

La protecció de dades en els currículums professionals

Marina Llompart Carbó

NIUB: 15000020

Treball final de grau

Tutora del treball: Esther Mitjans

Grau de Relacions Laborals

Universitat de Barcelona

Curs 2014

ABREVIACIONS

AEPD.	Agencia Española de Protección de Datos
APDCAT	Autoritat Catalana de Protecció de Dades
art.	article
CE	Comissió Europea
CV	Currículum vitae
DLeg / DLgs	Decret Legislatiu
ETT	Empresa de treball temporal
FJ	Fonament jurídic
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal fruit de la transposició de la Directiva 95/46/CE.
RLOPD	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
RRHH	Recursos Humanos
STC	Sentència del Tribunal Constitucional

Índex

JUSTIFICACIÓ	3
LA PROTECCIÓ DADES; PER QUÈ SORGEIX LA NECESSITAT D'UNA NORMATIVA	5
<i>La protecció de dades com a disciplina jurídica</i>	5
Principis de la protecció de dades.....	5
<i>El marc jurídic espanyol</i>	7
<i>Influència de l'evolució tecnològica</i>	8
<i>L'ús de la informació i les xarxes socials</i>	10
Informació personal en les xarxes socials.....	10
L'ús de les xarxes socials per a la recerca de feina.....	11
LA PROTECCIÓ DE DADES EN ELS CURRÍCULUMS PROFESSIONALS	13
<i>El Currículum vitae i la seva protecció</i>	14
<i>La creació de fitxers i les mesures de seguretat</i>	17
Mesures de seguretat.....	19
<i>Drets d'accés, rectificació, cancel·lació i oposició de les dades</i>	23
<i>Conflictes habituals</i>	25
La recepció massiva de currículums.....	25
La manca d'informació per part de l'empresari.....	27
La manca de destrucció dels documents.....	28
<i>Cas italià</i>	29
CONCLUSIONS I PROPOSTES DE SOLUCIÓ	31
BIBLIOGRAFIA	35
ANNEX	37
<i>Annex 1</i>	37
<i>Annex 2</i>	37
<i>Annex 3</i>	37

JUSTIFICACIÓ

La majoria de nosaltres no som conscients de la gran quantitat d'informació personal que posem a disposició de diferents empreses quan lliurem o enviem un Currículum vitae, i del problema que això pot suposar per a la nostra privacitat.

Des de principis de segle la innovació tecnològica ha disparat la circulació i la transferència de dades de caràcter personal via Internet i el Currículum vitae és un dels instruments que permet aquesta cessió de dades personals. Però el perill no està només en l'enviament de informació per les xarxes, sinó també del lliurement en mà d'aquest document.

L'objectiu principal d'aquest treball és trobar una possible solució a la manca d'informació que crec que es rep a l'hora de lliurar un currículum en mà. La decisió del tema la vaig prendre a partir de l'experiència de pràctiques extracurriculars en una empresa de treball temporal (E.T.T). En l'empresa on vaig estar, només s'acceptaven els currículums en paper i tot i que la pàgina web tenia un apartat per a l'enviament de currículums, només eren acceptats els que es lliuraven a la recepció de l'oficina. Sempre em va quedar el dubte de què passava amb els currículums que la gent enviava mitjançant la pàgina web i que un cop trucaven a l'oficina se'ls informava que només eren vàlids els lliurats en persona.

La meva funció era atendre les persones que venien a l'oficina a lliurar currículums o a informar-se de quin tipus de serveis portava l'empresa. Cada dia rebíem més d'una desena de currículums, que acabaven en un piló i que no eren revisats setmanalment. La meva curiositat va començar ja a les poques setmanes d'estar allà, quan em vaig anar adonant que quan una persona em lliurava el seu currículum només li deia "Moltes gràcies, si surt alguna cosa ja t'avisaran" i el paper quedava apilonat amb tota la resta.

Aleshores ja m'havia començat a informar sobre la protecció de dades i havia estat revisant la normativa. A mesura que passaven els dies vaig ser conscient dels molts drets que tenim les persones en quant a les nostres dades personals i al dret a la intimitat i que en aquella empresa, com ben segur en la gran majoria, molts drets s'incomplien. El dret a informació sobre el tractament de les dades és el que em va fer relacionar més quin era el problema amb el que em trobava cada dia, i allà va començar la meva preocupació.

Cada dia seguia rebent currículums sense informar les persones sobre quin tractament rebria el document que em lliuraven i alhora era conscient de la falta de preocupació de les persones, i la falta de coneixement d'aquests, sobre els seus drets en quant a protecció de les dades personals.

D'altra banda, vaig estar preguntant als treballadors que tractaven aquestes dades què passava amb aquella pila de papers i què en feien dels que no els interessaven, però no vaig obtenir una resposta clara ni vaig saber qui n'era el responsable.

Així doncs, vaig decidir centrar el meu treball en aquesta matèria, amb la intenció de conèixer més la normativa, trobar si hi ha buits legals i saber quines són les conseqüències d'aquesta falta d'informació a les persones quan lliuren el seu currículum en mà, amb la intenció de proposar una possible solució per aquest problema.

LA PROTECCIÓ DADES; PER QUÈ SORGEIX LA NECESSITAT D'UNA NORMATIVA

La protecció de dades com a disciplina jurídica

La protecció de dades és una disciplina jurídica que fa referència al dret fonamental de les persones a la privacitat enfront el risc que suposa la recopilació i l'ús indiscriminat de les seves dades personals. Està jurídicament considerada pel Tribunal Constitucional com un dret fonamental autònom i independent del dret a la intimitat personal i familiar (STC 292/2000). Quan cedeixes les teves dades personals a una organització, aquesta té el deure de mantenir-les de forma privada i segura. Aquest procés es coneix com la protecció de dades.

Segons l'article 1 de la Llei Orgànica 4/2000 de Protecció de Dades de Caràcter Personal, d'ara en endavant LOPD, aquesta té per objecte garantir i protegir les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, especialment el seu honor, la seva intimitat personal i familiar. Bàsicament, tot fitxer que emmagatzemi dades personals de persones físiques identificades o identificables, ha de tenir un tractament sotmès als principis i requisits que s'han establert.

La Directiva 95/46/CE, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la seva lliure circulació, dóna la següent definició de les dades personals inclosa en la lletra a) de l'article 2: "Toda información sobre una persona física identificada o identificable (el «interesado») se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente [...] mediante elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Principis de la protecció de dades

El Títol II de LOPD¹ estableix diversos principis de la protecció de dades. Els principis són les condicions generals sota les quals el responsable dels fitxers ha de recollir, tractar i cedir les dades per garantir la intimitat de les persones; la lletra c) de l'article 3 de la LOPD defineix el tractament de dades personals com: "Todas las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación,

¹ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín oficial del Estado*. Núm. 298. Articles 4- 6.

conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones y transferencias”.

Els principis inclouen la qualitat de les dades –principi pel qual només es podran recollir i tractar les dades de caràcter personal quan siguin adequades, pertinents i no excessives i per a les finalitats determinades, explícites i legítimes per a les quals s’han obtingut–; la cancel·lació dels fitxers que contenen dades personals quan deixin de ser necessaris per a la finalitat per a la qual s’havien creat, impedit així la identificació del interessat per un període superior al necessari (finalitat concreta); la previsió d’informació prèvia a l’interessat sobre l’existència d’un fitxer de dades de caràcter personal i de la identitat i direcció del responsable del seu tractament; i l’obtenció del seu consentiment per al tractament de les dades.

Són principis d’obligat compliment, ja que són la base de tot tractament de dades personals. És per això, que és fonamental que siguin coneguts per totes aquelles persones que directament tractin amb la informació.

El marc jurídic espanyol

El marc jurídic bàsic que configura la protecció de dades de caràcter personal a Espanya està format per les següents normes:

- **Directiva 95/45/CE** del Parlament Europeu i del Consell del 24 d'octubre de 1995: constitueix el text de referència, a escala europea, en matèria de protecció de dades personals.

La Directiva fixa uns límits estrictes per a la recollida i utilització de les dades personals i sol·licita la creació, en cada Estat membre, d'un organisme nacional independent encarregat de la protecció de les dades.

- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal fruit de la transposició de la Directiva 95/46/CE.
- **Real Decreto 1720/2007**, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- **Instruccions de l'Agència Espanyola de Protecció de Dades** per adequar els tractaments als principis establerts per la LOPD.

L'AEPD no té una normativa específica sobre CV, però sí que ha fet unes recomanacions respecte de la selecció de personal, tot i que centrat en internet.

Influència de l'evolució tecnològica

És vist que les normes jurídiques sorgeixen a conseqüència d'una necessitat social, el que fa del dret una fórmula de solucionar conflictes². La necessitat d'una regulació jurídica al respecte de la protecció de dades sorgeix quan el seu ús pot ser lesiu de drets, i és que la majoria de nosaltres donem poca importància a la protecció de tota aquella informació personal que proporcionem, i/o que no hauríem de donar a conèixer per a la nostra seguretat, encara que en alguns casos ens la requereixen per algun tràmit, bé sigui per sol·licitar feina, o per utilitzar serveis o complir certes condicions.

Per poder valorar amb exactitud la necessitat urgent de regular la qüestió de la protecció de dades vinculada a les noves tecnologies, cal tenir un coneixement suficient sobre quina ha estat l'evolució de la informàtica i com ha creat aquesta necessitat.

L'any 1935, el president nord-americà Roosevelt va crear la *Social Security Act*, una llei per vetllar pel benestar general, mitjançant l'establiment d'un sistema de prestacions per a la gent gran³ i amb la finalitat social d'actualitzar les dades relatives a treballadors. Va ser el primer gran repte de tractament de dades, però els mitjans tècnics de l'època no van permetre complir l'objectiu al cent per cent. Ara bé, si aquesta llei va evidenciar la necessitat de crear eines tècniques, el verdader impuls tècnic va arribar poc temps després, durant la II Guerra Mundial, quan els serveis militars britànics van construir el *Colossus* amb la finalitat de desxifrar els missatges secrets dels nazis, i l'any 1945 es va inventar el primer programa d'ordinador que podia realitzar operacions comptables.

A partir de 1950 es van introduir les primeres aplicacions civils de la informàtica: l'aplicació en sèrie del primer ordinador d'ús comercial (de la multinacional nord-americana *Remington Rand*). Els primers usos eren per fer operacions comptables així com per a les prediccions electorals. A Espanya els primers usos civils de la informàtica es donen el 1962 (RENFE) per a la gestió de personal, estadística i comptabilitat.

² Rebollo Delgado, Lucrecio, *Introducción a la Protección de Datos*, Madrid, Ed. Dykinson, S.L., 2006, pàg. 17.

³ Social Security Act. *The United States Social Security Administration* [en línia]. <<http://www.ssa.gov/history/>>

Anys més tard, el 1968 *IBM* va introduir el primer sistema de gestió de bases de dades relatives a persones, així com de comptabilitat. En aquest moment es despertà la primera reacció de preocupació per l'ús massiu de la informació i de la possible lesió de drets de les persones (dret a la intimitat) que la informàtica podia produir.

Durant els anys següents, amb l'avenç de la tecnologia, va anar incrementant-se l'interès per l'ús lesiu de la informàtica respecte els drets fonamentals, fins al punt de l'aparició en el Länder alemany de *Hessen*, de la primera norma que limitava l'ús de la informàtica, es tracta de la *Datenschutz*, de 7 d'octubre de 1970. Aquesta norma, juntament amb la *Data Lag* de Suècia el 1973, eren la plasmació jurídica de les pretensions anteriorment apuntades pel Consell d'Europa que va constituir, el 1967, una comissió consultiva per a l'estudi de les tecnologies de la informació i el grau de lesió d'aquestes sobre els drets de les persones. Anys després, el 1974 entrà en vigor als Estats Units la *Privacy Act*, la normativa més completa i millor estructurada jurídicament fins aleshores. És l'autèntica precursora de les actuals normes sobre la protecció de dades de caràcter personal.

Finalment, l'avenç tecnològic més important es va produir el 1983 amb la creació d'INTERNET, que substituï l'ARPANET, la que va ser la primera connexió d'ordinadors a través de la línia telefònica que permetia la transferència de dades, l'enviament de correu electrònic i la transferència d'arxius. Ambdues van coexistir fins el 1990. L'ús de la xarxa va fer que l'ordinador deixés de ser només una eina de treball i passés a ser un mitjà global d'intercanvi i comunicació de dades, potenciant el risc de lesió de drets fonamentals. Aquest fenomen provocà la necessitat d'una nova normativa, o la seva modificació, per la consciència de la internalització del problema i va requerir la intervenció de l'Estat i una legislació a nivell supranacional.

D'una banda, a nivell comunitari, i per la necessitat d'una normativa supranacional que unifiqués la dispersió legislativa, va sorgir la *Directiva Europea 95/46/CE*. A nivell estatal es creà la *Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal* (LOPD), fruit de la transposició d'aquest text legal europeu.

L'ús de la informació i les xarxes socials

Actualment l'ús de les telecomunicacions possibilita la racionalització, la simplificació i la celeritat en el tractament de la informació. Independentment que les dades de caràcter personal hagin estat aportades directament per la persona, o generades en el si d'una organització, totes elles resulten útils i necessàries per executar les tasques que recauen sota l'àmbit de competència d'una organització. Aquesta informació esdevé summament valuosa per a qualsevol entitat; és un actiu intangible absolutament imprescindible.

