8a Trobada de Professorat de Ciències de la Salut
Taller 2: Protecció de dades i Big data/Open data

Universitat de Barcelona

Àlvar Sánchez
Assessor jurídic del rectorat i Coordinador de Protecció de Dades (Secretaria General)
4 de febrer de 2015

Agenda

1. **Aspectes competencials i funcionals del dret fonamental a la PD**

   a) Distribució de competències entre les diferents autoritats de protecció de dades
   b) L'assignació de funcions en la UB: el responsable del fitxer i el responsable de seguretat

2. **Supòsits de cessió de dades en els centres universitaris**

   a) Cessió o comunicació de dades: concepte
   b) Transmissió intraadministrativa de dades
   c) A entitats instrumentals (Grup UB)
   d) Difusió de les notes d'examen: publicació

3. **Definició de dades de caràcter personal. Dades de caràcter personal relacionades amb la salut**

4. **Protecció de dades i Big data/Open data**

   a) Big data/Open data
   b) Projecte de la Generalitat de Catalunya Visc+

5. **Reforma del marc normatiu europeu en matèria de protecció de dades**

1. Aspectes competencials i funcionals del dret fonamental a la PD

Agències/Autoritat de Protecció de dades

Agència Espanyola de Protecció de dades

- Fitxers de titularitat privada
- Fitxers de titularitat pública de les CCAA sense Agència

Agència Basca de Protecció de Dades

- Fitxers de titularitat pública de la seva CCAA

Autoritat Catalana de Protecció de dades
(*EAC 2006. Llei 32/2010, d'1 d'abril*)

- Fitxers de titularitat pública CCAA
- Fitxers de titularitat privada sector públic
- Fitxers de titularitat pública i privada de col·legis professionals
- Fitxers (de titularitat pública i privada) del sistema universitari català i ens que en depenen

Funcions en matèria de PD a la UB

Rector: decideix, mitjançant resolució que es publica al DOGC, la creació, modificació i supressió dels fitxers. També designa el responsable dels fitxers de la UB.

Responsable dels fitxers: és la persona física o jurídica, pública o privada, o òrgan administratiu, que sol o conjuntament amb altres decideix sobre la finalitat, el contingut i l'ús del tractament de les dades personals que conté el fitxer, encara que no ho faci materialment. En la UB, el responsable del fitxer és la secretaria general (òrgan administratiu). Sobre el responsable del fitxer recauen les principals obligacions establertes per la LOPD i li correspon vetllar pel compliment de la normativa en PD: ha de notificar els fitxers, oferir el dret d'informació en la recollida de dades, assegurar-se que es compleix amb el principi de qualitat, obtenir el consentiment quan calgui, autoritzar les cessions de dades, garantir els deures de secret i de seguretat, garantir l'exercici dels drets ARCO, així com nomenar al responsable de seguretat.

Comissió de Seguretat de la LOPD: té assignades les funcions de Responsable de Seguretat de la LOPD de tots els fitxers de titularitat de la UB. Són funcions del responsable de seguretat: coordinar i controlar les mesures que estan definides en el document de seguretat, rebre informació sobre les incidències de caràcter greu, analitzar els informes d'auditoria i elevar les seves conclusions al responsable del fitxer, etc.

Aquesta comissió està integrada per:

- Secretària General, que exerceix la presidència.
- Director/a de l'Àrea de Serveis Comuns, Grup UB i Projectes.
- Director/a de l'Àrea TIC.
- Director/a de l'Àrea de Recursos Humans i Organització.
- Vocal de Secretaria General.

2. Supòsits de cessió de dades en els centres universitaris

Cessió o comunicació de dades

La cessió o comunicació de dades és el tractament de dades que suposa la seva revelació a una persona diferent de l'interessat o afectat. La revelació es refereix tant al lliurament, comunicació, consulta, interconnexió, transferència, difusió o qualsevol altra forma que faciliti l'accés a les dades d'un fitxer a un tercer, diferent del titular del fitxer. Exemple, publicació d'una llista de qualificacions.

