandre les persones, l'aparició del telèfon mòbil ha permès que el que es posa en comunicació siguin les persones, en portar a la butxaca el dispositiu que permet aquesta comunicació.

En general, un component importantíssim de l'evolució de les tecnologies ha estat la necessitat de facilitar la comunicació entre persones. Justament l'anomenat programari social (*software social*), sobre el qual es desenvolupen els serveis de xarxes socials, posa l'èmfasi en les capacitats identificades habitualment com a 3C:

- *comunicació*, ja que permet compartir informació
- *comunitat*, perquè les persones s'agrupen entorn a interessos comuns
- *cooperació*, és a dir fer activitats junts, de tots tipus: lúdiques, professionals, educatives, etc.

Un dels aspectes definitoris dels serveis de xarxes socials és que permet ampliar considerablement l'esfera de persones amb les quals podem estar en contacte, és a dir, de persones amb les quals podem compartir informació, formar comunitat i cooperar. Per tant, aparentment, les xarxes socials permeten relacionar-se amb un nombre elevat de persones que, d'una altra manera, no hauria estat possible conèixer; i dic *aparentment*, perquè un alt percentatge d'aquestes persones no sabem realment qui són, en el sentit que no vinculem el seu perfil a la xarxa social amb una identitat física.

És en aquest extens àmbit de relacions que habitualment es fa referència a la teoria del 6 graus de separació: si partim de la hipòtesi que tothom coneix 100 persones, en un màxim de 6 salts podríem estar en contacte amb tot el planeta (Frigyes Karinthy, escriptor hongarès, hi fa referència en una història curta, "Chains", al 1929).

Una vegada fetes aquestes reflexions introductòries, anem a concretar algunes qüestions, la primera de les quals relativa als sistemes d'identificació d'usuaris de les xarxes socials.

Cal tenir present que els requisits per ser usuari d'una xarxa social de propòsit general i gratuïta no passen, amb caràcter general, de la sol·licitud d'una adreça de correu electrònic. Aquest és un mecanisme d'identificació poc robust, i en relació a aquesta fragilitat voldria referir-me a un parell de conseqüències que se'n deriven.

La primera, la facilitat amb què es poden produir suplantacions, és a dir que una persona es faci passar per una

altra, usurpant-ne la identitat; o bé que algú s'inventi una identitat falsa, simulant que és una persona amb unes característiques d'edat, físiques, professionals, de gènere, etc. que no es corresponen amb la realitat.

La segona, molt més específica, és la que afecta els menors. Cada vegada més, l'edat d'incorporació a les xarxes socials es va reduint i ara mateix se situa entre els 9 i els 10 anys; això, malgrat que la majoria de les xarxes socials de propòsit general solen incloure, en les seves condicions d'ús, la clàusula que no s'accepten els menors de 13 o 14 anys com a usuaris.

La falta de control real sobre l'edat de qui es registra a la xarxa social no permet limitar els continguts a què tenen accés els menors, ni poden evitar que entrin en contacte amb adults. Òbviament, aquest fet suposa un risc real de relació amb persones malintencionades que, fent-se passar per menors, poden influir en el comportament d'aquest col·lectiu més vulnerable. En definitiva, els menors entren en contacte amb desconeguts en un context on poden compartir tot tipus d'informació.

Paral·lelament, cal reflexionar sobre dues qüestions més, que també giren al voltant de la identitat a les xarxes socials a Internet.

D'una banda, el fet que a Internet hi ha una certa sensació d'anonimat que, de fet, és d'una certa ingenuïtat en l'actual societat de la vigilància on hi ha fenòmens com:

- la videovigilància a la via pública i en espais privats
- el seguiment que es fa en els sistemes de pagament amb targetes financeres
- l'anàlisi del trànsit d'Internet en relació a la propietat intel·lectual
- la fi de les targetes anònimes de prepagament en telefonia mòbil
- les bases de dades d'ADN
- l'ús de tecnologies invisibles, com l'RFID
- la televisió IP
- i, per què no, el DNI electrònic

En definitiva, ens situem en un escenari on l'anonimat cada vegada té menys espai, almenys en relació a l'ús de les TIC i Internet.

Aquesta falsa sensació d'anonimat a les xarxes socials porta a una errònia percepció de control sobre la informació que s'hi publica, en el sentit de pensar que només aquells que ens coneixen saben qui som. Hi ha, per exemple, xarxes socials basades quasi exclusivament en la publicació de fotografies, com Fotolog o Flickr, en què el criteri d'accés als perfils és de tipus geogràfic; no obstant això, tot i que els usuaris no solen identificar-se en el cas de poblacions de pocs milers d'habitants és possible identificar persones físiques amb molta facilitat, només visualitzant les fotografies que han publicat al seu perfil.