La manca d'una deguda protecció de les dades personals pot derivar, també, en un acte de vulneració de l'honor i la intimitat de les persones, drets fonamentals protegits per la Constitució Espanyola en el seu article 18.4⁴. És per aquest motiu que el tractament de les dades personals deriva en la ineludible obligació de l'entitat d'adoptar totes aquelles mesures de caire jurídic, organitzatiu i tècnic, per garantir-ne la seguretat. La LOPD i posteriorment el *Reial Decret 1720/2007 de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal* (d'ara en endavant RLOPD) persegueixen aquest objectiu.

Informació personal en les xarxes socials

L'aparició de les xarxes socials ha tingut una gran influència en l'ús de la informació per la facilitat d'accedir a les dades de les persones que no tenen un bon control de la privacitat i ha influenciat les empreses a l'hora de seleccionar personal. Cal, però, tenir en compte que no tota la informació disponible en les xarxes socials és utilitzable i que tenir accés a aquestes dades no implica que tinguem dret a utilitzar-les, i és que no totes les xarxes socials són iguals. Cal diferenciar entre les professionals i les generalistes o d'oci.

El desconeixement del seu funcionament pot conduir la persona a la falsa convicció que interactua de forma anònima. Les xarxes socials generalistes o d'oci compten amb un nivell de risc superior al de les xarxes socials professionals (formació, experiència laboral) i, a més, permeten exposar de manera pública vivències, gustos o ideologies, fet que comporta la posada a disposició al públic de tot tipus de dades personals,

⁴ Constitución Española. *Boletín oficial del Estado*, 29 de diciembre de 1978. Núm. 311. Artículo 18.4.: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

sobretot dades especialment protegides. Això suposa un alt risc per a la protecció de les dades en l'àmbit de la privacitat i la intimitat de la persona, de tal manera que és molt important tenir un bon coneixement de la privacitat de les xarxes socials per evitar que terceres persones, incloses aquí les empreses, puguin obtenir informació nostra sense el nostre consentiment, perquè la finalitat de la publicació de dades personals és el tractament d'aquestes dades.

En efecte, quan publiquem dades personals s'entén que les publiquem perquè volem que puguin ser tractades i vistes pel altres, però quan aquesta finalitat no coincideix amb la nostra (com quan una empresa aconsegueix informació personal sense haver estat aportada directament per la persona) no s'hauria de fonamentar cap decisió en el procés de selecció de personal. Si no es compta amb el consentiment per a una finalitat concreta, no es pot utilitzar aquesta informació i constitueix una mala praxi professional i una pràctica sancionable per vulnerar la LOPD, sempre tenint en compte que si les fonts són accessibles al públic poden consultar-se sense previ avís però informant la persona sobre aquesta consulta.

L'ús de les xarxes socials per a la recerca de feina

El tema central d'aquest treball és el lliurement de currículums en mà, però convé primer mencionar la recerca de feina via el món virtual per entendre les diferències entres aquestes dues vies.

El mètode de recerca de feina que més s'ha popularitzat és via pàgines web de recerca de treball. Avui en dia internet és una eina indispensable i en matèria d'ofertes de treball ha agilitzat els processos de recepció de candidats així com el d'oferir llocs de treball. Internet ha permès intercanviar dades de forma ràpida i connectar ocupadors i candidats actuant com a intermediari, però aquesta visió idealista s'esfuma quan es parla del tractament de dades de caràcter personal i és que en aquests llocs web s'hi recullen moltes dades personals que permeten elaborar un perfil ajustat dels candidats.

Per la selecció de personal a través d'internet, l'*Agencia Española de Protección de Datos*, d'ara en endavant AEPD, va redactar un informe l'any 2005⁵ que aclareix dubtes sobre la seguretat, i inseguretat, de les dades personals que circulen per internet i hi fa recomanacions. Però parlem d'un informe de l'any 2005 i l'ús de xarxes socials o de les pàgines web professionals i la situació laboral han canviat molt des

⁵ *Informe de conclusiones y recomendaciones de la sobre selección de personal a través de Internet. Agencia Española de Protección de Datos; 17 de noviembre del 2005.*

d'aleshores per tant, caldria actualitzar-lo. Tot i així, és important que en el seu moment l'AEPD reaccionés davant el fenomen d'expansió de l'ús de les xarxes socials en l'àmbit laboral.

Breument, cal fer esment del mètode d'informació sobre la protecció de dades en el món digital. Com ja hem vist, el dret a la protecció de dades té uns principis que ha de complir i per tant, tota organització que reculli dades personals ha de tenir una política de privacitat que tingui uns objectius bàsics que fonamentalment seran garantir la confidencialitat, integritat i disponibilitat de les dades, i quin ús se'ls donarà. Quan es tracta de llocs web, aquesta ha d'estar en un apartat ben identificat i accessible. Quan l'empresa reuneixi aquests requisits sabrem, en principi, que és creïble i de confiança.

Una bona política de privacitat ha de descriure quin és l'objecte de l'empresa, quins serveis ofereix, les obligacions per l'usuari/a i de l'empresa, com es recullen les dades i per a quina finalitat, quin és el dret d'informació per a l'usuari/a, on es guarden i quin ús es farà de la informació recollida així com les mesures de seguretat que es prenen, ja que, en proporcionar dades personals implica l'acceptació d'aquesta.

Així, doncs, tota política de privacitat ha d'estar en conformitat amb el que disposa la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal i la seva normativa de desenvolupament (el Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999).

LA PROTECCIÓN DE DADES EN ELS CURRÍCULUMS PROFESSIONALS

Fins ara ens hem introduït en matèria veient que la protecció de dades és una disciplina jurídica que fa referència al dret fonamental de les persones a la privacitat enfront el risc que suposa la recopilació i l'ús indiscriminat de les seves dades personals, i que el sorgiment d'una normativa ha estat causa de la influència de l'evolució tecnològica. Però el tema central d'aquest treball és la protecció de dades i en concret les que conté un Currículum vitae.

D'entrada veurem què és un currículum i per què necessita que les dades que conté estiguin protegides, així com tot el procediment i mesures de protecció necessàries per complir amb la normativa. Tot i l'existència de diversos formats de currículum, en particular m'interessa centrar-me en aquells que lliurem en paper directament a l'empresa.

En darrer lloc, i a fi de treure'n una conclusió, compararem allò regulat en la legislació espanyola amb els conflictes més habituals que ens trobem actualment en parlar de currículums vitae lliurats en paper per tal de trobar els principals problemes que existeixen i pensar en una possible solució.

El Currículum vitae i la seva protecció

El concepte *Currículum vitae* prové del llatí i significa “carrera de la vida”. En l’actualitat, el concepte Currículum vitae, d’ara en endavant CV, es refereix a un document que conté la informació personal i professional d’una persona on destaca tot allò positiu i valuós de la seva experiència per poder presentar una candidatura per ocupar un lloc de treball. És, doncs, un dels primers elements que l’empresari rep en relació amb la persona que busca feina i se sol utilitzar per a la selecció dels candidats, sovint seguit d’una entrevista per verificar les dades o conèixer més el candidat.

Els currículums contenen dades de caràcter personal que estan subjectes a la LOPD. Generalment inclouen informació de l’interessat referent a dades personals, formació acadèmica i complementària, experiència professional, idiomes, informàtica o altres dades d’interès, tals com la disponibilitat horària, aficions, qualitats i aptituds, etc. Com ja s’ha esmentat anteriorment, l’Agencia Española de Protección de Datos (AEPD) va emetre el 2005 un *Informe de conclusiones y recomendaciones de la AEPD sobre selección de personal a través de Internet* on en el seu apartat 6.7, paràgraf 2n, es referia al CV de la forma següent: “Un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo”, expressió repetida en diverses sentències de l’Audiència Nacional, considerant els currículums com un conjunt de dades suficients per valorar la personalitat d’un individu i no només la seva capacitació professional i que, per tant, necessiten ser protegits en ser un dret de la persona.

Aquest dret a la impugnació de valoracions està regulat a l’article 13 LOPD, pel qual els ciutadans tenen dret a no veure’s sotmesos a decisions amb efectes jurídics basades en un tractament de dades destinat a avaluar determinats aspectes de la seva personalitat. Aquestes decisions privades que impliquin una valoració de la personalitat de la persona, l’únic fonament de les quals sigui un tractament de les dades que ofereixi una definició de les seves característiques o personalitat, podran ser impugnades. Ara bé, en la selecció de currículums és molt difícil que la persona afectada arribi a saber si el seu CV ha patit aquest tractament.

L’article 7 LOPD ens parla sobre les dades especialment protegides –referides a la ideologia, la religió, creences de la persona, origen racial, dades sanitàries o de la vida sexual–, que tenen una protecció especial i el seu emmagatzematge està prohibit. No és gaire comú veure dades d’aquest tipus en un CV, però les empreses podrien trobar-se en aquesta situació.

La protecció de les dades que ens aporten els currículums està subjecte als principis de la protecció de dades de la LOPD. Entre aquests principis, esmentats anteriorment, cal destacar el principi de la finalitat concreta, aplicable en el CV, ja que, a cada organització a qui proporcionem el nostre CV, el lliurement d'aquest té una finalitat determinada de ser escollits per ocupar un lloc de treball, i per tant, el tractament de les dades que inclou només podrà estar destinat a aquesta fi.

Els principis d'informació a l'interessat i petició del seu consentiment per al tractament de la dades, estan molt relacionats entre si. La regla general és que per poder donar tractament a les dades d'una persona, sempre tenint en compte el principi de la finalitat concreta, s'ha de sol·licitar a l'interessat el seu consentiment. L'article 6 LOPD estableix que el seu tractament requereix el consentiment inequívoc de l'afectat, però la LOPD preveu excepcions a aquesta petició, com el de l'apartat 2 del mateix article, pel qual "no será preciso el consentimiento cuando los datos que se recojan (...) se refiera a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa i sean necesarios para su mantenimiento o cumplimiento". No obstant això, el fet de no precisar el consentiment dels interessats per poder tractar les seves dades personals no treu que l'empresa hagi de complir amb el deure d'informació de l'article 5 LOPD. Així, doncs, segons aquest article, l'empresa haurà d'informar al treballador/a:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".

De tal manera que qui tracta amb informació aliena per oferir un lloc de treball tindrà l'obligació d'informar sobre el tractament de les dades. Així mateix, el tractament de dades sense el consentiment dels afectats constituirà un límit al dret fonamental a la protecció de dades.

Aquest dret, en paraules del Tribunal Constitucional en la seva Sentència 292/2000, de 30/11 (FJ. 7 primer paràgraf):

“consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular”.

En definitiva, el CV és un document que requereix una protecció especial pel sol fet de ser un resum de dades identificadores i professionals d'una persona a través de les quals proporciona una gran quantitat d'informació personal, i això és comprensible quan l'acció que ha de dur a terme l'empresa és la de filtrar i avaluar candidatures per facilitar la recerca del candidat més adequat.

La creació de fitxers i les mesures de seguretat

Des del moment en què rebem un currículum hem de decidir si es conserva per a possibles seleccions de personal o si el destruïm. La recepció d'aquest pot ser en mà o via online a través d'una pàgina web o un correu electrònic. Si es decideix guardarlo, bé en un arxivador (CV en paper), bé en una safata del nostre gestor de correu electrònic, estem tractant dades personals, de manera que ens veiem en l'obligació d'aplicar les mesures de seguretat tècniques, legals i organitzatives per protegir aquestes dades personals. Des del moment en què una empresa decideix guardar un CV es posa en marxa tot el procediment de la LOPD. Si el CV no es guarda no es crearà un fitxer i si no hi ha fitxer amb dades de caràcter personal no serà d'aplicació la LOPD.

L'article 25 LOPD recull les condicions de la creació de fitxers de titularitat privada, els quals només podran ser creats quan resultin necessaris per assolir l'activitat o objectiu legítim de la persona, empresa o entitat titular i es respectin les garanties legals per a la protecció de les persones. Els currículums que es guarden constitueixen un fitxer de dades de caràcter personal a definir que s'ha de registrar a l'Agència de Protecció de Dades. En l'article 3.b) LOPD es considera un fitxer tot conjunt organitzat de dades de caràcter personal que identifiquen o que permeten identificar una persona. Serà suficient la mera existència d'un conjunt de dades personals organitzat de forma que permeti accedir-hi utilitzant un criteri determinat perquè legalment es consideri que estem davant d'un fitxer, independentment de la forma o modalitat de la seva creació, emmagatzematge, organització o accés, ja sigui de manera manual (fitxers no automatitzats) o a través de procediments informatitzats (fitxers automatitzats).

Cal diferenciar bé les dues modalitats de fitxer: els no automatitzats dels automatitzats. La principal diferència entre ambdós és el procediment d'emmagatzematge, d'organització i d'accés a les dades de caràcter personal que continguin.

Els fitxers no automatitzats estan definits legalment en l'article 5.1.n RLOPD com "todo conjunto de datos de carácter personal que permitan acceder sin esfuerzos desproporcionados a sus datos personales", és a dir, són fitxers d'arxius en format paper i que es gestionen i s'organitzen manualment en arxivadors sempre i que estiguin estructurats de manera que en faciliti la localització utilitzant criteris identificadors determinats. D'altra banda, són fitxers automatitzats tot conjunt de dades de caràcter personal organitzats de manera que es pugui accedir a les dades personals utilitzant qualsevol tipus de procediment informàtic (fitxers de currículums rebuts per correu electrònic).

El pas previ a la creació o modificació d'un fitxer és la seva notificació i és que l'article 26.1 de la LOPD assenyala que tota persona o entitat que procedeixi a la creació de fitxers de dades de caràcter personal ho notificarà prèviament a l'Agència de Protecció de Dades, és a dir, la notificació de fitxers és el procediment a través del qual la persona o entitat privada informa l'Agència de Protecció de Dades -l'Autoritat Catalana de Protecció de Dades, en el cas de Catalunya, o a l'AEPD, d'àmbit estatal- de la intenció de crear un fitxer de dades personals. És necessària la seva autorització.