La cessió implica una important pèrdua de control sobre les dades personals, atès que aquestes passen a entitats o persones diferents d'aquelles a qui, en un principi, s'han facilitat. Per això, l'art. 11 LOPD requereix, com a principi general, **el consentiment previ de l'interessat**, encara que hi ha excepcions.

Excepcions a la necessitat del consentiment per a la cessió:

a) Quan la cessió està autoritzada per una **llei**. Exemples de cessions de dades en la UB: la que es fa a la Tresoreria de la Seguretat Social (art. 13 TRLGSS), a l'Agència Tributària (art. 93 LGT), etc.
b) (...)
c) (...)
d) (...)

Transmissió intraadministrativa de dades

Si d'acord amb la normativa de protecció de dades es considera cessió o comunicació tota revelació de dades realitzada a una **persona diferent** de la persona interessada, les transmissions de dades entre òrgans o unitats que formen part d'una mateixa administració, és a dir, d'una mateixa persona jurídica, no es consideren una comunicació de dades, sempre que es doni el **principi de finalitat**.

Si la transmissió entre òrgans diferents de la mateixa administració pública no respon a la mateixa **finalitat** estarem davant d'una cessió de dades i caldrà obtenir el consentiment de l'afectat (AVPD CN11-031). *"Debe descartarse dicha posibilidad porque, aún siendo cierto que la LOPD no contempla expresamente la cesión "intraadministrativa", la misma debe quedar sometida al mismo régimen jurídico general al que se somete la cesión o comunicación de datos en cuanto el aspecto clave para una correcta protección del derecho fundamental, no radica en la existencia o no de personalidad jurídica en los hipotéticos cedente y cesionario, sino en la correcta aplicación del* ***principio de finalidad*** *que es en definitiva lo que se encuentra en la base tanto del artículo 11 como del artículo 21 de la LOPD."*

El fet que un òrgan o una unitat administrativa gestioni o tracti dades personals, no vol dir que totes les persones d'aquesta unitat puguin accedir a totes les dades. Segons l'article 91 del RLOPD "*Control d'accessos*",

1. Els usuaris han de tenir accés només als recursos que necessitin per a l'exercici de les seves funcions.
2. El responsable del fitxer s'ha d'encarregar que hi hagi una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'ells.
3. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a recursos amb drets diferents dels autoritzats.

Supòsit pràctic: accés a l'expedient acadèmic d'un alumne

APDCAT Resolució d'arxiu IP 98/2013

La persona denunciant considerava que l'advocada del seu exmarit, en un procés judicial sobre divorci, gràcies a la seva condició de professora de la UdG hauria accedit a les dades del seu expedient acadèmic referents a la realització de dos màsters. Això, de confirmar-se, podria suposar una comunicació de dades il·legítima.

La UdG va dir que "*no tenia constància que aquella professora hagués sol·licitat l'accés a l'expedient acadèmic de la denunciant,* ***ni com a professora d'aquesta Universitat tenia un perfil d'usuari que li permetia tal accés.***"

L'APDCAT va assenyalar que *"Doncs bé, el cert és que de les actuacions efectuades en el marc de la informació prèvia no es desprenen indicis que permetin considerar que l'esmentada professora i advocada hagués accedit a l'expedient acadèmic de l'aquí denunciant custodiat per la UdG. És per això que, en base al principi de presumpció d'innocència, procedeix acordar l'arxiu de les presents actuacions, d'acord amb allò que determina l'article 10.2 del Decret 278/1993."*

Cessió o comunicació a entitats instrumentals (Grup UB)

