

Dictamen en relació amb la consulta formulada pel Síndic de Greuges d'una Universitat pública pel que fa a les consideracions efectuades en el Dictamen CNS 28/2011 de l'Autoritat Catalana de Protecció de Dades

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit emès pel Síndic de Greuges d'una Universitat en què, un cop examinades les consideracions realitzades per aquesta Autoritat en el Dictamen CNS 28/2011, sol·licita un nou dictamen per tal de determinar si el sistema d'autenticació emprat per aquesta Universitat per accedir al seu campus virtual, així com la publicació de determinades dades personals en aquest espai, resulta conforme amb la normativa de protecció de dades personals.

S'adjunta a la petició un informe del Director de l'Àrea de Sistemes de la Informació i Comunicacions de la Universitat en què s'explicita el funcionament del campus virtual d'aquesta Universitat.

Analitzada la consulta, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

El dictamen CNS 28/2011, a què fa referència el Síndic de Greuges de la Universitat (en endavant, Síndic) en el seu escrit de consulta, va ser emès, com s'ha avançat en els antecedents d'aquest informe, per l'Autoritat Catalana de Protecció de Dades en resposta a una anterior consulta plantejada per aquest mateix Síndic en relació amb la possibilitat d'utilitzar el número de DNI com a login i la seva possible publicació al web de la Universitat.

Un cop revisades les consideracions que, a partir de la informació que en aquell moment es va facilitar, va efectuar l'Autoritat en l'esmentat dictamen CNS 28/2011 per l'Àrea de Sistemes de la Informació i Comunicacions de la Universitat i fetes per aquesta mateixa unitat unes puntualitzacions al respecte, el Síndic torna a plantejar, si bé de manera més detallada, les següents quatre qüestions:

1. És correcte utilitzar per l'accés al campus virtual un login format per la lletra del NIF més els 7 primers dígit del DNI i un password d'un mínim de 8 dígit i que ha de contenir obligatòriament 3 dels 4 tipus de caràcters següents: majúscules, minúscules, dígit (0-9), signes de puntuació...?
2. És correcte que aquest login consistent en la lletra del NIF i els 7 primers dígit del DNI aparegui al costat del nom i cognoms de l'alumne, dins l'eina de missatges del campus virtual, per poder identificar de forma inequívoca un alumne tenint en compte el context del campus virtual, que és una eina destinada únicament a la docència i que la finalitat d'aquesta eina és poder avaluar amb garanties als alumnes (...)?

3. Pel que fa a l'eina de missatges del campus virtual referida en la pregunta anterior, estaria emparada per la Disposició addicional 21a, punt 3, de la Llei orgànica 4/2007, de 12 d'abril, per la que es modifica la Llei orgànica 6/2001, de 21 de desembre, d'Universitats, o bé per altra llei? En el seu cas, caldria el consentiment previ de l'alumne?

4. Donat que la queixa de la persona interessada es centra en que el seu document d'identitat no figuri en el campus virtual, en cursos on hi intervenen persones alienes a la Universitat (...), té dret a que se li canviï el login només per aquests casos?

L'anàlisi d'aquestes qüestions es realitza en els següents apartats d'aquest dictamen, tenint en compte la informació addicional aportada en l'escrit de consulta.

III

Tal i com ha manifestat aquesta Autoritat en dictàmens anteriors, entre d'altres, en els dictàmens CNS 20/2011, CNS 24/2011 o, especialment, en l'esmentat CNS 28/2011 (disponibles al web de l'Autoritat www.apd.cat), el número del Document Nacional d'Identitat (DNI) constitueix, sens dubte, una dada de caràcter personal (article 3.a) de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal), atès que, de conformitat amb allò establert al Reial decret 1553/2005, de 23 de desembre, pel qual es regula l'expedició del Document Nacional d'Identitat, permet identificar inequívocament una determinada persona física. Per tant, és clar que el seu tractament estarà subjecte als principis i obligacions de la normativa en matèria de protecció de dades.

En el cas examinat, es planteja, en primer lloc, si es pot emprar, com a sistema d'identificació i d'autenticació per accedir al campus virtual de la Universitat, un login format per la lletra del NIF més els 7 primers dígit del DNI i un password d'un mínim de 8 dígit amb unes determinades característiques (ús de majúscules, minúscules, dígit o signes de puntuació).

Com a consideració prèvia pel que fa a l'ús del número del DNI com a login, convé recordar, com es va fer en l'anterior dictamen CNS 28/2011, que el fet que no hi aparegui la darrera xifra (s'afirma, en aquest sentit, que s'inclouran els 7 primers dígit del DNI) no altera la seva consideració com a dada personal, atès que, a banda de la facilitat amb què es pot esbrinar aquesta darrera xifra, en la mesura que aquest número s'utilitza com a login o sistema d'identificació, constitueix ja en si mateix (com a número de 7 xifres que identifica un usuari) una dada de caràcter personal.