Abans d'iniciar qualsevol tractament de dades personals, el responsable del fitxer ha de notificar el fitxer, sol·licitar-ne la inscripció al registre de protecció de dades corresponent i obtenir-ne la inscripció. El Registre de Protecció de Dades té com a finalitat fer efectiu el dret de tota persona a conèixer l'existència de tractaments de dades de caràcter personal, les seves finalitats i la identitat del responsable del fitxer, per tal de poder exercir davant seu els drets d'accés, rectificació, cancel·lació i oposició (drets ARCO). És un registre de consulta pública i gratuïta.

Quan el fitxer ja existeixi i hi hagi canvis respecte de la inscripció inicial, s'ha de fer la modificació al registre de protecció de dades corresponent. Si se cessa en l'ús del fitxer, aquest s'ha de suprimir. Per tant, la creació, la modificació o la supressió del fitxer comporta fer-ne la notificació i la sol·licitud d'inscripció al registre de protecció de dades corresponent.

En aquest punt adquireix una importància essencial la persona responsable del fitxer o del tractament. És responsable del fitxer o tractament aquella persona física i jurídica que decideix sobre la finalitat, contingut i ús del tractament⁶ i sobre el qual recau el compliment de gran part de les obligacions derivades de la llei, tals com el compliment dels principis de la protecció de dades. L'incompliment de la normativa, vulneració dels principis i garanties establerts en la LOPD, li serà atribuïble i pot ser constitutiu d'una infracció lleu, greu o molt greu.

En primer lloc, aquest responsable té l'obligació de recollir les dades de forma legal, adequada i pertinent, procurant no tenir més dades de les necessàries ni utilitzar-les per a les finalitats incompatibles amb les que en van motivar la seva recollida. Si les dades deixen de ser necessàries i pertinents per a la finalitat que va originar la seva recollida, les haurà de cancel·lar d'ofici (art.4.5 LOPD).

⁶ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín oficial del Estado*. Núm. 298. Article 3.d)

És també el responsable d'obtenir el consentiment inequívoc del interessat per a la recollida de dades i per iniciar el tractament (art.6 LOPD), així com d'informar els afectats sobre el deure d'informació de l'article 5 LOPD. És aconsellable conservar les proves que confirmin l'existència del dret d'informació per comprovar que el responsable del fitxer ha complert amb la seva obligació.

Mesures de seguretat

La seguretat de les dades constitueix un dels aspectes que formen part del contingut del dret fonamental a la protecció de dades. La seguretat es converteix en un element essencial en la protecció de les persones a través de la protecció de les seves dades i dels tractaments de les quals en formen part.⁷

L'article 9 de la LOPD disposa que el responsable del fitxer, i en el seu cas, l'encarregat del tractament, haurà d'adoptar les mesures d'índole tècnica i organitzativa necessàries per garantir la seguretat de les dades de caràcter personal i evitar-ne l'alteració, el tractament o l'accés no autoritzat.

El responsable doncs, té l'obligació d'elaborar un «document de seguretat» (art.88-89 RLOPD). Es tracta d'un document intern de l'empresa d'obligat compliment per a tot el personal que tingui accés a les dades i que recull la normativa sobre seguretat. Ha de mantenir-se sempre actualitzat i ha de contenir: una especificació detallada dels recursos que protegeix; quines són les mesures de seguretat i procediments estàndards per al seu nivell; una descripció dels fitxers i els sistemes d'informació; els procediments de notificació i resposta davant incidències; els procediments de còpies, recuperació de dades i els de destrucció de documents; i a més a més per a fitxers de nivell mitja o alt haurà d'identificar el responsable o responsables de la seguretat i els controls periòdics a realitzar per comprovar el compliment del document i les mesures a adoptar per a l'eliminació d'aquest.

Tots els fitxers o tractament de dades han d'adoptar les mesures de seguretat de nivell bàsic, però el CV està considerat pel RLOPD com un fitxer de nivell mitjà, en aplicació del seu article 81.2.f)⁸. Al poder obtenir una avaluació de la personalitat de la persona i

⁷ Rebollo Delgado, Lucrecio, *Introducción a la Protección de Datos*, Madrid, Ed. Dykinson, S.L, 2006, pàg. 139.

⁸ Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Artículo 81.2.f): "Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos."

crear-ne un perfil a partir de les dades, a més de les mesures de seguretat de nivell bàsic se'ls aplicaran les mesures de nivell mitjà.

En aquest sentit, sent exigible l'adopció de mesures de nivell mitjà, seran les establertes en el RLOPD. Vist que existeixen dos tipus de fitxers, els automatitzats i els no automatitzats, ambdós requeriran diferents mesures de seguretat.

Les mesures aplicables en fitxers i tractaments automatitzats estan regulades en el Capítol III del RLOPD. Com els fitxers de currículums són de nivell mitjà seran les de la Secció 2^a del mateix capítol. Cal recordar que són fitxers automatitzats els que s'organitzen mitjançant procediments informàtics.

Totes les obligacions i funcions dels usuaris amb accés a les dades de caràcter personal han d'estar clarament definides i documentades en el document de seguretat citat anteriorment. A causa que poden sorgir incidències que afectin les dades ha d'existir un procediment de notificació i gestió d'aquestes establint-ne un registre on consti el tipus d'incidència, el moment en què s'ha produït o detectat, la persona que realitza la comunicació i a qui va dirigida, i els efectes derivats d'aquesta, així com les mesures correctores aplicades i el procés de restauració.

L'accés a les dades està només permès a aquells qui ho requereixin per al desenvolupament de les seves funcions i que estiguin autoritzats en el document de seguretat; és tasca del responsable del fitxer tenir actualitzada la llista d'usuaris amb dret d'accés així com d'establir mecanismes de control.

Quan el responsable del fitxer actua com a intermediari laboral (en aquest cas en empreses de treball temporal o en pàgines web de recerca de feina) els ocupadors seran considerats cessionaris i el responsable actuarà en qualitat d'encarregat del tractament. Però la realització d'aquest tractament per compte de tercers haurà d'estar regulat en un contracte escrit que estableixi expressament que l'encarregat del tractament només tractarà les dades conforme les instruccions dels responsable del tractament i no per a una finalitat distinta.⁹ Una vegada complerta la relació contractual, les dades o suports que en continguin hauran de ser destruïdes o retornades al seu responsable.

Els suports i documents que contenen dades de caràcter personal han de permetre identificar el tipus d'informació que contenen. S'ha d'establir un sistema de registre d'entrada de suports que permeti conèixer el tipus de document, la data i hora

⁹ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín oficial del Estado*. Núm. 298. Article 12.

d'entrada, l'emissor, el número de documents i tipus, la forma d'enviament i la persona responsable de la seva recepció que haurà d'estar degudament autoritzada. Igualment, hi haurà un registre per a la seva sortida; la seva sortida fora de locals sota el control del responsable del fitxer haurà d'estar degudament autoritzada en el document de seguretat i adoptant les mesures adequades per al seu trasllat per evitar-ne la sostracció, pèrdua o accés indegut a la informació.

S'han d'establir mecanismes per evitar la possibilitat d'intentar reiteradament l'accés no autoritzat. Per a la seva identificació s'utilitzaran sistemes d'etiquetatge comprensibles i identificables –sobretot en documents que continguin dades sensibles– per als usuaris amb accés autoritzat i que alhora dificultin la identificació a la resta de persones. Quan el mecanisme es basi en contrasenyes, aquestes es renovaran periòdicament i mai en un termini superior a un any.

En tractar-se d'un fitxer de nivell mitjà, els sistemes d'informació i totes els instal·lacions d'emmagatzematge i tractament de les dades, s'hauran de sotmetre a una auditoria, almenys cada dos anys, o menys si s'hi produeixen modificacions substancials, per verificar el compliment de les mesures de seguretat i proposar mesures correctores. Els informes d'auditoria seran analitzats pel responsable del fitxer o tractament perquè adopti les mesures correctores adequades i quedaran a disposició de l'Agència de protecció de dades. És també molt important establir procediments setmanals de còpies dels fitxers i procediments per a la recuperació de les dades per garantir, en tot moment, la seva reconstrucció en cas de pèrdua o destrucció no intencionada.

D'altra banda, les mesures aplicables en fitxers i tractaments no automatitzats de nivell mitjà estan regulades en el Capítol IV del RLOPD, Secció 2^a. Són fitxers automatitzats els currículums impresos en paper.

Per als fitxers no automatitzats de nivell mitjà, les mesures són molt més simples. Tal com per als fitxers automatitzats és necessari un registre d'incidències, controlar-ne l'accés i tenir una bona gestió dels suports i documents, però bàsicament es requereix la designació d'un o més responsables de seguretat que coordinin i controlin les mesures definides en el document de seguretat. A més a més, també se sotmetran, almenys cada dos anys, o menys si s'hi produeixen modificacions substancials, a una auditoria per verificar el compliment de les mesures.

Hem de tenir en compte que els CV en paper no sempre s'entreguen en mà, sinó que en algun cas poden ser enviats mitjançant el fax. En aquest cas, seria aconsellable que abans d'enviar-lo l'interessat fés un preavis de l'enviament i s'assegurés que l'empresa l'ha rebut i que aquesta té el fax en un lloc del local que no estigui a l'abast de tothom.

Vist que les mesures de seguretat de fitxers no automatitzats són més senzilles, una proposta seria l'ús d'etiquetes mitjançant la identificació per radiofreqüència o RFID (*Radio Frequency IDentification*). És un sistema que permet identificar un objecte gràcies a una ona emissora incorporada a un producte. Per al control de fitxers que contenen CV, s'enganyarien al carpesà o document que els contingui. Aquestes etiquetes transmeten dades per radiofreqüència i, en aquest cas, permetrien controlar l'accés als documents i saber els moments en què l'arxiu ha estat obert.

Igualment, en els casos en què les etiquetes continguin informació personal o associada a persones físiques, serà aplicable la RLOPD.

Drets d'accés, rectificació, cancel·lació i oposició de les dades

Els drets Arco (accés, rectificació, cancel·lació i oposició) són el conjunt de drets a través dels quals la LOPD garanteix a les persones el poder de control sobre les seves dades personals. Són de caràcter personalíssim, per la qual cosa només els pot exercir la persona afectada directament o a través de representant voluntari acreditat vàlidament conforme a dret, o el seu representant legal quan l'afectat es troba en minoria d'edat o està declarat incapaç per exercir els seus drets.

Per al seu exercici és imprescindible que el responsable del fitxer posi a disposició del interessat, o a través d'una comunicació per escrit, la informació sobre el procediment per exercir els drets Arco a través d'un mitjà senzill i gratuït. En cap cas pot suposar un ingrés addicional per al responsable del tractament enfront el qual s'exerciten.

Els drets Arco estan regulats reglamentàriament en el Títol II, Capítol I del RLOPD.

El dret d'accés consisteix a permetre l'afectat de dirigir-se al responsable d'un fitxer per sol·licitar informació sobre les seves pròpies dades de caràcter personal que estan sent objecte de tractament, la finalitat del tractament, així com la informació sobre l'origen d'aquestes dades i les comunicacions realitzades o que es prevegi fer.

El dret de rectificació permet a l'interessat de requerir al responsable del fitxer que rectifiqui les dades quan resultin ser inexactes, incompletes, inadequades o excessives.

El dret d'oposició permet negar-se al tractament de les dades o anul·lar-lo.

El dret de cancel·lació de fitxers de currículums va lligat al dret a la seva destrucció. La cancel·lació permet la supressió de les dades que resultin ser inadequades o excessives, sens perjudici del deure de bloqueig conservant-les únicament a disposició de les Administracions públiques, Jutjats o Tribunals, per a l'atenció de possibles responsabilitats nascudes del tractament i durant el termini de prescripció que estigui establert¹⁰. Convé tenir en compte les consideracions del Consell d'Europa en l'article 14 de la seva Recomanació 2/1989, per la qual "los datos personales obtenidos a través de una solicitud de trabajado deberían borrarse tan pronto como se decida que, por lo que respecta, no se realizará una oferta de trabajo" i d'altra banda "cuando estos datos se hayan conservado en vista a un posterior proceso de selección, se tendrán que eliminar si el candidato lo solicita".

¹⁰ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín oficial del Estado*. Núm. 298. Article 16.3.

Aquest dret s'exerceix quan les dades, o fitxers, hagin deixat de ser necessaris o pertinents per a la finalitat per la que havien estat recollides o registrades –principi de la finalitat concreta– o quan l'ocupador resolgui negativament la sol·licitud, excepte que el sol·licitant expressi explícitament la seva voluntat en sentit contrari.

La LOPD regula que no poden ser conservats de forma que permetin la identificació de l'interessat durant un període superior al necessari i han de ser cancel·lats per pròpia iniciativa del responsable del fitxer o tractament (article 5.4 LOPD). Quan les dades hagin estat cedides, el responsable del fitxer ha de comunicar la cancel·lació de les dades al cessionari. Aquesta comunicació no requerirà cap comunicació alguna a l'interessat.

Per tant, sempre que es vulgui eliminar qualsevol tipus de fitxer que conté currículums s'haurà de procedir a la seva destrucció mitjançant l'adopció de mesures dirigides a evitar l'accés a la informació que contingui i a la seva possible recuperació posterior (article 92.4 RLOPD).