La segona qüestió, potser derivada de la sensació d'anonimat esmentada, és la facilitat amb què es publiquen a la xarxa tot tipus de dades personals, ja sigui en format de text o en imatges (fotografia, vídeo, àudio, etc.). Parlem de

dades personals no només del titular del perfil, sinó també d'altres persones que ni tan sols són usuàries del servei però a les quals, especialment per mitjà de fotografies i vídeos, se'ls vulnera la privacitat i les dades personals. Tot aquest fenomen, en conjunt, s'ha començat a identificar amb el concepte d'*extimitat*.

Voldria tractar ara la qüestió de quines haurien de ser, almenys des d'una perspectiva garantista, les característiques bàsiques d'una identitat electrònica que ens aporti seguretat, robustesa, fiabilitat, garanties, etc.

Hi ha un primer element que a mi em sembla bàsic, que és abordar els problemes globals amb solucions globals ja que, en general, quan parlem de qüestions relacionades amb Internet les solucions locals o parcials no són eficaces.

La identitat electrònica, entesa com el mecanisme que permet conèixer, amb garanties, qui fa què a la xarxa, ha de ser "interoperable", és a dir que s'ha de poder utilitzar indistintament per a qualsevol dels agents públics i privats que operen a Internet prestant els seus serveis. I ha d'estar disponible o accessible des de qualsevol dels dispositius o canals que ens permeten accedir als serveis que ofereix la xarxa (telèfons mòbils, ordinadors portàtils, cibercafès, ordinador a casa, a l'oficina, etc.).

Un segon tret definitori de la identitat digital és que ha de ser respectuosa amb la privacitat, de manera que s'haurà de protegir d'una forma especial perquè aquesta identitat és la que realment ens donarà capacitat d'obrir a la xarxa. De fet, ja hi ha propostes, almenys en el context de la investigació en matèria de protecció de dades personals, sobre la necessitat de considerar la identitat electrònica com una dada de caràcter sensible (el prof. Yves Pouillet, per exemple, dóna suport a aquesta tesi). Per tant, aquesta informació s'ha de protegir d'una forma especial no només en el moment de crear-la, sinó també en utilitzar-la, sobretot pensant en l'ús que se li pot donar en un context d'ús intensiu dels mitjans electrònics.

Aquest respecte per la privacitat de les persones ha d'incloure la possibilitat de preservar la identitat en el món electrònic de la mateixa manera que ho fem en les relacions presencials (per exemple, en comprar el diari en un quiosc i pagar en efectiu). Per descomptat, sense perdre la possibilitat de estar perfectament identificats quan realment sigui necessari, cosa que implica aplicar criteris de proporcionalitat en l'ús dels mecanismes d'identificació.

I en aquest punt ens apareix el concepte d'*anonimat*. Més d'un autor sosté que el mecanisme que permet donar més garanties de privacitat és precisament l'anonimat, que no vol dir el desconeixement de qui ha fet què. Per exemple, l'ús de pseudònims en els certificats digitals porta implícit el fet que algú coneix quina és la identitat real de qui ha al darrere d'aquell pseudònim i per tant, en cas de necessitat motivada i proporcionada, serà possible saber qui ha fet què i en quin moment. Lògicament, en aquest punt la concurrència de terceres parts de confiança és un element clau per a la coherència del sistema.

La identificació de les persones a la xarxa és un autèntic repte, i més tenint en compte l'ús intensiu que s'està fent, i que es farà, dels mitjans electrònics. Per tant, si ho apliquem a les xarxes socials, se'ns planteja el repte de tenir perfectament identificat qui accedeix als serveis de xarxes socials, alhora que se'n preserva l'anonimat i es garanteix que té el control sobre la difusió de la informació personal que publica.

Per finalitzar, voldria apuntar el que poden ser unes certes prediccions de futur.

D'una banda, la possible configuració jurídica de l'anonimat con un dret, amb totes les seves conseqüències: dotar-lo de contingut, límits, excepcions, àmbit d'aplicació, condicions o requisits per exercir-lo, determinar-ne els subjectes titulars, els mecanismes de tutela o protecció, etc.

I d'una altra banda, el fet que en un futur qui ens proporciona la identitat digital siguin els proveïdors d'accés a la xarxa. No hem d'oblidar que ells són els qui tenen realment la capacitat de donar-nos accés o no a la xarxa i els que saben tot el que hi fem, a partir dels serveis que els contractem.

Certament, ara aquest proveïdors es limiten a posar-nos la infraestructura de comunicacions, però no hi ha cap motiu tecnològic perquè això no inclogui, en un futur, la identificació personal per navegar per la xarxa. De fet, a aquests operadors de telecomunicacions ja se'ls està donant un paper extra, com ara les obligacions en relació a la retenció de dades de trànsit o el que els pretenen atorgar legislacions com la francesa o l'anglesa, en relació al control del trànsit d'Internet i la descàrrega de continguts il·legals o protegits pel dret de propietat intel·lectual i els drets d'autor.

En tot cas, el temps ho dirà.