



**Jornades Tecnològiques per a la Protecció de Dades. dat 2009**  
**Discurs inaugural**  
**Barcelona, 9 de juny de 2009**

El dret a la protecció de dades o, si volem utilitzar un terme més ample, la privacitat, no és únicament un conjunt d'obligacions de les empreses i de les administracions, sinó també pot ser un important instrument per generar la confiança del client i dels ciutadans.

És més, en un moment com l'actual, en què el comerç electrònic o l'administració electrònica prenen cada dia més força davant d'una societat en crisi, és vital fomentar la confiança dels usuaris.

Aquesta confiança només es podrà crear si dissenyem entorns col·laboratius que tinguin en compte la privacitat, la protecció de dades personals i, dins d'aquest aspecte, la transcendència del concepte de seguretat de la informació com a valor i actiu de qualsevol entitat.

Parlem de privacitat dissenyada (*privacy by design*), i en aquest sentit és molt il·lustrativa la metàfora que utilitzen els anglosaxons:

«La privacitat s'ha de coure amb el pastís, és a dir, no s'ha d'afegir més tard com el sucre de llustre.»

La privacitat ha de ser un ingredient principal a l'hora de gestar un projecte, no pot ser un afegit per a la presentació final.

La majoria dels inconvenients per incorporar les garanties de protecció de dades a un projecte sorgeixen perquè s'hi pensa quan ja s'ha dissenyat i, normalment, a pocs dies d'engegar-lo.

No entraré a tractar tots els aspectes que cal garantir per complir la normativa de protecció de dades, però, des de la perspectiva de la seguretat de les dades personals (o de qualsevol informació de negoci), una de les preguntes que ens hem de fer és:

Com garantir que les dades personals només siguin accessibles a les persones autoritzades?

Recordem que es tracta del fet que les persones adequades tractin les dades adequades per a les finalitats adequades.

Però, a més a més, també d'una manera adequada. És a dir, amb una gestió integral de la seguretat que tinguin en compte el conjunt de normes i de regles existents per garantir la seguretat de la informació.

Cal comprovar constantment el grau de seguretat i cal analitzar els riscos en tots els processos d'una organització. No és suficient analitzar-ho en el lloc de treball concret, sinó



que cal integrar-ho en el conjunt de l'organització per evitar fuites derivades de tractaments de dades que impliquin més d'un lloc de treball .

Un altre dels entorns que cal reforçar és el de la gestió de la seguretat fora del lloc de treball. Estudis recents han comprovat que el 45 % dels executius i dels alts funcionaris que viatgen passen unes dues hores setmanals treballant en espais públics: el 31 % al bar, el 18 % al gimnàs, entre altres.

Hi ha consciència del perill?

Mesures que ens poden semblar tan òbvies com protegir amb contrasenyes els llapis de memòria o bloquejar els portàtils quan no són utilitzats, es porten realment a terme?

A priori, a alguns de vostès els podria semblar que estan molt conscienciats, però els estudis a què m'acabo de referir diuen que les persones enquestades han destacat que el problema més greu que tenen quan viatgen és trobar una impressora per imprimir documents confidencials o trobar un lloc per fer trucades.

Veiem que prenem consciència del perill quan pensem que ens poden agafar algun paper o escoltar alguna trucada, però poques vegades pensem en els suports de la informació.

A tall d'anècdota els volia comentar que, segons dades d'aquest mateix estudi, el 59 % dels americans i el 67 % dels britànics han escoltat d'amagat converses de negocis, per la qual cosa es recomana fer les trucades en sales privades o, en cas que s'hagin de fer en espais públics, utilitzar un llenguatge codificat. Potser seria bo que vostès mateixos es plantegessin si ho tenen en compte.

Pel que fa a la informació continguda en portàtils, el 34 % dels americans han vist informació confidencial i, en el cas dels britànics, el percentatge puja al 67 %.

Aquestes pèrdues d'informació tenen un cost. Concretament en el cas de perdre un portàtil es valora que la pèrdua total està al voltant dels 36.000 €. Dins d'aquest cost total, el cost concret per la pèrdua de les dades pot significar el 80 % del cost.

Tampoc podem oblidar un altre element que caldria afegir com a cost econòmic en el cas de perdre un portàtil, i és la pèrdua de la propietat intel·lectual.

Podem, per tant, pensar que el cost del software i del hardware és residual respecte del cost total produït per la pèrdua de la informació.

Que cada cop es té més consciència d'aquesta situació ens ho demostra la proliferació d'empreses que fan assegurances per cobrir el cost de la pèrdua de dades.

Tots aquests exemples em serveixen per inaugurar aquesta jornada amb una idea: les normes que regulen la protecció de les dades personals són una eina per garantir la seguretat de la informació. Cal pensar en una seguretat integral i integrada en el conjunt de



l'organització i en la consciència de tots els qui tracten la informació per tal d'assegurar l'eficàcia de qualsevol mesura que posem en marxa dins de les nostres institucions.

Esther Mitjans Perelló  
Directora