Conflictes habituals

La recepció massiva de currículums

Durant els últims anys, i per causa del creixent nombre de persones desocupades, moltes empreses han passat de buscar candidats per ocupar llocs de treballs a rebre'ls de manera espontània. Diàriament es van acumulant una gran quantitat de currículums en els departaments de RRHH, bé rebuts en paper, o bé per correu electrònic. Seria lògic, doncs, que el tipus d'empreses que rebessin més volum de currículums fossin les ETT, però des de fa uns anys i amb l'inici de la crisi, el tancament d'empreses o l'augment de contractes temporals enfront els indefinits, ha augmentat la recerca de treball i en conseqüència la circulació de CV i l'increment de la seva recepció per part d'empreses diferents a les ETT.

Un dels principals problemes amb els quals es troba una empresa en aquesta situació no és que molts persones vulguin treballar-hi, sinó en el document que aquestes els hi lliuren voluntàriament i que conté una gran quantitat de dades de caràcter personal, que en alguns casos poden ser dades sensibles especialment protegides, i que posen l'empresa en un compromís legal. I és que el sol fet de rebre un CV ja activa la legislació sobre protecció de dades (LOPD i RLOPD) i els procediments a seguir.

Aquesta desesperació per trobar feina ha portat les persones a oblidar-se dels seus drets quant a les dades personals i renunciar-hi, o simplement a ignorar que els tenen i no voler ni informar-se'n. Aquesta idea es manifesta en la disposició dels ciutadans a cedir el que sigui, a despreocupar-se dels seus drets per poder treballar i guanyar diners per alimentar-se i sobreviure. Aquests són els casos més extrems, però és una realitat que s'està vivint. Encara que el problema que aquí es tracta és la falta de protecció, el fet de repartir molts currículums és un inconvenient per aquella persona que busca feina perquè demostra la seva desesperació i dona la imatge de que no s'interessa per una àrea específica sinó que acceptarà "qualsevol feina".

És un fet que posa èmfasis en el pensament que "la privacitat és només per als rics", i es que només les persones que realment necessiten feina, sigui la que sigui, són les que reparteixen desenes de currículums, mentre que una persona ben assentada generalment trobarà feina a partir d'un contacte i no n'haurà repartit tants, o fins i tot cap ni un, i mantindrà la seva recerca en reserva.

En conseqüència, ens trobem amb la dificultat que les persones posin atenció a la falta de privacitat que poden tenir les seves dades personals o a la vulneració del dret d'informació de l'article 5 LOPD al estar vivint uns anys de crisi on la majoria de persones desocupades busquen feina desesperadament. Com ja hem dit, actualment la seva màxima preocupació és trobar una feina, sigui com sigui, sense ni tan sols pensar en la quantitat d'informació personal que estan repartint.

Aquesta falta de consciència i preocupació és comprensible, però té els seus riscos. Un CV té un gran valor econòmic i quasi ningú ho té en compte. Quan una persona redacta un CV hi inclou informació personal i professional, però molts cops es produeix un abús quan la persona inclou més informació de la que seria necessària per optar a un lloc de treball. L'abús es pot produir tant al redactar i emetre el CV voluntàriament – en aquest cas s'entén que les dades que remet ho fa de forma voluntària– així com a l'omplir formularis de dades en pàgines webs per crear el propi CV, en casos on les webs inclouen qüestionaris de preguntes per obtenir informacions més completes sobre la idoneïtat d'un candidat i la seva personalitat. Si no s'especifica quines dades són obligatòries i quines facultatives poden no complir amb el requisit d'adequació, pertinença i no excés de l'article 4.1 LOPD.

Incloure més informació de la requerida és un fenomen que es dona molt sovint i manifesta la falta de coneixement de les persones sobre els requisits per omplir un CV, però també sobre la normativa de protecció de dades i el seu dret a la intimitat en donar a conèixer massa informació personal. Són carències molt importants, però és molt difícil posar-hi solució per la falta d'interès d'exercir els drets que es tenen en l'avantposar les necessitats bàsiques.

La manca d'informació per part de l'empresari

Com hem vist, el primer moment del tractament de les dades personals és la recollida. Una recollida que requereix ser consentida per legitimar-ne el tractament. Com que el consentiment ha de ser degudament informat, en el moment de la recollida de les dades s'ha de complir amb la clàusula informativa de l'article 5 de la LOPD. Recordem el contingut d'aquest article:

“1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante”.

A diferència de l'enviament d'un CV via pàgines webs, on generalment s'inclou aquesta clàusula informativa, quan lliurem un CV en mà rara vegada rebrem informació sobre el tractament que donaran a les nostres dades. Ens trobem doncs enfront una vulneració d'aquest dret. L'article 44.1.c) de la LOPD qualifica com una infracció l'incompliment del deure d'informació a l'afectat sobre el tractament de les seves dades personals quan les dades són recopilades del mateix interessat.

Vist que generalment les persones desconeixem els nostres drets regulats per la normativa de protecció de dades i a la vegada no rebem informació per part de l'empresari, és comprensible doncs trobar-nos en aquesta situació d'incertesa, ja que sembla ser que la normativa espanyola tampoc ha tingut interès a regular aquestes carències de control sobre aquest dret d'informació. Però és ben cert que si preguntem a la gent del nostre voltant que si al lliurar un CV en paper els han informat sobre el tractament de les dades personals, la majoria d'ells diran que no, i a més a més, probablement comentaran que tampoc s'ho havien plantejat ni havien trobat a faltar aquesta informació.

Tanmateix, com hem vist en la introducció en la matèria, a diferència del lliurement en mà d'un CV, l'enviament online està més regularitzat, ja que generalment, compta amb una política de privacitat que informa el sol·licitant de feina sobre els seus drets.

Així, doncs, els problemes no són només el lliurement massiu de currículums, la falta de preocupació i ignorància, sinó sobretot la falta d'informació per voluntat pròpia de l'empresari que suposa una infracció de la LOPD.

La manca de destrucció dels documents

Un altre conflicte habitual, i de molta importància, sobretot econòmica, és la vulneració de l'obligació de destrucció dels currículums quan deixen de ser necessaris o quan es rebutgen.

Hem vist que el responsable dels fitxers que contenen dades personals té l'obligació de cancel·lar i destruir aquests fitxers, però aquesta obligació molts cops s'ha vulnerat. En diversos processos sancionadors instruïts per l'AEPD el fet denunciat ha estat l'aparició de currículums llençats en contenidors o pel carrer (PS/00525/2008 o E/03460/2010).

Aquest fet només pot passar amb els currículums en paper, és un dels perills que tenen. Aquesta falta de mesura de seguretat per part d'una empresa posa en perill la intimitat d'una persona si treu els fitxers del seu local sense les degudes mesures de seguretat i difonent dades personals fora de l'àmbit de l'entitat que en té la custòdia. És clar, doncs, que no només vulnera el dret a la intimitat, sinó que també incompleix amb les mesures de seguretat.

Per justificar-ho tornem a recórrer a la STC 292/2000, segons la qual "El derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, su uso y destino [...] que impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada".

Cas italià

Per comparar amb el cas espanyol, és interessant comentar que a Itàlia l'1 de gener de 2004 va entrar en vigor el *D.Lgs 196/2003* –actualment en espera de ser renovat–, un decret legislatiu sobre la protecció de dades titulat com el “Codi en matèria de protecció de les dades personals”.

Basant-se en l'article 13 d'aquesta norma, a Itàlia es va impulsar la idea que al final de tot CV s'havia de fer referència a aquest article per autoritzar el tractament de les pròpies dades del CV¹¹:

“Autorizzo il trattamento dei dati personali contenuti nel mio Curriculum Vitae in base art. 13 del D. Lgs 196/2003”

(Autoritzo el tractament de les dades personals del meu Curriculum Vitae en base a l'art. 13 del D. Lgs 196/2003)

Aquest article 13 (equivalent a l'article 5 LOPD en el cas espanyol) diu el següent:

“Art. 13 (Informativa)

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

- a) le finalita' e le modalita' del trattamento cui sono destinati i dati;
- b) la natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualita' di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- e) i diritti di cui all'articolo 7;
- f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato piu' responsabili e' indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalita' attraverso le quali e' conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando e' stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, e' indicato tale responsabile.”

¹¹ Vegeu Annex 1. Exemple de Curriculum vitae amb inclusió de l'autorització.

Versió en català:

“Art. 13 (Informativa)

1. L'interessat o persona de la qual es recullen les dades de caràcter personal han de ser informats amb anterioritat oralment o per escrit sobre:

- a) l'objecte i la manera com seran processades aquestes;
- b) el caràcter obligatori o voluntari de l'atorgament de les dades sol·licitades;
- c) les conseqüències d'una eventual negativa a respondre;
- d) els subjectes o categories de subjectes als quals les dades personals poden ser comunicades o que les poden arribar a conèixer com a gestors o agents, i l'abast de la difusió d'aquestes dades;
- e) els drets previstos en l'article 7;
- f) la identitat del titular i, si ha estat nomenat, del representant a l'Estat pel que fa a l'article 5 i al responsable. Quan el titular ha designat més gestors i se n'ha indicat almenys un, indicant el lloc a la xarxa de comunicacions o la modalitat a través de la qual es pot accedir fàcilment a la llista actualitzada dels responsables. Quan ha estat designat un responsable per al retorn a l'interessat en cas d'exercici dels drets previstos a l'article , i ha estat indicat aquest responsable.

És interessant comentar aquesta idea, ja que tot i que la normativa no especifica la inclusió d'aquesta autorització és una pràctica molt comuna i a diferència del que sembla ocórrer a l'Estat espanyol, a Itàlia es van preocupar del dret de tota persona a donar el consentiment sobre el tractament de les seves dades personals. Però tot i que a priori sembla una bona idea que en tot CV la mateixa persona autoritzi el tractament d'aquestes dades, aquesta autorització ha estat molt criticada, perquè molts cops s'introduïa la clàusula en formularis prèviament impresos per les empreses i que els candidats havien de completar.

Un problema que es pot trobar en aquesta pràctica, on són els mateixos candidats els qui presenten de forma espontània l'autorització de tractament, és també la falta d'informació, ja que només amb aquesta citació una empresa no s'assegura que el candidat/a conegui la normativa i encara menys que conegui el propòsit de l'empresa sobre el tractament de les seves dades personals. També és un problema la falta d'especificació de la finalitat del tractament pel qual un dóna el seu consentiment, ja que s'entén que el candidat dóna el consentiment per a qualsevol tipus de finalitat. És per això que una possible solució seria que les finalitats estiguessin especificades en aquesta autorització i que, davant qualsevol canvi, es requerís novament el consentiment.

Així, doncs, sembla una bona pràctica sempre que es trobés la manera de comprovar que la persona que lliura el currículum està ben informada sobre els seus drets, ja que la sola citació d'aquest article només pot assegurar el coneixement de la normativa, però no dóna informació sobre el tractament de les dades i les mesures de seguretat que cada empresa decideixi aplicar, sempre complint la norma.

CONCLUSIONS I PROPOSTES DE SOLUCIÓ

Recollint el més important, sembla que els currículums en paper que es donen en el món físic espanyol tenen manca de regulació. Per poder donar forma al treball, he buscat en la legislació espanyola tot allò que tingués relació amb la protecció de dades, i concretament en la protecció de dades dels CV, però després d'analitzar-la no he trobat cap tipus de normativa que reguli aquesta matèria en concret, a diferència de la videovigilància, per exemple.

He vist que en la normativa general sobre protecció de dades (LOPD i RLOPD) en cap moment s'especifica un procediment per al tractament i la protecció d'un CV en paper, A més a més, tal com l'AEPD ha prestat atenció a l'augment de la recerca de feina per internet, redactant un informe de recomanacions sobre aquesta matèria, crec que ha deixat de banda el lliurement en mà.

Des del meu punt de vista, aprofitant que l'AEPD té capacitat per dictar instruccions amb caràcter normatiu, hauria de dictar una instrucció específica sobre CV, prestant atenció als CV en paper, perquè totes les empreses complissin amb els drets, deures i procediments regulats en la normativa, ja que tot el que s'ha citat en aquest treball és aplicable a un CV, però en el dia a dia no s'aplica en la seva totalitat.

L'objectiu principal d'aquest treball era trobar una possible solució a aquesta manca d'informació que rebem a l'hora de lliurar un currículum en mà i, analitzant la situació actual, he trobat més buits legals en la protecció dels CV en paper, com la vulneració de l'article 5 de la LOPD, l'article 18 RLOPD –sobre l'acreditació del compliment del deure d'informació– i, a més a més, no es donen garanties respecte de la donació del consentiment per a altres finalitats – si és per a una feina concreta o per a qualsevol–, més enllà de les que puguin estar especificades en la recollida.

Per això, l'empresa hauria de fixar uns procediments d'informació que suposessin la confirmació, per part del candidat/da, de conèixer les condicions en les quals es desenvoluparà el tractament de les seves dades personals. Quan l'empresa decideix quedar-se amb el CV per a possibles seleccions de personals, en el moment del lliurament és molt important informar a l'interessat de la creació d'un fitxer que conté els CV i les seves mesures de seguretat. Però sovint les persones no saben que poden accedir al Registre General de Protecció de Dades de l'AEPD per conèixer si les empreses notifiquen el fitxer, la recollida de dades amb els CV (vegeu pàg. 17 i ss.) i si empren correctament les mesures de seguretat adients segons el tipus de fitxer (en

el text fax, RFID, etc.). En cas contrari, si decideix desfer-se'n, el CV en paper haurà de ser destruït per una destructora de documents i demanar un certificat al respecte.

En relació amb la petició de destrucció d'aquests CV, o amb la cancel·lació per fi de la relació laboral, conforme els principis de la protecció de dades serà essencial que aquells que tractin amb les dades respectin el deure de secret sobre el contingut dels documents, fins i tot un cop acabada la relació laboral o negada l'acceptació del CV, ja que suposa una obligació perpètua de secret.