Informe Jurídic 0494/2008 de l'AEPD**:** És criteri uniforme de l'AEPD que l'existència d'un grup d'empreses no afecta per a que cadascuna de les societats integrades en el mateix no mantingui diferenciada i plena la seva personalitat jurídica. A tots els efectes jurídics, la circumstància que una societat estigui participada per una altra, no afecta el fet que ambdues siguin diferents persones, de manera que la comunicació de dades es produeix entre dues persones diferents, sense que hi hagi una previsió legal que flexibilitzi els requisits per a la legitimitat de la cessió. Aquest criteri ha estat ratificat per la Sentència de la Secció Novena de la Sala Contenciosa Administrativa del Tribunal Superior de Justícia de Madrid, de 16 d'octubre de 2000, quan en el seu fonament de dret quart assenyala que, "*Qualsevol empresa és lliure de constituir-se en qualsevol de les formes societàries que el dret mercantil regula. Així mateix, les empreses poden unir-se a través de les diferents formes regulades en dret: fusió, absorció, etc. Però, per descomptat, el que no cal és que hi hagi dues societats anònimes i, com a tals, independents i amb personalitat jurídica autònoma i que pel fet que una sigui propietat de l'altra, el particular que contracta amb la primera pugui veure's perjudicat, precisament, per l'estructura empresarial que la societat ha triat. Si la recurrent ha preferit constituir dues societats i treballar amb elles de manera independent, beneficiant-se així del manteniment de dues persones jurídiques diferents, ha de ser posteriorment coherent amb aquesta decisió*"

Dictamen CNS 17/2010 de l'APDCAT: La comunicació de dades entre l'Administració pública matriu i un ens instrumental encaixa en el concepte de cessió de dades. L'ens instrumental ha de ser considerat un "*tercer*" aliè a l'Administració Pública, i per tant cal sotmetre aquesta transmissió de dades al règim general de cessió de dades establert en la LOPD (articles 11 i 21).

Difusió de les qualificacions dels aprenentatges

Amb la LOPD (1999), la publicació de les qualificacions es considera una cessió de dades que precisa el consentiment de l'afectat o una previsió legal que l'empari. Així, doncs, a partir d'aquest moment la publicació de les qualificacions dels alumnes suposava cometre una infracció. En aquest sentit, l'informe de l'AEPD 469/2004 "*Publicación en tablones de las calificaciones de alumnos universitarios*",

> "*En consecuencia la difusión de dichas notas de calificación a través de los tablones de anuncios de la Universidad, constituirá una cesión de datos de carácter personal de los alumnos no autorizada por una norma con rango de ley formal.*"

Per tal d'intentar solucionar aquesta situació, la pròpia AEPD proposaria al Govern estatal l'aprovació d'un precepte en una llei que contemplés l'exempció del consentiment per tal de poder continuar publicant les qualificacions dels alumnes. Aquest objectiu es va assolir amb la introducció de la Disposició addicional vint-i-unena. *Protecció de dades de caràcter personal de la LOU de 2007:*

> *3. No és necessari el consentiment dels estudiants per a la publicació dels resultats de les proves relacionades amb l'avaluació dels seus coneixements i competències, ni dels actes que siguin necessaris per a l'adequada realització i seguiment de l'avaluació.*

A partir d'aquest moment, l'AEPD ha interpretat que (R/00224/2010, de 10 de febrer de 2010),

> *"En consecuencia, la entidad denunciada (Universidad Politécnica de Valencia) se encuentra habilitada legalmente para exponer las notas de sus alumnos en los tablones de anuncios sin contar con el consentimiento de los mismos".*

No obstant, sobre la norma es plantegen com a mínim dues qüestions: a) amb quines dades identificatives es podia procedir a la publicació, i b) lloc de publicació, o el que és el mateix, quin abast ha de tenir aquesta publicació.

Dades identificatives de l'alumne que es poden publicar

Resolució del procediment sancionador núm. PS 19/2014, referent a la UPF, on la persona denunciant exposava que "*el dia 19/06/2013, a l'Aula Global de la Facultat de Ciències de la Salut i de la Vida de la UPF, es va publicar un document que contenia dades relatives a 27 persones. Les dades personals publicades eren, entre d'altres, el nom i cognoms, el número d'identificació universitària (NIA) i la nota mitjana obtinguda als estudis de grau de Medicina*.". L'APDCAT diu,

- La publicació es pot realitzar en virtut de la previsió legal de la Disposició Addicional 21, apartat 3, de la LOU.