Dit això, s'analitza a continuació la possibilitat d'emprar el sistema d'identificació i d'autenticació indicat, per accedir al campus virtual de la Universitat.

D'acord amb l'informe de l'Àrea de Sistemes de la Informació i Comunicacions de la Universitat adjuntat a la consulta, el campus virtual es configura com un conjunt de processos de comunicació i d'intercanvi d'informació a través de la xarxa, dissenyat específicament per optimitzar l'ensenyament a distància i per oferir el màxim nombre d'eines al professorat a l'hora d'avaluar els seus estudiants. Entre les diferents eines disponibles, ubicades dins un mateix espai del campus virtual (que correspon a una assignatura en concret), figuren algunes funcionalitats que permeten als participants presentar activitats, realitzar tests d'avaluació, debatre, consultar les qualificacions obtingudes o conèixer la resta d'estudiants d'una mateixa assignatura.

Totes aquestes eines o funcionalitats del campus virtual permeten recollir i intercanviar informació personal dels seus participants (estudiants i professors) dins d'un context estrictament educatiu, de tal manera que, des de la vessant del dret a la protecció de dades personals, és necessari garantir que terceres persones alienes a aquest entorn puguin accedir fàcilment a aquesta informació.

En aquest sentit, convé tenir en compte que la normativa de protecció de dades personals imposa l'obligació al responsable del tractament i, si s'escau, a l'encarregat del tractament d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries per tal de garantir la seguretat de les dades personals que seran tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9 LOPD). Aquestes mesures de seguretat venen regulades en el Reglament de desplegament de la LOPD, aprovat pel Reial decret 1720/2007, de 21 de desembre (RLOPD).

En el cas examinat, i d'acord amb la tipologia de dades personals que sembla ser que serien tractades (dades identificatives, acadèmiques, professionals...), les mesures de seguretat a implementar corresponen a les de nivell bàsic (article 81.1 RLOPD), atès que *a priori* no es preveu tractar dades personals que requereixin l'adopció d'un nivell superior de mesures de seguretat.

En concret, tenint en compte que el tractament d'aquestes dades s'efectua de manera automatitzada, correspon aplicar les mesures descrites en els articles 89 a 94 del RLOPD i, especialment, les relatives a l'establiment d'un control d'accés (article 91) i a l'adopció de mecanismes que permetin la correcta identificació i autenticació dels usuaris (article 93 RLOPD):

“Article 91. Control d'accés

- 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.*
- 4. Exclusivament el personal autoritzat per fer-ho en el document de seguretat pot concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, de conformitat amb els criteris que estableix el responsable del fitxer.*
- 5. En cas que existeixi personal aliè al responsable del fitxer que tingui accés als recursos, ha d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi.”*

“Article 93. Identificació i autenticació

- 1. El responsable del fitxer o tractament ha d'adoptar les mesures que garanteixin la correcta identificació i autenticació dels usuaris.*
- 2. El responsable del fitxer o tractament ha d'establir un mecanisme que permeti la identificació de forma inequívoca i personalitzada de qualsevol usuari que intenti accedir al sistema d'informació i la verificació conforme està autoritzat.*
- 3. Quan el mecanisme d'autenticació es basi en l'existència de contrasenyes, hi ha d'haver un procediment d'assignació, distribució i emmagatzematge que en garanteixi la confidencialitat i integritat.*
- 4. El document de seguretat ha d'establir la periodicitat, que en cap cas ha de ser superior a un any, amb què s'han de canviar les contrasenyes que, mentre estiguin vigents, s'han d'emmagatzemar de forma intel·ligible.”*

Per tant, d'acord amb aquests preceptes, es poden utilitzar sistemes d'identificació i d'autenticació basats en un usuari i una contrasenya per accedir al contingut de pàgines web, si bé en aquests casos cal que:

- El procediment de gestió de les contrasenyes garanteixi la confidencialitat i la integritat de les mateixes.
- La contrasenya sigui robusta. La major o menor exigència en aquest aspecte dependrà de la naturalesa de la informació protegida, però en qualsevol cas pot portar a establir uns requeriments mínims.
- El responsable estableixi perfils d'usuaris per tal que cada usuari pugui accedir només a aquella informació per a la qual estigui autoritzat.
- Les contrasenyes es canviïn de forma periòdica, i en qualsevol cas sempre abans d'un any.

En el cas examinat, com s'ha indicat, el mecanisme que es vol emprar com a sistema d'identificació i d'autenticació per accedir al campus virtual de la Universitat consistirà en l'ús d'un usuari (lletra del NIF més els 7 primers dígits del DNI) i d'una contrasenya (mínim de 8 dígits que obligatòriament contindrà 3 dels 4 tipus de caràcters següents: majúscules, minúscules, dígits (0-9) o signes de puntuació).