Tal com hem vist, consentiment i informació són coses diferents, tot i que relacionades, i per tant les persones encara que voluntàriament hagin enviat el CV han de ser informades dels drets de l'article 5 de la LOPD, si bé és cert que habitualment no podrà realitzar-se amb anterioritat a la recepció de les dades, si no és que l'empresa té un mitjà articulat per a això.

Així, doncs, proposo que seria bo obligar les empreses a lliurar una notificació de la recepció del CV en paper (vegeu Annex 3) i establir una pràctica per la qual el receptor només acceptés el CV si es firma un document de lliurement amb la clàusula informativa.

El contingut d'aquesta notificació hauria de ser tota aquella informació referent al tractament que rebran les dades proporcionades, informació de l'empresa receptora, les finalitats concretes del tractament i els drets que pot exercir la persona quant a les seves dades.

D'altra banda, també seria una bona praxi incloure una clàusula al final de cada pàgina d'un CV, com en molts CV d'Itàlia, ja que això permetria que si els papers se separessin quedés evidenciat que la informació continguda en cada paper requereix d'un consentiment per ser tractada. Com s'ha vist en el cas italià, seria bo que en aquesta pràctica la persona informés per a quin tractament dóna el consentiment.

Per tant, un cop vista la normativa i plantejats els problemes més habituals quant als currículums vitae en paper, podem dir que si l'empresa té un bon mètode de recollida de currículums i es preocupa d'informar les persones adequadament, tindrà la seguretat d'estar complint amb la normativa vigent.

Tal com he dit en la justificació, el motiu pel qual vaig escollir investigar sobre la protecció de dades en els currículums vitae en paper va ser fruit d'una experiència laboral que em va inspirar per poder fer aquest treball. Després d'analitzar la normativa

espanyola sobre protecció de dades en la matèria en la qual m'he centrat m'he adonat que, en aquest sentit, encara queda molt per fer i que el món físic s'ha deixat de banda per donar pas al món virtual. Penso que això s'ha reflectit molt en el fet que l'AEPD, a part de la manca de legislació, s'ha preocupat per fer recomanacions sobre l'ús d'internet, i ha oblidat que molts processos de selecció i lliurement de CV encara es fan en mà.

Donar-li forma a aquest treball m'ha servit per reaccionar sobre la quantitat de dades personals que cedeixo ja sigui per inscriure'm a pàgines webs, a diferents botigues per fer el carnet de client i tenir avantatges, etc. Entrant en matèria de protecció de dades, he descobert els perills que això comporta i he decidit donar de baixa les meves dades a més d'un lloc en ser conscient del perill que això suposa per a la meva intimitat.

Quant a currículums, m'he basat en una visió global, en l'experiència com a recepcionista en una ETT recollint tots els CV que es lliuraven, i sobretot basant-me en l'entorn econòmic en el qual vivim i fixant-me en el comportament i coneixement sobre la matèria de la gent que m'envolta, ja que personalment encara no he passat per l'experiència d'haver de repartir gaires CV per buscar feina.

D'aquest treball en trec una lliçó personal, ja que m'ha advertit dels perills que suposa la cessió de dades personals i de repartir CV sense cap mena de control ni preocupació per les dades que proporcionem. Alhora, m'ha servit per conèixer bé tota la normativa per d'ara en endavant tenir un millor control sobre les meves dades personals i la de la gent del meu voltant.

BIBLIOGRAFIA

BIBLIOGRAFIA

- Rebollo Delgado, Lucrecio i Serrano Pérez, M^a Mercedes. *Introducción a la protección de datos*. Ed. Dykinson, S.L, Madrid, 2006. 249 pág. ISBN: 8497728912.
- Lucas Murillo de la Cueva, Pablo. *El Derecho a la autodeterminación informativa*. Fundación Coloquio Jurídico Europeo, cop. Madrid, 2009. 179 pág. ISBN: 9788461334704.
- Troncoso Reigada, Antonio. *La Protección de Datos Personales. En Busca del Equilibrio*. Ed. Tirant lo Blanch, 2011. 1990 pàg. ISBN13: 9788498769807.

NORMATIVA I RECOMENACIONS

- Luxemburg. Directiva 95/45/CE. Parlamento Europeo, 24 de octubre de 1995.
- Espanya. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, de 14 de diciembre de 1999, núm. 298, p. 43088.
- Espanya. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *Boletín Oficial del Estado*, de 19 de enero de 2008, núm. 17, p. 4103.
- *Decreto Legislativo, 30 giugno 2003, n° 196, Codice in materia di protezione dei dati personali.*
- Estats Units. Social Security Act. 14 d'agost de 1935.
- Informe de conclusiones y recomendaciones de la sobre selección de personal a través de Internet. *Agencia Española de Protección de Datos*; 17 de noviembre del 2005.
- *Recommendation R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data used for Employment purposes., on 18 January 1989, at the 423rd meeting of the Ministers' Deputies.*

JURISPRUDÈNCIA

- Espanya. Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. *Boletín Oficial del Estado*, de 4 de enero de 2001, núm. 4, p. 104.

RECURSOS ELECTRÒNICS

- *Autoritat Catalana de Protecció de Dades* [en línia] Cat.
<<http://www.agpd.es>>
- *Agencia Española de Protección de Datos* [en línia] Esp.
<<http://www.agpd.es>>
- *Boletín Oficial del Estado: Cerca de legislació* [en línia] Esp.
<<http://www.boe.es>>
- *Criteris de citació bibliogràfica* [en línia] Cat.
<<http://www.ub.edu/criteris-cub/>>
<<http://www.bib.ub.edu/ajuda/com-citar/>>
- *Cuida tu datos: portal formativo sobre protección de datos* [en línia] Esp.
<<http://cuidatusdatos.com>>
- *European Commission* [en línia]. Ang.
<<http://ec.europa.eu/justice/data-protection>>
- *La tecnología de Identificación por Radio Frecuencia (RFID)* [en línia] Esp.
<<http://www.pc-doctor.com.mx/>>
- *Legge sulla Privacy da inserire nel curriculum per trattamento dei dati* [en línia] It.
<<http://www.curriculumvitaeuropeo.org/2011/06/legge-sulla-privacy-da-inserire-nel.html>>
- *The United States Social Security Administration* [en línia]. Ang.
<<http://www.ssa.gov/history/>>

ANNEX

Annex 1

S'adjunta el Currículum Vitae d'un polític italià on al final de cada pàgina hi consta la clàusula: "Autorizzo il trattamento dei dati personali contenuti nel mio Curriculum Vitae in base art. 13 del D. Lgs 196/2003"

Aquest ha estat extret de la pàgina web del govern italià.

<<http://www.governo.it/AmministrazioneTrasparente/Personale/IncarichiAmministrativiVertice/>>

Annex 2

S'adjunta proposta pròpia de notificació del consentiment a l'entrega d'un currículum.

Annex 3

S'adjunta una part de les recomanacions de l'AEPD sobre la selecció de personal per internet en relació a totes aquelles entitats que, a través d'internet, recullen dades de caràcter personals dels sol·licitants de feina. És una eina d'ajuda sobre l'aplicació de la LOPD i la RLOPD en la recopilació de dades via internet.

Annex 1

CURRICULUM VITAE**INFORMAZIONI PERSONALI**

NOME	[REDACTED]
Luogo e data di nascita	[REDACTED]
Nazionalità	Italiana

TITOLI DI STUDIO E PROFESSIONALE ED ESPERIENZE LAVORATIVE

Titolo di studio	Laurea in Economia e Commercio presso l'Università di Parma
Altri titoli di studio e professionali	Accreditamento al ruolo di Direttore Generale presso Andigel- Fondazione Alma Mater
Esperienze professionali (incarichi ricoperti)	<p>Capo di Gabinetto del Ministro per gli Affari Regionali e le Autonomie (dal 15 maggio 2013 al 22 febbraio 2014)</p> <p>Altre esperienze istituzionali (dal 1/1/1999 al maggio 2013)</p> <p><u>Incarichi di direzione</u></p> <ul style="list-style-type: none">• Dal Febbraio 2012 Presidente di Andigel – Associazione Nazionale Direttori Generali Enti Locali.• Dal Gennaio 2005 Direttore Generale del Comune di Reggio Emilia. In questa veste, oltre alle funzioni di Direttore Generale, preside la Delegazione Trattante di parte pubblica, ricopre ed ha ricoperto <i>ad interim</i> la responsabilità delle seguenti strutture:<ul style="list-style-type: none">– dal 1/11/2012 _ Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi Informativi– dal 1/3/2011 _ Area Ingegneria e Gestione delle Infrastrutture– dal 3/10/2007 al 31.12.2009 _ Servizio Programmazione e Controllo– dal 1/1/2006 al 31.12.2009 _ Servizio Comunicazione, Relazioni Esterne e Marketing• Dal Febbraio 2005 Amministratore Unico di AGAC Infrastrutture S.p.a. (Società delle reti idriche dei Comuni della Provincia di Reggio Emilia).• Dal Marzo 1999 al Dicembre 2004 presso il Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri, ha diretto progetti complessi, volti a favorire lo sviluppo dell'innovazione organizzativa e manageriale nelle amministrazioni pubbliche italiane. <p><i>I programmi e progetti per i quali ha svolto le attività di ideazione e direzione sono i seguenti:</i></p> <ul style="list-style-type: none">– Dal giugno 2001 al dicembre 2004 Cantieri, programma nazionale di sostegno all'innovazione organizzativa nelle amministrazioni statali, regionali e locali promosso dal Dipartimento della Funzione Pubblica (Ministro Franco Frattini) in collaborazione con Anci, Upi, Conferenza dei Presidenti delle Regioni e delle Province autonome, Confindustria, Formez, Scuola Superiore della Pubblica Amministrazione, Scuola Superiore della Pubblica Amministrazione Locale. Il programma è stato premiato dall'ONU come migliore politica d'innovazione del settore pubblico per il 2003 e riconosciuto dal rapporto "Innovation around the world" della JFK School of Government di Harvard tra le più interessanti iniziative dei Paesi OCSE.

- Dal Marzo 1999 al Maggio 2001 Ripensare il lavoro pubblico, progetto finalizzato a sostenere i responsabili del personale di tutte le amministrazioni pubbliche italiane nell'innovazione delle politiche di direzione del personale nelle Amministrazioni Pubbliche, promosso dal Dipartimento della Funzione Pubblica (Ministro Franco Bassanini) in occasione dell'introduzione della contrattazione integrativa e della revisione dell'ordinamento professionale. Il progetto è stato realizzato in collaborazione con Aran, Anci, Upi e Conferenza dei Presidenti delle Regioni e Province autonome e ha coinvolto oltre 1200 amministrazioni italiane. Il progetto ha inoltre tenuto relazioni per scambi e contributi di esperienze con amministrazioni di altri Paesi e i principali programmi stranieri di innovazione (Svezia, Spagna, Stati Uniti, Inghilterra).

Incarichi universitari di docenza e ricerca

- Attualmente svolge docenze in diversi Master presso Università Roma Tre (Masterdasa), Università Cattolica di Milano (MIPA), Università di Tor Vergata Roma (MIMAP).
- Dall'anno accademico 2002/2003 all'anno 2004/2005 Professore a contratto all'Università di Parma (Dipartimento di Economia), docente del corso di organizzazione e sviluppo del personale del Master "Politiche del lavoro e risorse umane" diretto dal Prof. Gianni Geroldi e del corso di gestione dei progetti pubblici (Project management) nel Master "Sviluppo Locale" diretto dal prof. Guglielmo Wolleb. Presso la stessa università incaricato, insieme con il Prof. Marco Carcano, del coordinamento scientifico dell'Osservatorio sulle Politiche del personale della Regione Emilia Romagna. Inoltre titolare dell'insegnamento di gestione delle risorse umane nel Master "Organizzazione e funzionamento delle amministrazioni pubbliche" dell'Università la Sapienza di Roma (Facoltà di Giurisprudenza), diretto dal prof. Sabino Cassese.
- Dal 1999 al 2004. Presso la Scuola Superiore per la Pubblica Amministrazione della Presidenza del Consiglio dei Ministri, ha avuto numerosi incarichi di insegnamento e ricerca in tema di Organizzazione e gestione delle risorse umane. Nel 2003 è stato responsabile del corso su "Innovazione nelle amministrazioni pubbliche" nel Master "Public management" diretto dal Prof. Emanuele SgROI.
- Nell'anno accademico 2001/2002 Professore a contratto all'Università di Bologna, sede di Forlì, docente del Master Europeo "Politiche e amministrazioni pubbliche" e diretto dal Prof. Giliberto Capano della Facoltà di Scienze Politiche.
- Nell'anno accademico 2000/2001. Professore a contratto all'Università di Firenze, docente del corso di Marketing dei Servizi Pubblici della Facoltà di Lettere.

Altri incarichi istituzionali

- Dal Settembre 2012 Presidente dell'O.I.V. del Comune di Bologna.
- Dal Novembre 2011 Presidente dell'O.I.V. del Comune di Arezzo.
- Dal 2010 Membro del Gruppo Tecnico del Comitato di Settore ANCI presso l'ARAN e membro del Gruppo Tecnico ANCI per la Sperimentazione della L. 150/2009 nelle pubbliche amministrazioni.
- Dal 2001 al 2004 Membro del Comitato degli esperti per l'innovazione del Dipartimento della Funzione Pubblica.
- Ha collaborato come esperto con ARAN, FORMEZ, ISFOL, ISTAT e Regione Emilia Romagna in attività di ricerca e intervento sullo sviluppo organizzativo, la comunicazione pubblica, le politiche del personale.
- Dal 2003 al 2004 Componente del Comitato dei garanti della Regione Emilia Romagna e del nucleo di valutazione di RETE di Reggio Emilia.
- Nel 2002 e 2003 Membro della "Commissione di studio sulle politiche di gestione delle risorse umane e sul mobbing" del Dipartimento della Funzione Pubblica promossa dal Ministro Franco Frattini e presieduta dal Prof. Michele Piccione.