- *"L'apartat primer de l'article 4 de la LOPD consagra el principi de proporcionalitat en el tractament de dades personals, en virtut del qual només es poden tractar aquelles dades personals que resultin pertinents, adequades i no excessives d'acord amb la finalitat que justifiqui aquest tractament, i que impedeix, per tant, el tractament d'aquelles dades que no siguin necessàries o proporcionades a la finalitat que justifica el tractament. Així les coses, cal dilucidar si la inclusió del número de NIA, juntament amb el nom i cognoms, complia amb aquest principi de qualitat de les dades*."

"S'hauria pogut assolir sense necessitat de publicar el nom i cognoms juntament amb el número del NIA, ja que la identificació de les persones interessades quedava garantida mitjançant la publicació del seu nom i cognoms, i només en el cas que aquests fossin coincidents en dos o més persones interessades -circumstància que, val a dir, no es dóna en el supòsit que ens ocupa-, estaria justificada la publicació del NIA, sense que fos necessària tampoc la publicació de totes les xifres, ja que podria resultar suficient, a tall d'exemple, les tres darreres.". **Declaració d'infracció greu**.

Acord d'inici i del plec de càrrecs del procediment sancionador referent a la Universitat de Barcelona.

"Dels fets que s'han relatat als antecedents i de les actuacions practicades durant la informació prèvia, s'infereix que la UB podria haver vulnerat la LOPD, ates que va publicar a la plataforma "Campus Virtual de la Universitat de Barcelona", (...) un llistat en el que s'incloïen dades personals que podrien considerar-se excessives i desproporcionades, atenent a la finalitat perseguida amb la publicació d'aquella llista. En concret, atès que en el llistat esmentat hi figurava el nom i cognoms dels estudiants per identificar-los, es considera que podria ser excessiva la inclusió del NIUB (número d'identificació dels estudiants de la Universitat de Barcelona)."

Lloc on s'han de publicar les qualificacions dels aprenentatges a la UB

A partir del curs 2012-2013, la Normativa reguladora dels plans docents de les assignatures i de l'avaluació i la qualificació dels aprenentatges (Aprovada per Consell de Govern en data 8 de maig de 2012), assenyala a l'article 18.4 que: "*La informació pública sobre el resultat de les avaluacions, siguin parcials o finals, té lloc mitjançant els mecanismes establerts amb aquesta finalitat. El professorat pot fer la difusió de les qualificacions de manera virtual, a través de les aplicacions institucionals establertes a aquest efecte*", per afegir posteriorment a l'Annex, que "*La publicació de les qualificacions virtuals es fa a través de l'espai específic de l'assignatura al Campus Virtual (o a l'espai que el substitueixi en el futur) o a través de l'expedient acadèmic de l'estudiant (Món UB), al qual es pot accedir, de manera individual i privada, telemàticament*".

Criteri del responsable dels fitxers de la UB (Secretaria general)

1) Es recomana publicar les qualificacions en el Campus Virtual de forma individualitzada (D'aquesta forma també s'evitarà que hi hagi estudiants que facin una fotografia de la llista de notes i la pugin a Facebook o Twitter.).

2) Si es fa en llistes, l'abast únicament hauria de restringir-se al grup de l'assignatura. S'ha de realitzar amb les dades identificatives de nom i cognoms o del NIUB, però no amb les dues formes d'identificació. En cas de coincidència de nom i cognoms s'han de publicar les tres darreres xifres del NIUB. La llista s'hauria de retirar en el termini de vint dies o en el moment en què la finalitat de la publicació hagi acabat.

El document on constin les qualificacions hauria de contenir la següent menció:

"*Aquest document s'ha publicat en el Campus Virtual de la UB amb la finalitat de publicar les qualificacions. Qualsevol ús per a una altra finalitat pels membres del Campus de totes o part de les dades que conté, o la seva difusió o publicació per qualsevol mitjà, i particularment en Internet, pot constituir una infracció sancionable d'acord amb la normativa de protecció de dades de caràcter personal*".