Aquest mecanisme, que difereix de l'analitzat en el dictamen CNS 28/201, resultaria una mesura de seguretat adequada i, per tant, es podria emprar per accedir al campus virtual de la Universitat.

IV

D'altra banda, es planteja (qüestió segona) si és correcte que aquest login consistent en la lletra del NIF i els 7 primers dígits del DNI aparegui al costat del nom i cognoms de l'alumne dins l'eina de missatges del campus virtual, per poder identificar de forma inequívoca un alumne, tenint en compte el context del campus virtual.

Així mateix, es planteja (qüestió tercera) si aquesta eina de missatges del campus virtual estaria emparada per la Disposició addicional 21a, punt 3, de la Llei orgànica 4/2007, de 12 d'abril, per la que es modifica la Llei orgànica 6/2001, de 21 de desembre, d'Universitats, per una altra llei o si, en el seu cas, caldria el consentiment previ de l'alumne.

D'acord amb l'informe adjuntat a la consulta, aquesta eina de missatges del campus virtual permet enviar missatges entre professors i alumnes i entre els propis alumnes, per tal de comunicar qualsevol aspecte relacionat amb l'assignatura, entregar treballs o comunicar qualsevol tipus d'informació o incidència.

Tot i que no s'esclareix si la comunicació es produeix en un àmbit privat –al qual només tindria accés la persona que envia o rep el missatge- o bé si aquesta eina funciona d'una manera similar a la corresponent al debat i, per tant, la informació continguda en aquests missatges (cos i remitent) resulta accessible per a la resta de participants -en publicar-se en l'espai de l'assignatura del campus virtual-, dels termes en què es formula la consulta es desprèn que, efectivament, ens trobem davant d'aquest darrer cas.

En aquest sentit, cal assenyalar que la publicació de la dada personal DNI, en els termes indicats, dins l'espai de missatges del campus virtual al costat del nom i cognoms d'un alumne constitueix, des del punt de vista de la protecció de dades, una

comunicació o cessió (article 3.i) LOPD), atès que comporta revelar aquesta dada a tercers persones (els estudiants i/o professors) diferents del seu titular.

D'acord amb el règim general aplicable a les comunicacions o cessions de dades, per a que aquesta cessió (la publicació) sigui conforme amb la normativa de protecció de dades personals cal comptar amb el consentiment previ de l'afectat (article 11.1 LOPD) o bé amb una norma amb rang de llei que l'habiliti (article 11.2.a) LOPD).

En aquest cas, davant la manca de consentiment dels afectats, cal examinar si aquesta cessió, com s'assenyala en l'escrit de consulta, podria estar emparada per la Disposició addicional 21a, punt 3, de la Llei orgànica 4/2007, de 12 d'abril, per la que es modifica la Llei orgànica 6/2001, de 21 de desembre, d'Universitats. Aquesta disposició estableix que:

“1. Lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, será de aplicación al tratamiento y cesión de datos derivados de lo dispuesto en esta Ley Orgánica.

Las universidades deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados.

2. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido de los currículos a los que se refieren los artículos 57.2 y 62.3.

3. No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación.

4. Igualmente no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación.

5. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido académico y científico de los currículos de los profesores e investigadores que las universidades y las agencias o instituciones públicas de evaluación académica y científica pueden hacer público, no siendo preciso en este caso el consentimiento previo de los profesores o investigadores.”

Així, d'acord amb aquesta disposició i, en concret, amb allò establert a l'apartat 3, la llei només habilitaria la publicació, sense consentiment dels estudiants, dels resultats de les proves d'avaluació i dels actes necessaris per fer-ne l'avaluació (exàmens, treballs, etc.) però no així del número del DNI junt amb el nom i cognoms, atès que la seva publicació no sembla perseguir aquesta finalitat.

La Universitat manté que la finalitat per la qual es vol publicar aquest número junt amb el nom i cognom dels estudiants a l'espai de missatges del campus virtual és poder identificar de forma inequívoca un alumne.

Si bé, amb caràcter general, el compliment d'aquesta finalitat d'identificació no requereix fer públic el número corresponent al DNI de l'alumne, atès que, de conformitat amb el principi de qualitat de les dades (article 4.1 LOPD), es considera suficient en aquests casos publicar només el nom i cognoms dels alumnes, s'entén que només en l'eventual cas que dos participants tinguin el mateix nom i cognoms pot ser convenient introduir alguna informació addicional per tal de diferenciar-los. En

aquest sentit, l'Autoritat ha proposat en dictàmens anteriors (per exemple, CNS 20/2011 o l'esmentat CNS 28/2011) que es podria emprar el número del DNI però sense incloure, per exemple, les quatre darreres xifres.