ESPERIENZE ISTITUZIONALI PRECEDENTI al 1/1/1999

Incarichi istituzionali

- Nel 1998. Membro della commissione di riordino del Ministero dei Trasporti per la riorganizzazione della struttura centrale promossa dal Ministro Tiziano Treu. Consulente del Dipartimento della Funzione Pubblica per la revisione del sistema strategico e gestionale dei progetti finalizzati.

- Nel 1997/1998. Consulente del Ministro del Lavoro e della Previdenza Sociale per il riordino delle strutture centrali e periferiche e per il programma di attuazione del decentramento delle funzioni con particolare riferimento agli aspetti organizzativi e di gestione delle risorse umane. In tale ambito è stato membro della Commissione di riordino (presieduta da A. Pizzinato e promossa dal Ministro T. Treu) e del Comitato gestione programmi formazione personale coinvolto nei processi di decentramento.
- Nel 1997. Ha diretto il gruppo di consulenza per il Comitato Permanente per l'attuazione della Carta dei servizi pubblici (presidente prof. Franco Pizzetti) presso la Presidenza del Consiglio dei Ministri (Dipartimento della Funzione Pubblica). Consulente del Dipartimento della Funzione Pubblica per la revisione del sistema strategico e gestionale dei progetti finalizzati e per la progettazione delle politiche di innovazione amministrativa.
- Nel 1996/1997. Ha coordinato il progetto pilota "Cento progetti al servizio dei cittadini" del Dipartimento della Funzione Pubblica presso la Presidenza del Consiglio dei Ministri, promosso in collaborazione con ANCI, UPI, Conferenza dei Presidenti delle Regioni e delle Province Autonome. Di tale progetto è tuttora membro del comitato scientifico. Il progetto ha lo scopo di premiare e diffondere le migliori prassi di innovazione nelle amministrazioni italiane.

Incarichi didattici

- Dal 1994 al 1999 è stato Direttore Didattico del Master Post laurea per "Innovatori della Pubblica Amministrazione" (1200 ore) promosso da Regione Emilia Romagna e dalle istituzioni locali della provincia di Reggio Emilia (Comitato Scientifico Proff. A. Barbera, A. De Maio, C. Dell'Aringa, G. Della Rocca, G. Pastori, M. Ricciardi) presso La Cremeria di Cavriago.
- Nell'anno accademico 1993/94 è stato Direttore didattico del Master Post laurea in "Organizzazione e gestione delle risorse umane" (1500 ore) organizzato a Modena nell'anno formativo da AGF (Agenzia Generale della Formazione).

ESPERIENZE NON ISTITUZIONALI DI CONSULENZA

Ha operato, dal 1989, nella consulenza organizzativa e nella formazione, principalmente nell'ambito della Pubblica Amministrazione.

Si è occupato in particolare di:

- Processi di ascolto e partecipazione dei cittadini per la formulazione e valutazione delle politiche pubbliche e dei servizi.
- Rapporto tra politiche pubbliche e sistemi di governo e gestione.
- Comunicazione pubblica, relazioni istituzionali, processi decisionali inclusivi.
- Valutazione delle strategie di gestione dei servizi.
- Analisi e progettazione dei processi di lavoro e delle strutture organizzative.
- Programmazione e controllo della gestione delle attività.
- Sviluppo delle risorse umane, sistemi di valutazione del lavoro, politiche retributive.
- Analisi del clima organizzativo, comunicazione interna, percorsi di partecipazione dei lavoratori.
- Formazione del personale e sviluppo della leadership.
- Relazioni sindacali.

Dal 2001 al 2004

Ha svolto attività di consulenza individuale per grandi istituzioni nazionali. Saltuariamente svolge attività di formazione per dirigenti e consulenza strategica per società di consulenza manageriale (SDA Bocconi, LIUC Castellanza, ISMO, Lattanzio e Partner, Istituto IARD).

Dal 1998 al 2001

Ha svolto attività di consulenza come capo progetto presso il Consorzio MIPA di Roma (Metodologie per lo sviluppo e l'innovazione della pubblica amministrazione) presieduto dal prof. Alberto Zuliani composto dalle Università S. Anna di Pisa, di Siena, di Roma La Sapienza, di Roma Tor Vergata, di Cagliari, dal Formez e dall'ISTAT.

	<p><u>Dal 1990 al 1998</u> Ha svolto attività di consulenza come professionista presso la società di consulenza in organizzazione e direzione aziendale Main - Management e Innovazione di Milano Presidente Prof. Adriano De Maio. Ha svolto attività soprattutto nell'ambito dell'innovazione organizzativa della Pubblica Amministrazione e dello sviluppo delle risorse umane con particolare riferimento ai sistemi retributivi e alle relazioni sindacali.</p> <p><u>Dal 1988 al 1990</u> Ha collaborato con il servizio personale e organizzazione della Provincia di Reggio Emilia per l'introduzione della programmazione e controllo della gestione delle attività.</p> <p>Le principali amministrazioni pubbliche per le quali, a vario titolo, ha svolto attività di consulenza o formazione sono:</p> <ul style="list-style-type: none"> • Presidenza del Consiglio dei Ministri • Dipartimento della Funzione Pubblica • Ministero del Tesoro - Ragioneria Generale dello Stato • Ministero degli Interni • Ministero del Lavoro • Ministero dei Trasporti • ARAN • FORMEZ • ISTAT • ISFOL • EIPA European Institute of Public Administration (Maastricht) • Scuola Superiore della Pubblica Amministrazione <p>Scuola superiore della pubblica amministrazione locale della Lombardia</p> <ul style="list-style-type: none"> • Regione Emilia Romagna • Regione Sardegna • Regione Puglia • Regione Basilicata • Regione Molise • Provincia di Reggio Emilia • Provincia di Como • Provincia di Catania • Comune di Roma • Comune di Parma • Comune di Ravenna • Comune di Verona • Comune di Palermo • Lega delle Autonomie Locali <p>Ha inoltre operato per la ridefinizione della struttura organizzativa in diversi Comuni di medie e piccole dimensioni della Lombardia, Emilia Romagna e Toscana.</p>
<p>Pubblcazioni</p>	<ul style="list-style-type: none"> • [REDACTED] "smart city in pratica: una possibile road map", Ottobre 2012 – <i>in corso di pubblicazione.</i> • [REDACTED] "Le città a colori: una alternativa per tornare a crescere", Saperi PA Forum PA, Ottobre 2012. • [REDACTED] "La carta delle autonomie: un'occasione da non perdere per risolvere il pasticcio della dirigenza", Sole 24 Ore – Rivista Pubblico Impiego, n. 5 Maggio 2012. • [REDACTED] "Governare la rete: dalle parole ai fatti" – Saperi PA Forum PA, Giugno 2011; Labsus Papers (2012), Paper n. 24, Gennaio 2012. • [REDACTED] "Dieci idee per innovare la pubblica amministrazione (in modo rapido e fattibile)", Saperi PA Forum PA, Novembre 2011 • [REDACTED] "Lo spreco", Labsus Papers (2012), Paper n. 14, Novembre 2009. • [REDACTED] "Globalizzazione e deficit di democrazia rappresentativa: proposta forte per l'innovazione amministrativa" in RU – Risorse umane nella PA n. 3 2009.

	<ul style="list-style-type: none"> • ██████████ Sviluppo organizzativo etico per la pubblica amministrazione” in A.A.V.V. “Formazione di valore” a cura di M. Rotondi - F. Angeli 2006. • ██████████ lo spreco”, Labsus Papers (2012), Paper n. 14, Novembre 2009. • ██████████ Globalizzazione e deficit di democrazia rappresentativa: proposta forte per l’innovazione amministrativa” in RU – Risorse umane nella PA n. 3 2009. • ██████████ Sviluppo organizzativo etico per la pubblica amministrazione” in A.A.V.V. “Formazione di valore” a cura di M. Rotondi - F. Angeli 2006. • ██████████ lo sviluppo organizzativo nella pubblica amministrazione” in Sviluppo & Organizzazione – n. 211 Settembre/Ottobre 2005 • ██████████ Governo locale e innovazione organizzativa: le amministrazioni in trasformazione” in RU – Risorse umane nella PA n. 2/2005. • ██████████.Testa “Persone al lavoro. Politiche e pratiche per migliorare il Benessere organizzativo” Rubbettino 2004. • ██████████ P.Testa “Un’agenda per migliorare le relazioni nel lavoro pubblico: proposte per la gestione del personale e la contrattazione integrativa” in RU- Risorse umane nella P.A. n..2 Maggio 2004. • ██████████ “La dimensione organizzativa sottovalutata: il caso delle politiche del lavoro” in P. Saraceno (a cura di) “Rapporto Federalismo 2004 – Aspetti quantitativi e confronto con le esperienze europee”, Reforme - CARIPO, Milano. • F. Avallone – ██████████ Il benessere organizzativo. Per migliorare la qualità del lavoro nelle amministrazioni pubbliche” Rubbettino 2003. • ██████████ Rosa Giolitti , “La contrattazione integrativa negli Enti Locali: elementi di opportunità per la gestione del personale” in L.Bordogna (a cura di) “Contrattazione integrativa e gestione del personale nelle pubbliche amministrazioni. Un’indagine sull’esperienza del quadriennio 1998 – 2001” F. Angeli 2002. • Stolfi E. – ██████████ cura di) “La consapevolezza di un valore. Storie e immagini del lavoro pubblico” Poligrafico dello Stato, 2001 • ██████████ Ripensare il lavoro pubblico – Come gestire le risorse umane e la contrattazione integrativa nella pubblica amministrazione” Rubbettino 2001. • ██████████ “Le comunità di pratica nei processi di innovazione della pubblica amministrazione” in Battistelli F. (a cura di) “La P.A. tra riforma e mutamento culturale” Franco Angeli, 2001. • ██████████ Contrattazione integrativa e nuovo inquadramento negli Enti Locali” in Quaderni di Rassegna Sindacale n.4 2000. • ██████████ L. Nardella “La partecipazione nel settore pubblico: le evidenze empiriche”, L’impresa al plurale - quaderni della partecipazione, n. 6, 2000. • ██████████ Prefazione a G. Della Rocca – L. Rampino “Prima della contrattazione integrativa” Rubbettino 2000. • ██████████ L. Cattivelli “Le relazioni con il pubblico: una leva per il supporto alla riforma” in Quaderni di Comunicazione pubblica n. 1, 1999 ed. Clueb. • ██████████ Possibili livelli di cooperazione istituzionale nei processi di innovazione” in A.A.V.V. “La legislazione regionale per i Piani degli Orari delle città: confronti e prospettive”. • ██████████ Riforma Bassanini: l’onere della prova”, Quale Stato n. 2, 1997. • ██████████ La domanda di servizi nell’impresa” in A.A.V.V. Economie locali e politiche per lo sviluppo. Ires materiali n. 2, 1995. • ██████████ E. Lattanzio “Incentivi di produttività negli Enti Locali: fine di un mito?” Studi Organizzativi n. 1, 1991. • ██████████ G. Della Rocca “Efficienza e produttività nella P.A.” in A.A.V.V. “Stato sociale, Servizi, Pubblico impiego” Jovene editore, 1990.
Capacità linguistiche	Inglese: buono Spagnolo: sufficiente
Capacità nell’uso delle Tecnologie	Buona

Annex 2

DOCUMENT A FIRMAR PER L'INTERESSAT

Acusem recepció del seu currículum vitae i li informem que als efectes del que estableix la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), i conforme l'article 5 LOPD, L'**EMPRESA X**, amb **domicili X**, **nº**, **Codi Postal**, **Ciutat (Província)**, li informa que les dades personals que ens ha facilitat mitjançant el lliurament del seu currículum vitae s'incorporaran a un fitxer no automatitzat (Fitxer de "Currículum Vitae"), inscrit en el registre de fitxers de titularitat privada de l'Autoritat Catalana de Protecció de Dades per a les següents finalitats: 1) analitzar el seu perfil professional i valorar la seva adequació al lloc de treball ofert 2) per poder-li notificar l'acceptació, si escau 3) i per establir i mantenir una relació contractual amb vostè.

D'acord amb la LOPD:

Les seves dades personals només podran ser comunicades a un tercer quan es compti amb el seu consentiment exprés en el mateix currículum o amb la firma d'un formulari que contempli la clàusula de consentiment, excepte els casos expressament establerts en l'article 11 de la LOPD.

L'article 10 de la LOPD regula que el responsable o responsables del fitxer i tractament de les dades –la informació de la identitat i direcció del qual pot sol·licitar-la en qualsevol moment– es compromet a guardar el secret professional respecte d'aquestes. Aquesta obligació subsistirà encara després de finalitzar la relació amb el titular del fitxer o el responsable d'aquest.

L'EMPRESA X prendrà les mesures necessàries per assegurar que la informació transmesa rep el nivell de protecció legal adequat conforme al Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

En el cas que canviïn les finalitats del tractament de les dades per a les quals s'ha donat el consentiment, més enllà de les esmentades, s'utilitzaran les dades personals per demanar una nova confirmació del consentiment.

La remissió del seu currículum i el tractament de les dades personals que ens facilita tenen caràcter voluntari. A tals efectes, mitjançant l'acceptació d'aquesta clàusula l'EMPRESA X entén atorgat el seu consentiment per al tractament de les seves dades personals d'acord amb les finalitats esmentades i confirma que en queda informat.