3) Qualsevol altra forma de publicació de llistes de qualificació s'ha de considerar inadequada a la vista de la legislació de Protecció de Dades.

3. Definició de dades de caràcter personal. Dades de caràcter personal relacionades amb la salut

Dades de caràcter personal i dades de caràcter personal relacionades amb la salut

Dades personals ≠ dades de caràcter personal. No obstant, en la pràctica, s'utilitzen indistintament.

Definició de dades de caràcter personal: **Qualsevol informació** referent a **persones físiques identificades** o **identificables** (art. 3 LOPD). El RD 1720/2007, de 21 desembre ha concretat aquesta informació en el sentit de que pot ser numèrica (DNI, número de la SS, NIUB. etc.), alfabètica (nom i cognoms), gràfica (signatura), fotogràfica (foto), acústica (veu) o de qualsevol altre tipus. A la vista d'aquesta definició, també poden ser dades personals l'empremta digital, el grup sanguini, l'iris, o les dades genètiques (ADN). Però també són dades de caràcter personal la durada d'una determinada trucada telefònica, les pàgines web que visitem i a l'hora que ho fem, etc.

Les agències de protecció de dades han resolt en sentit positiu alguns dubtes sobre la categorització com a dada de caràcter personal de: DNI o NIE, adreça electrònica, núm. mòbil, o l'adreça IP.

Definició de dades de caràcter personal relacionades amb la salut: les informacions que concerneixen la salut passada, present i futura, física o mental, d'un individu. En particular, es consideren dades relacionades amb la salut de les persones les referides al seu percentatge de discapacitat i a la seva informació genètica (art. 5 g RLOPD).

"Qualsevol informació"

L'amplitud del concepte de "*dada de caràcter personal*" ve determinada per les avançades tècniques de processament de la informació, que són capaces d'aglutinar molta informació sobre una persona. No existeix una dada irrellevant. D'això era ben conscient Google quan va unificar les polítiques de privacitat dels més de 70 productes en una de sola, en entendre que únicament té un servei que denomina "*Servei on-line*", la qual cosa li ha possibilitat agrupar i combinar les dades que obté de qualsevol persona que utilitza els seus productes.

Per això, un antic director d'informació de Google i fundador de ZestFinance -una empresa que fa ús de les dades per subministrar informació sobre capacitat de crèdit-, va dir al *The New York Times* l'any 2012: "*Totes les dades són útils per al crèdit. Aquesta és la matemàtica que vam aprendre a Google. Una pàgina era important pel que hi havia en ella, però també per la qualitat de la seva gramàtica, per quina era la seva font tipogràfica, quan es creava o s'editava*". Amb aquest propòsit, examina 70.000 indicadors i els inclou en 10 models diferents de subscripció per avaluar el risc. Els resultats són comparats en mil·lèsimes de segon i es genera un perfil de risc del sol·licitant del crèdit.

L'empresa nord-americana Cignifi utilitza la durada de les trucades, el moment del dia i la localització per calcular l'estil de vida -i per tant la fiabilitat- dels sol·licitants de préstecs.

Tres científics de la Universitat de Cambridge han desenvolupat un model matemàtic on s'assenyala que amb els "*M'agrada*" de Facebook es pot saber amb una probabilitat del 95% la raça, un 85% si és de dretes o esquerres, un 88% si és homosexual o no, un 80% la seva religió. Els investigadors van analitzar dades de 58000 usuaris i la seva única pretensió era millorar la privacitat.

“Referent a persones físiques identificades o identificables”

Les **dades relatives a persones identificades** són aquelles dades que apareixen vinculades amb la persona respecte de la qual aporten informació. Així, quan disposem del nom i cognoms, del càrrec o posició de la persona en una organització, etc.