En el cas examinat, la Universitat afirma que actualment hi ha dos alumnes matriculats en una mateixa assignatura que comparteixen els mateixos noms i cognoms. Per evitar problemes en la seva identificació, plantegen publicar, en concret, la lletra del NIF i els 7 primers dígit del DNI.

Tal i com s'ha posat de relleu anteriorment, la facilitat per esbrinar la darrera xifra d'aquest número i el fet que coincideixi plenament amb el login que s'utilitzaria per accedir al campus virtual, desaconsellaria la seva publicació en aquest espai de missatges junt amb el nom i cognoms dels alumnes. Per aquest motiu, caldria optar per publicar aquesta dada, com s'ha avançat, sense les quatre darreres xifres o bé emprar altre tipus d'informació addicional.

A tall d'exemple, la Universitat en el moment en què l'alumne accedeix per primer cop al campus virtual podria donar-li l'opció de configurar la seva informació personal afegint-hi un pseudònim o, fins i tot, una imatge –que podria coincidir o no amb la seva imatge personal-, per tal que, en el cas que existeixi coincidència en el nom i cognoms amb un altre estudiant, sigui aquesta informació i no el número del DNI la que es publiqui a l'espai de missatges o a qualsevol altre espai del campus virtual en què sigui necessari.

Això, sens perjudici, és clar, del fet que la publicació plantejada (la lletra del NIF i els 7 primers dígit del DNI) es pugui dur a terme si es compta amb el consentiment previ, lliure, inequívoc, específic i informat dels estudiants (article 3.h) LOPD).

V

Finalment, en la consulta es planteja si, atès que la queixa de la persona interessada es centra en que el seu document d'identitat no figuri en el campus virtual, en cursos on hi intervenen persones alienes a la Universitat, té dret a que se li canviï el login només per aquests casos.

Pel que fa al fet que el número del DNI figuri o no en el campus virtual de la Universitat, cal fer avinent que, amb independència que en l'assignatura hi participin o no persones alienes a la Universitat, la publicació d'aquest número al costat del nom i cognoms d'un alumne dins els espais de l'assignatura que es desenvolupa en el campus virtual només es podria dur a terme, tal i com s'ha assenyalat en l'apartat anterior d'aquest dictamen, amb el consentiment previ de l'alumne o bé quan aquesta publicació sigui estrictament necessària per identificar inequívocament dos estudiants que comparteixen nom i cognoms i sempre que, com a mínim, aquest número es publiqui sense les darreres quatre xifres.

Per tant, tret que el nom i cognoms de la persona que ha plantejat la queixa coincideixin exactament amb els d'un altre estudiant d'aquell mateix curs o bé mentre que aquesta persona no manifesti el seu consentiment per a que el seu número de DNI es publiqui en el campus virtual, la Universitat no podrà publicar aquesta dada en no trobar habilitació en la Llei orgànica 6/2001, de 21 de desembre, d'Universitats.

D'altra banda, pel que fa a la possibilitat de canviar el login facilitat inicialment a l'estudiant, cal fer avinent que qualsevol participant del campus virtual té dret a que se

li atorgui un login i una contrasenya segurs, de tal manera que només siguin coneguts per ell i no així per terceres persones.

Per tant, sempre que existeixen motius per pensar que la seguretat en l'accés al campus virtual es podria veure compromesa (per exemple, per pèrdua del login o de la contrasenya o perquè es creu que aquestes dades són o poden ser conegudes per altres persones) caldrà facilitar-li un nou login i/o contrasenya de manera immediata.

D'acord amb les consideracions fetes en aquest dictamen en relació amb la consulta plantejada, es fan les següents,

Conclusions

L'ús d'un sistema d'identificació i d'autenticació per accedir al campus virtual de la Universitat basat en un login, format per la lletra del NIF més els 7 primers dígit del DNI, i una contrasenya es considera un mecanisme adequat d'identificació i d'autenticació.

La publicació d'aquest login, junt amb el nom i cognoms d'un alumne, dins l'espai de missatges del campus virtual només és possible si es compta amb el consentiment de la persona afectada o bé es dóna el cas excepcional de que dos participants que estan matriculats en la mateixa assignatura comparteixen els mateixos noms i cognoms.

En aquest darrer cas, la publicació d'aquest número no es podrà dur a terme de manera íntegra, sent recomanable emprar les darreres quatre xifres, o bé optar per la utilització d'altres tipus d'identificadors.

Sempre que la seguretat en l'accés al campus virtual de la Universitat pugui veure's compromesa caldrà facilitar un nou login i/o contrasenya als participants d'aquest espai.

Barcelona, 13 de febrer de 2012