Firma de l'interessat:

D'acord amb l'article 16 de la LOPD vostè pot exercir, en qualsevol moment, els drets d'accés, rectificació, oposició i cancel·lació de les seves dades, així com revocar el consentiment prestat, mitjançant un escrit a la direcció **EMPRESA X, carrer Domicili Social, numero X, Codi Postal, Ciutat**, en els termes establerts a la LOPD.

Annex 3



SELECCIÓN DE PERSONAL A TRAVÉS DE INTERNET

PLAN DE INSPECCIÓN DE OFICIO

INFORME DE CONCLUSIONES Y RECOMENDACIONES

17 de noviembre de 2005



6. CONCLUSIONES GENERALES.

En relación con cada uno de los principios consagrados por nuestra legislación, se exponen a continuación las principales conclusiones obtenidas respecto de los sitios *web* analizados, siguiendo para ello el orden sistemático que presenta la propia LOPD.

6.1. PRINCIPIO DE CALIDAD DE LOS DATOS.

De acuerdo con la definición contenida en el artículo 3.c) de la LOPD, tratamiento de datos es el conjunto de “operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.”

En un medio como internet, al recabarse datos curriculares, existe siempre asociado un tratamiento de datos de carácter personal, tanto si el procedimiento de recogida consiste en la utilización de un formulario como si se ha habilitado un buzón electrónico para la recepción de los CV.

6.1.1. Adecuación, pertinencia y carácter no excesivo de los datos.

En general, los datos curriculares que suelen recabarse de los demandantes de empleo incluyen los puramente identificativos (nombre y apellidos, dirección postal y electrónica, teléfonos), características personales (fecha y lugar de nacimiento, sexo, nacionalidad, estado civil, número de hijos), formación académica, conocimientos de idiomas, historial profesional, cualificación y aptitudes para el puesto de trabajo, categorías profesionales de interés o retribución mínima requerida.

Aparte de éstos, en algunas *webs* se recogen también datos sobre aficiones, y otras características personales que, en principio, no tienen una relación directa con la solicitud de un puesto de trabajo, pero que suelen obtenerse con objeto de realizar una aproximación más cercana a la personalidad del candidato y no sólo a su capacitación profesional. En ciertas ocasiones, para el desempeño de determinados puestos de trabajo, puede ser relevante conocer las circunstancias familiares u otros datos más íntimos acerca del candidato. No obstante, la recogida de esta información de forma indiscriminada no puede considerarse adecuada.

Entre los servicios ofrecidos por algunos portales a las entidades que publican ofertas de trabajo figura la posibilidad de incluir, junto a la descripción del puesto ofertado, un cuestionario de preguntas (las denominadas, en argot anglosajón, “*killer questions*”), más o menos extenso, con el que el empleador puede obtener una información más completa acerca de la idoneidad de cada candidato para el puesto y así facilitar la labor de clasificación (“*screening*”) de los interesados. Sin embargo, se ha observado que, por lo general, los portales no realizan un control sobre el contenido de estos cuestionarios, a pesar de que las respuestas van a formar parte de un fichero del que son responsables los propios portales, pudiendo ocurrir que entre estos datos figuren algunos cuya recogida pueda vulnerar los derechos de los candidatos, por no respetar los requisitos de adecuación, pertinencia y no exceso previstos en el artículo 4.1 de la LOPD o, incluso, por constituir datos de los que el artículo 7 de la LOPD considera especialmente protegidos.



Se ha verificado que determinados sitios *web* ofrecen al empleador herramientas específicas que le facilitan la evaluación de los candidatos que optan a cada puesto de trabajo publicado. Estas utilidades suelen permitir el almacenamiento, junto a los datos del candidato, de información relativa a las valoraciones subjetivas realizadas por los entrevistadores, valoraciones que muchas veces están estandarizadas, pero que, en ciertos casos, se registran en campos de texto libre, lo que aporta flexibilidad al proceso pero, simultáneamente, introduce un riesgo evidente para el responsable del fichero al que se incorporarán los datos, cuya posición jurídica no suele coincidir con la del que realiza la evaluación de los candidatos. Las inspecciones realizadas han puesto de manifiesto la relevancia y gravedad de ciertas observaciones registradas en tales campos, por personas no suficientemente concienciadas de su trascendencia. Esta información incluye por lo general referencias al aspecto físico, nivel cultural, capacidad de trato social, interés por el puesto o valía del candidato, aunque en algunos casos se han encontrado valoraciones peyorativas (*“es un poco gordita”, “borde”, “se cree muy bueno”, “soberbio”, “bastante impertinente”, “inteligente y con seguridad, pero falta carisma y no es que parezca un delincuente pero no pondría la mano en el fuego acerca de su honestidad y sinceridad”*), otras relativas a circunstancias personales o incluso referencias a los antecedentes penales del candidato (*“ha tenido problemas de drogadicción y es población ex reclusa”, “tiene antecedentes e incluso puede llegar a quitar dinero, por lo tanto no para trabajos que estén relacionados con manejo de dinero, pero sí de mozo”*) o a su supuesta tendencia sexual.

En otros casos la Inspección ha comprobado que, aunque el proceso de filtrado y evaluación de candidaturas está en gran parte automatizado, determinadas compañías (en particular, las especializadas en la selección de personal y consultoría de RRHH) llevan a cabo con posterioridad evaluaciones adicionales que incluyen tests psicotécnicos o psicológicos, así como pruebas de esfuerzo, reconocimientos médicos o entrevistas personales, cuyos resultados generalmente no se automatizan, conservándose, sin embargo, en muchas ocasiones en soporte papel.

Así mismo, algún portal ofrece al usuario la posibilidad de cumplimentar a través de internet tests de variada tipología (personalidad, inteligencia, motivación, actitud directiva, idiomas), pudiendo optar por recibir los resultados en un buzón electrónico. Pues bien, se ha comprobado que tales resultados se conservan junto al resto de datos aportados por el candidato, sin que éste sea informado convenientemente de esta circunstancia.

La Inspección no ha detectado que, para la valoración de los CV recibidos, las entidades obtengan habitualmente datos personales distintos de los que los candidatos aportan voluntariamente. No obstante, en algunos casos se invita a éstos a que en sus solicitudes incluyan referencias de contacto de entidades o personas que puedan informar acerca de su historial profesional. Pues bien, no siempre se informa adecuadamente al candidato de la posibilidad de que la información obtenida por esta vía sea tratada o incluso incorporada a un fichero. Por otra parte, el responsable del fichero no siempre es consciente de que si, a través del candidato, se recaban datos personales relativos a contactos (como pueden ser nombre, apellidos y cargo en una determinada entidad), sería de aplicación la obligación de informar dentro de los tres meses siguientes al momento del registro de tales datos, de conformidad con lo establecido por el artículo 5.4 de la LOPD.

6.1.2. Finalidad.

En relación con las finalidades para las que se usan los datos de los demandantes de empleo recogidos a través de internet, generalmente éstas incluyen el envío, a través del correo electrónico, de comunicaciones relacionadas con la finalidad principal de facilitar la



búsqueda de empleo. Para ello, el usuario debe suscribirse a este servicio (“*newsletters*”), lo que le permite recibir en su propio buzón electrónico información relativa a novedades del sitio *web* que pueden ser de su interés. En ocasiones, se ofrece al usuario el servicio de recepción de “*alertas*” (por lo general, a través de correo electrónico), que le permite estar informado de las nuevas ofertas de trabajo que publica el portal y que pueden adecuarse a su propio perfil profesional .

También se ha observado que, en ciertos casos, en particular en la categoría de portales, el sitio *web* informa al usuario de que sus datos podrían ser utilizados con “*finés comerciales*”, o para la “*oferta de bienes y servicios*” o “*para el envío de comunicaciones comerciales*”. Generalmente, este tipo de actividades se realizan a través del correo electrónico o SMS (“*short message service*” o servicio de mensajes cortos), de tal forma que resulta aplicable la regulación específica prevista en el artículo 21² de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. De acuerdo con la definición que figura en esta Ley, se entiende por comunicación comercial “*toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional*”.

De acuerdo con lo establecido en esta Ley, no sería exigible el consentimiento de los interesados para la realización de este tipo de prácticas, siempre y cuando los productos o servicios ofertados o promocionados sean de la misma entidad que presta el servicio de empleo y además puedan ser considerados como “similares” a éste. No obstante, las entidades inspeccionadas que han reconocido realizar este tipo de comunicaciones incluyen en el sitio *web* una reseña específica informando sobre ello, independientemente de que los productos y servicios promocionados tengan o no relación con el servicio de empleo.

En determinados sitios *web* en los que el servicio de empleo es sólo uno más de los servicios que se ofrecen (por ejemplo, en *webs* institucionales o corporativas o en aquellas otras que, no siendo portales de empleo, sí disponen de secciones de empleo) se ha observado que muchas veces la información facilitada al usuario (que suele estar centralizada en una única página) es tan genérica que no es posible determinar cuáles son las finalidades concretas a las que se destinarán los datos de los demandantes de empleo, ocasionando cierta confusión en éstos, al no saber a ciencia cierta, por ejemplo, si sus datos se utilizarán o no con los mismos fines (generalmente comerciales) con los que se emplean los datos recabados para otros servicios.

En este apartado, cabe también reseñar, por su interés, una denuncia recientemente recibida en la Agencia, según la cual los datos curriculares, que inicialmente habían sido facilitados por el interesado a un portal de empleo, acabaron siendo publicados en otra *web* cuyo objeto era bien distinto. Esta circunstancia, que constituye un evidente desvío de finalidad, puede ser más factible precisamente en aquellos sitios en los que se publican los CV con carácter general, aunque tal riesgo existe siempre si se considera la facilidad con que, en algunas ocasiones, puede accederse a determinadas bases de datos de CV por usuarios no suficientemente identificados.

6.1.3. Exactitud y cancelación.

En relación con el requisito legal de que los datos de carácter personal sean exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado, es evidente que cuando se ofrece a los usuarios la facilidad de acceder y modificar sus propios

² Artículo modificado por la disposición final primera de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.



datos curriculares a través de la *web* (como ocurre en los portales de empleo) disponen de un medio eficaz para mantenerlos, si así lo desean, actualizados en todo momento. No obstante, en algunos sitios *web* que no ofrecen esta funcionalidad (por ejemplo, las Universidades) se informa al candidato de que los datos se mantendrán en la base de datos por un tiempo determinado, obligándose a los demandantes de empleo a renovar su solicitud o CV una vez transcurrido este plazo.

Teniendo en cuenta que en gran número de los sitios *web* analizados los datos no se cancelan tras los procesos de evaluación de las candidaturas, se aprecia que no existe una información explícita a los interesados acerca del tiempo de permanencia de tales datos en los ficheros del responsable o sobre el tiempo que un determinado empleador dispondrá de tales datos, bien en sus propios ficheros (si los incorpora a éstos) o bien formando parte de los subproductos de los ficheros (documentos impresos en papel).

6.1.4. Tratamientos especiales de datos.

Las “*cookies*” son ficheros de texto que se pueden almacenar en el disco duro del usuario y de los cuales el sitio *web* puede conservar una copia. Una “*cookie*” puede contener todo tipo de información que el sitio *web* quiera incluir en ella: páginas visitadas, anuncios consultados, número de identificación del usuario,... Las “*cookies*” aumentan la capacidad de los sitios *web* de almacenar y personalizar la información sobre sus visitantes, ya que el sitio puede releer la “*cookie*” de forma periódica con objeto de identificar a un usuario de internet y reconocerlo cuando vuelva a visitar el sitio. Estos datos tienen la consideración de datos personales cuando son asociados a personas identificadas o identificables.

El artículo 22.2 de la ya citada Ley 34/2002 establece que “*cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito*”, si bien matiza que “*lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario*”.

Se ha comprobado que son numerosos los sitios *web* que, dentro de su particular “*Política de Privacidad*”, informan al usuario acerca de la colocación de “*cookies*”. No obstante, se observa que la información aportada no siempre es suficientemente precisa por haber sido redactada de forma muy genérica, sin especificar claramente los usos concretos a los que se destinan tales datos. Por otra parte, las “*cookies*” más comúnmente utilizadas en los sitios analizados son las denominadas “*de sesión*”, que se extinguen un tiempo después de la desconexión del usuario al sitio *web* visitado, circunstancia ésta de la que también convendría informar adecuadamente al usuario.

Cuando se establece una conexión a un sitio *web*, el servidor en el que se aloja la página recaba automáticamente información sobre el usuario de internet que lo visita. Todas las solicitudes de acceso van acompañadas de la dirección IP del solicitante, así como de la referencia de la página previa desde la que se conecta el usuario y de otros datos (sistema operativo, tipo y versión del navegador, protocolos utilizados en la navegación y preferencias de idioma). La información sobre las visitas al sitio *web*, que se almacena habitualmente en el servidor en el que se aloja el sitio, en un fichero de “*log*” (“*fichero histórico común*”), puede utilizarse con el fin de acumular, mediante un analizador de registros, información sobre el



tráfico procedente de un sitio *web* o con destino a éste, así como sobre las actividades de los visitantes.

En el ámbito que nos ocupa, según han declarado los responsables de los sitios *web* inspeccionados, generalmente esta información se conserva durante un tiempo limitado a disposición de la autoridad judicial, transcurrido el cual suele borrarse. No obstante, en algún caso el sitio *web* informa al usuario del posible uso comercial de estos datos aunque la información que se facilita no es suficientemente clara, pues este uso se confunde a veces con la mera explotación estadística de los datos para la obtención de información global sobre visitas recibidas por el sitio.