Les **dades relatives a persones identificables**: es tracta de dades que no s'associen directament a una persona determinada, ja que aquesta no apareix identificada però és relativament fàcil saber-ho. Així, mitjançant un número de telèfon, una combinació de criteris significatius (edat, sexe, ocupació). L’article 5, apartat o) del RLOPD defineix persona identificable, com a “*qualsevol persona la identitat de la qual es pugui determinar, directament o indirectament, mitjançant qualsevol informació referida a la seva identitat física, fisiològica, psíquica, econòmica, cultural o social. Una persona física no es considera identificable si la dita identificació requereix terminis o activitats desproporcionats*” (cost, temps, treball, finalitat, etc.)

Si la dada no es pot associar a una persona és una dada anònima o anonimitzada. Evidentment, a les dades anònimes o anonimitzades, per la pròpia definició de dada de caràcter personal, no se’ls aplica la LOPD. La Directiva 95/46, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, estableix al Considerant 26 que "*els principis de la protecció no s'aplicaran a aquelles dades fetes anònimes de tal manera que ja no sigui possible identificar l'interessat*".

4. Projecte Visc+

Big data i Open Data

Big data i Open data són conceptes similars però no iguals.

1) El fenomen **Big Data** es refereix a l'acumulació massiva de dades amb el propòsit d'analitzar-les. S'ha de posseir una tecnologia prou avançada perquè el seu tractament permeti realitzar tot tipus d'anàlisi de les mateixes mitjançant algoritmes. No cal que les dades estiguin anonimitzades.

2) Després d'analitzar i d'ordenar aquestes dades, si es decideix posar d'ofici una part a disposició de tothom ens trobarem dins l'àmbit de l'**Open Data**. Per publicar-les, les dades han d'estar anonimitzades.

Ex. Ajuntament de Barcelona i Open data

Ex. Tendències de cerca en Google

Projecte Visc+: presentació i cronologia

1) **Juny de 2013**: Aprovació del projecte Visc+ (Més Valor a la informació de Salut de Catalunya) pel govern de la GC amb la finalitat de "*relacionar i estructurar*" tota la informació sanitària digitalitzada obtinguda de centres d'atenció primària, hospitals, així com de les receptes electròniques, i tenir-la a disposició "*dels ciutadans, de les empreses i de la recerca*".

2) **Juliol de 2014**: L'APDCAT va emetre el Dictamen CNS 34/2014, de data 23 de juliol, on manifestava determinades objeccions en relació amb les mesures de seguretat del projecte i el projecte en sí.

3) **Octubre de 2014**: Interpel·lació al Govern sobre el Projecte VISC+. Una diputada del Parlament de Catalunya, en seu parlamentària, va posar de manifest els eventuals perills del projecte. La majoria dels grups parlamentaris van considerar necessari aturar el projecte i obrir un període de debat amb actors socials.

4) **Gener de 2015**:Reunió entre representants del projecte, l'APDCAT i parlamentaris catalans.

Projecte Visc+: alguns beneficis

A judici dels promotors del projecte, es poden trobar els següents beneficis.

1) **Per a la ciutadania**. Algunes de les preguntes que es podran respondre utilitzant VISC+ seran, per exemple:

- *Quins efectes té sobre la salut futura la radiació rebuda en les etapes infantils?*
- *Quina és l'efectivitat comparada (atenció real) de diferents medicaments per una mateixa indicació?*
- *Quina diferència en termes d'esperança de vida presenten els pacients que reben tractaments de quimioteràpia respecte als que reben tractaments pal·liatius en els darrers tres mesos de vida?*

2) **Per als investigadors**. Existeix una creixent demanda de la comunitat científica de disposar d'informació anonimitzada de salut procedent de diferents fonts, de qualitat i de manera relacionada per contribuir a la recerca.

3) **Per al sistema sanitari**. L'anàlisi de les dades anonimitzades permet millorar la presa de decisions i la capacitat de gestió del Departament de Salut. Així, permet cercar tractaments més efectius, incrementant la capacitat d'avaluació dels serveis i la cerca de millors pràctiques sanitàries, millorant l'experiència del pacient.

Riscos Projecte Visc+: experiència NHS

Un exemple d'un projecte similar al Visc+ és el projecte *Care.Data del National Health Service* (NHS) d'Anglaterra. Es van començar a recopilar un gran volum de dades procedents dels Hospitals i dels metges de capçalera per tal de posar-les a l'abast de qui estigués interessat sense haver demanat el consentiment dels afectats. La revista científica *Nature* va publicar un dur editorial crític amb el govern anglès dient que "*falla a l'hora d'informar sobre l'amenaça real i les possibles conseqüències del programa*" i assenyala com a problema que el govern no ha facilitat als ciutadans l'opció de no participar en el programa.

El tema es va agreujar quan el diari Telegraph, va publicar un article afirmant que l'any 2012 el NHS va vendre per 2.220 € a una associació d'actuaris un conjunt de dades massives que incloïa informació sobre l'estada de pacients en els hospitals entre els anys 1997 i 2010 i les seves històries clíniques, identificant-los mitjançant la data de naixement i el codi postal. Aquesta associació va elaborar una guia que permetia, per exemple, a les companyies d'assegurances redefinir les seves ofertes als ciutadans a partir dels **perfils** que havien generat amb la base de dades provinent del NHS. El propi NHS va admetre que hi ha un "petit risc" de que els pacients siguin identificats ja que aquestes companyies d'assegurances, així com les companyies farmacèutiques, podien creuar les dades del NHS amb les seves pròpies.

Es va generar una gran preocupació ciutadana i com a conseqüència, el NHS ha aturat temporalment el programa amb la finalitat de poder escoltar l'opinió pública i adoptar les aportacions que realitzessin.

Projecte Visc+: consentiment i re-identificació

1) Necessitat de consentiment per tal de procedir a la dissociació de les dades.

Procediment de dissociació (art. 3 f LOPD) definit com qualsevol **tractament de dades** personals de manera que la informació que s'obtingui no es pugui associar a una persona identificada o identificable.

En ser el procediment de dissociació un tractament de dades sotmès a la LOPD, cal el **consentiment previ** de la persona afectada (o una llei que així ho contempli) per tal de poder-lo realitzar.

2) **Risc de re-identificació.**

Si bé existeixen processos d'anonimització de les dades, també existeixen processos de re-identificació, és a dir que, mitjançant diverses tècniques informàtiques es poden creuar les dades fins arribar a identificar les persones i relacionar-les amb la seva informació mèdica personal.

Segons el Grup de Treball de l'Article 29, el risc de re-identificació és inherent a qualsevol tècnica d'anonimització, per la qual cosa la intimitat i el dret a la protecció de dades del titular, es podria veure compromesa.

També l'Observatori de Bioètica de la UB considera que hi ha molts mètodes informàtics per tal de re-identificar a una persona en el sistema de salut. Document sobre Bioètica i Big Data de salut: explotació i comercialització de les dades dels usuaris de la sanitat pública (gener 2015).

També el Síndic de Greuges de Catalunya està realitzant un informe.

Possibles models de gestió del projecte VISC+ (I)

En el document "*Més valor a la informació de salut de Catalunya - Anàlisis dels possibles models per a la gestió del projecte*" publicat al desembre del 2014 per l'Agència de Qualitat i Avaluació Sanitàries de Catalunya (AQUAS) es presenten dos possibles models de gestió del projecte VISC+:

1) L'AQUAS exercirà la governança i operativitat del projecte.
2) L'AQUAS exercirà la governança i un o més col·laboradors externs a l'administració pública exerciran l'operativitat del projecte, amb la possibilitat de subcontractació.

En els dos models, l'AQUAS és qui té la responsabilitat de la governança del projecte, com no podria ser d'una altra manera ja que no és possible renunciar a les responsabilitats que se li han encomanat per una llei.

L'aspecte diferenciador dels dos models de gestió és qui construirà i executarà tots els aspectes tècnics i operatius.

Possibles models de gestió del projecte VISC+ (II)

Tasques	Model de gestió I	Model de gestió II
Procés d'anonimització i relació de les dades de salut	Agència de Qualitat i Avaluació Sanitàries de Catalunya	Agència de Qualitat i Avaluació Sanitàries de Catalunya
Gestionar les sol·licituds de serveis		
Tasques de comunicació i transparència de cara a donar retiment de comptes als ciutadans		
Controlar que en tot moment s'apliquin els principis ètics i de protecció de dades		
"*Gestionar el valor i la qualitat de tots els actius (tangibles i intangibles)*" que es creïn durant el projecte		
Crear els serveis d'Open Data, serveis d'anàlisi i estadística de dades, serveis d'informes maquetats en diversos formats com ara PDF, infografies o pòsters, etc.		Col·laboradors externs a l'Administració pública
Donar a conèixer el projecte als possibles sol·licitants dels serveis (nivell nacional i internacional)		
Elaborar els elements tecnològics del projecte: plataformes o programes d'explotació de les dades anonimitzades, pàgines web de comunicació, programes de control i auditoria, etc.		

5. Reforma del marc normatiu europeu en matèria de protecció de dades

Procés de substitució de la Directiva 95/46/CE per un Reglament

La **Directiva 95/46/CE, de 24 d'octubre de 1995**, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, és el principal instrument actual de la legislació en matèria de protecció de les dades personals a la UE. Es va fer quan només un 1% dels europeus feia servir habitualment Internet (50.000 persones). Avui, en canvi, el 90% es connecta a la "*Xarxa*". Internet és arreu i els ciutadans en fan ús per a tot.

Han aparegut nous serveis associats a Internet com les xarxes socials, els cercadors, la geolocalització, la realitat augmentada, el RFID (identificació per radiofreqüència), el codi QR (codi de barres de resposta ràpida), reconeixement facial, Big data, etc.

També, es pretén flexibilitzar les garanties que ofereix aquest dret als ciutadans en favor del mercat de les telecomunicacions i les gran empreses de màrqueting, atès que es queixen que l'actual Directiva implica moltes càrregues administratives que els hi resta competitivitat (ex. Inscriure els seus fitxers en cadascun dels estats de la UE en que operi, haver de complir amb 28 legislacions de protecció de dades que tenen importants matisos).

Per això, s'ha posat en marxa un procés de substitució de la Directiva 95/46/CE per un reglament, d'obligació immediata per als estats de la UE sense necessitat de ser transposat. Es troba en fase d'aprovació.

Proposta de Reglament Europeu de Protecció de dades: sancions, DPO i PIA

En el text d'aquesta proposta de reglament es contemplen importants novetats que afectaran sensiblement a l'actual regulació. Així i pel que fa al nostre àmbit, cal destacar:

a) les administracions públiques podran ser objecte de **sancions econòmiques**. Cal posar de manifest que les quanties de les sancions augmentaran considerablement en relació a les establertes en la LOPD,

b) obligació que totes les administracions públiques disposin d'un **Data Protection Officer** (Delegat de Protecció de Dades). Se li atribueixen un gran ventall de funcions, per exemple, actuar com interlocutor davant la corresponent autoritat de protecció de dades o comprovar que es duu a terme "*l'Avaluació de l'impacte relatiu a la protecció de dades*" (P.I.A, per les seves sigles en llengua anglesa).

c) la implantació dels **Privacy Impact Assessment** (P.I.A) que consisteix en avaluar l'impacte en relació amb la protecció de dades quan es posa en marxa un nou projecte o aplicació on es vagin a tractar dades de caràcter personal (ex. un projecte de recerca que vagi a utilitzar dades de caràcter personal, una nova aplicació informàtica que vagi a tractar dades de caràcter personal, etc.). L'objectiu que es persegueix amb els P.I.A. és instaurar l'obligació que, a diferència de com es fa en l'actualitat on l'avaluació de protecció de dades es realitza al final del projecte amb els consegüents i possibles problemes de modificar-lo quan ja està plenament finalitzat i a punt de ser implementat, el personal de protecció de dades intervingui prèviament des de la posada en marxa d'aquest projecte.

Moltes gràcies per la seva atenció

protecciodedades@ub.edu