En algún sitio *web* se ha detectado que, tras aceptar el candidato el envío de los datos curriculares con los que ha cumplimentado el correspondiente formulario, tales datos se incorporan automáticamente a un mensaje electrónico, en el que, de forma inadvertida para el usuario, se hace constar como remitente la dirección electrónica que éste había configurado por defecto en su programa de correo, no pudiendo entenderse que este dato haya sido obtenido con el consentimiento inequívoco del candidato.

6.2. PRINCIPIO DE INFORMACIÓN EN LA RECOGIDA DE LOS DATOS.

Se han observado deficiencias respecto de la información que se incluye en los sitios *web* para atender el principio de información que consagra el artículo 5 de la LOPD, Ley que es explícitamente mencionada en muchos casos, aunque en algunos, sorprendentemente, sigue haciéndose referencia a la LORTAD, varios años después de ser derogada.

Tal y como ya se ha mencionado antes, lo que no siempre queda suficientemente claro es si, aparte de la finalidad principal de la recogida (la búsqueda de empleo), los datos van a destinarse a otros fines distintos, como podría ser la promoción comercial de productos y/o servicios.

En general, en los formularios se especifica cuáles de los datos recabados son obligatorios y cuáles son facultativos, lo que no ocurre evidentemente en el caso de que los CV deban ser remitidos a un buzón electrónico, siendo entonces el propio demandante quien decide qué datos voluntariamente remite.

En particular en la categoría de los portales de empleo, no siempre se identifica claramente en la *web* el nombre y la dirección del responsable del tratamiento o del fichero, incluyéndose tan sólo referencias al nombre del dominio, lo que impide al demandante de empleo tener conocimiento fehaciente de la persona jurídica (con su denominación social) o física que se esconde tras ese nombre.

Es particularmente relevante el caso en que no se hace referencia al domicilio de la sociedad responsable y resulta que éste está ubicado fuera de las fronteras de nuestro país. Considerando que estamos tratando del medio internet, esta circunstancia condiciona cuál será la legislación aplicable y, por tanto, los derechos que se le reconocen al demandante.

Precisamente dentro de la categoría de los portales de empleo, se han analizado varios en castellano cuyo dominio, generalmente *.NET* o *.COM*, está registrado desde Italia o Gran Bretaña. No obstante, también se ha hallado algún portal ubicado en un dominio territorial *.ES*, cuyo registrante es una persona física que posiblemente reside legalmente en España³, pero en el que se declara como responsable del tratamiento una compañía

³ De acuerdo con las normas establecidas por el *Plan Nacional de Nombres de Dominio de internet bajo el código de país correspondiente a España*, que desarrolla los criterios de asignación establecidos en la Disposición Adicional Sexta de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.



británica ubicada en Edimburgo. Si el tratamiento (parcial o totalmente) no se efectuara en territorio español, tanto en el primero como en el segundo de los escenarios planteados, no sería aplicable la LOPD, a pesar de que el destinatario de los servicios que ofrecen los portales pudiera radicar en España.

Al igual que ya se detectó en la inspección que esta Agencia realizó en su día sobre sitios de comercio electrónico, siguen existiendo todavía *webs* en las que la información facilitada al demandante de empleo se limita a una mera mención al hecho de que “*los datos que nos facilite serán protegidos de acuerdo a la Ley*” o a que “*los datos son estrictamente confidenciales*”, de lo que no puede deducirse, en modo alguno, que los derechos del interesado estén convenientemente garantizados.

En relación con la localización del texto informativo, se ha observado que generalmente se integra como parte del documento en el que se incluyen las condiciones de prestación del servicio, en forma de *Aviso legal* o bien dentro de la *Política de Privacidad* o *Compromiso de Privacidad*, documentos éstos que no siempre están disponibles en todas las páginas del sitio desde las que se recaban datos personales. En otras ocasiones, el texto se incorpora junto a los formularios o junto al buzón destinado a recibir los CV.

Se han encontrado sitios en los que el enlace con el texto informativo está presente en las correspondientes páginas, pero no así el texto al que supuestamente se enlaza, dándose incluso un caso en el que la información que se ofrece es la siguiente: “*en espera de texto legislativo*”, a pesar de que el formulario de recogida de datos (incluido alguno especialmente protegido) sí está activo, produciéndose una clara vulneración de la LOPD. En otros casos se han detectado curiosas anotaciones al margen como éstas: “*sería recomendable eliminar la referencia genérica de los datos referentes a la identidad, dirección, responsable del tratamiento o, en su caso, de su representante*” o “*dado que quizá el requerimiento de la APD sea impracticable, recomendamos que a partir de ahora se incluya una mención expresa a la posible cesión de datos a terceros*”.

6.3. TRATAMIENTO DE LOS DATOS ESPECIALMENTE PROTEGIDOS.

En el caso particular de las agencias de colocación, los datos que se recaban a través de internet están condicionados por, al menos, los que luego deben ser suministrados a la Administración Pública de acuerdo con lo previsto en los respectivos convenios de colaboración suscritos (número de Seguridad Social, nombre y apellidos, fecha de nacimiento, municipio de residencia, país de nacimiento, nacionalidad, sexo, estado civil, actividad económica, fecha de inscripción, situación laboral, situaciones especiales, causa de pérdida del último empleo, nivel académico, profesiones solicitadas). Aún hoy en los formularios utilizados (que emplean las tablas de codificación suministradas por la propia Administración) puede consignarse el valor “*religioso*” en el campo correspondiente al estado civil, lo cual tiene una trascendencia tan clara que implicaría su consideración como dato especialmente protegido, en los términos que establece el artículo 7.2 de la LOPD.

Se plantea, en particular entre las empresas de trabajo temporal, la necesidad de almacenar en ciertas ocasiones información relativa a la religión de los trabajadores cuando ésta pudiera tener incidencia en el desarrollo de sus tareas laborales (por ejemplo, el descanso en determinados días de la semana o la manipulación de ciertos alimentos de origen animal), lo que, sin duda, obligaría a cumplir también los requisitos previstos en el mencionado artículo 7.2. A este respecto, cabe precisar que, ni siquiera en estos casos, la confesión religiosa es un dato necesario, sino que puede considerarse excesivo y no



pertinente para la finalidad perseguida, dado que es posible reseñar sin más en el fichero las condiciones laborales que precisa el candidato, sin necesidad de concretar su religión.

Entre los datos recabados a través de internet es habitual encontrar, fundamentalmente en los sitios *web* de las Fundaciones y de las agencias de colocación, los relativos a las discapacidades (físicas o mentales) de los demandantes de empleo, incluyendo tanto la especificación de la minusvalía concreta como el grado (o porcentaje) de incidencia en el desarrollo de las actividades diarias habituales. A pesar de que ambos datos hacen referencia a la salud de los candidatos en los términos establecidos por el artículo 7.3 de la LOPD, no siempre son recabados con su consentimiento expreso, no existiendo tampoco una Ley que lo disponga por razones de interés general. Por otra parte, estos datos no siempre han sido declarados como tales a la hora de ser notificados a la Agencia los correspondientes ficheros para su inscripción en el Registro General de Protección de Datos.

Se ha detectado que en los ficheros inspeccionados aún sigue almacenándose información relativa a las causas de exención del servicio militar, aun cuando éste dejó, hace ya unos años, de tener carácter obligatorio en nuestro país. Independientemente de que este dato no resulta adecuado en la actualidad, es claro que entre esas causas pueden figurar referencias a la salud de los candidatos, las cuales pueden no haber sido obtenidas con el consentimiento expreso de los interesados. Se ha comprobado, además, que en algunos casos esta información seguía siendo suministrada a los empleadores.

Por lo demás, en los ficheros que han sido objeto de análisis, en general, no se almacenan datos relativos a la ideología, afiliación sindical, creencias, origen racial o vida sexual de los demandantes de empleo. No obstante, de acuerdo con lo expresado en el apartado 6.1.1 del presente documento, el responsable del tratamiento o del fichero debería realizar un exhaustivo análisis de los campos de texto libre y establecer estrictas normas de cumplimentación por parte del personal, para evitar que en tales campos pueda almacenarse información especialmente sensible que revele alguno de esos aspectos acerca de los candidatos.

6.4. ACCESO A LOS DATOS POR CUENTA DE TERCEROS.

Son variadas las relaciones que establece responsable del fichero o del tratamiento de los datos curriculares con otras entidades que bien participan, de una u otra forma, en dicho tratamiento o bien tienen acceso a los mismos.

Cuando el responsable del fichero o del tratamiento actúa como intermediario laboral (lo que ocurre en las tres primeras categorías analizadas, organizaciones con fines de interés general, portales de empleo y empresas de trabajo temporal) los empleadores deben ser considerados como cesionarios, entendiéndose que la comunicación de datos se produce para el cumplimiento de fines directamente relacionados con las funciones legítimas tanto de aquél como de los propios empleadores, por lo que el acceso a los datos por parte de estos terceros se analizará en el siguiente apartado.

Se ha comprobado que en numerosas ocasiones el alojamiento ("*hosting*") del sitio *web* (y generalmente del fichero en el que se almacenan los datos personales de los demandantes) es contratado por el responsable del fichero a terceras entidades (proveedores de servicios de internet), con las que no siempre se ha suscrito un contrato por escrito en los términos que exige el artículo 12 de la LOPD.

Un caso particular es aquél en el que el servicio de correo electrónico está contratado con otra entidad, que es la que aloja temporalmente en sus servidores los



buzones en los que se reciben los CV de los demandantes, que posteriormente se descargarán en el fichero del destinatario. Procede clarificar a este respecto que, a pesar de que los datos permanecen almacenados en servidores ajenos durante un tiempo limitado, bien por obligación legal o por decisión del propio destinatario, en ningún caso estaría justificado el acceso a los mismos por parte de esa entidad, ya que lo contrario vulneraría el secreto de las comunicaciones previsto en los artículos 18.3 y 55.2 de nuestra Constitución y, más específicamente, en el artículo 33 de la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones, y sin perjuicio de las obligaciones que se recogen en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Se han detectado también ciertos sitios *web* que para la recogida de datos curriculares enlazan con otras *webs*. El recurso a estas *webs* se justifica porque ofrecen soluciones estandarizadas para la gestión de CV, que son fácilmente adaptables a las necesidades básicas de, por ejemplo, las compañías que necesitan gestionar las nuevas incorporaciones de plantilla a través de sus propios portales sin realizar para ello una gran inversión. En este tipo de situaciones puede darse la circunstancia de que el usuario no advierta que abandona la *web* inicial en el momento en que se transfiere el control a la otra *web*. Las consecuencias son especialmente graves en aquellos casos en los que no se informa adecuadamente al demandante acerca de quién asume la responsabilidad sobre el tratamiento o sobre el fichero al que se incorporan los datos facilitados.

Pese a la variedad de las situaciones constatadas, puede decirse que, generalmente, el titular de la *web* a la que se accede en los casos descritos actúa en calidad de encargado del tratamiento, siendo los servidores de éste los que alojan los distintos ficheros de cada una de las compañías que utilizan esta tecnología específica. Evidentemente, esta situación no tiene lugar en aquellos casos, también numerosos, en los que, si bien se utiliza una tecnología específica, ésta está incorporada al propio portal de forma tal que el tratamiento se realiza en sus servidores.

Mención especial merece el caso de un portal de empleo que presta sus servicios a una ETT, realizándose la contratación a través de una central de compras que actúa como intermediario y que en realidad es una división de negocio de otro portal de empleo, dándose la circunstancia de que en el contrato suscrito se incluyen garantías especiales para el caso de que este último portal tuviera acceso a los datos de los candidatos, circunstancia esta que, teniendo en cuenta la exclusiva labor de intermediación que desarrolla el portal, no tiene justificación en ningún caso.

6.5. COMUNICACIÓN DE DATOS.

Con carácter general, el tratamiento realizado por los sitios *web* analizados se desarrolla en el marco de una relación establecida con los demandantes de empleo cuyo desarrollo no implica necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este sentido cabe considerar que, para llevar a cabo la labor de intermediación, el intermediario podría facilitar al interesado los datos de contacto de las ofertas laborales que pudieran ser de su interés sin para ello facilitar a los empleadores los datos personales de aquél. No obstante, se ha observado que, excepto en la última de las categorías analizadas (grandes compañías), los empleadores generalmente intervienen como cesionarios de los datos de los demandantes de empleo recabados por internet, aunque no siempre tienen acceso a la totalidad de los datos que se recaban.

Aunque no es la norma general, en ocasiones, especialmente en el caso de los portales de empleo, se incluyen en el sitio *web* las condiciones de prestación de servicio



aplicables a los empleadores, entre las cuales suelen figurar referencias, más o menos explícitas, a la confidencialidad de los datos personales y a su utilización con fines exclusivos de empleo. Son varios los portales de empleo que ofrecen distintas modalidades de confidencialidad, de tal forma que el candidato puede optar porque, por parte de todas las empresas, sean accesibles todos sus datos (incluidos los identificativos y de contacto) o, por el contrario, sólo lo sean aquellos referidos a su historial profesional, o bien porque esos datos sólo puedan ser consultados por las compañías por cuyas ofertas de empleo se ha interesado previamente el candidato.

Esta forma de actuar ofrece más garantías al ciudadano sobre el destino de los datos que facilita, ya que es el propio demandante el que puede ejercer un control sobre la identidad de los destinatarios de la comunicación o, al menos, determinar qué ofertas concretas son las que pueden ocasionar el acceso a sus datos, evitando así que sus datos circulen descontroladamente entre las empresas que, por el mero hecho de inscribirse como usuarias, consultan las bases de datos de CV, o entre aquellas otras a las que el propio responsable del fichero decide comunicar los datos.

Se ha comprobado que los empleadores no suelen suscribir con el responsable del tratamiento o fichero acuerdos específicos, en los que aquéllos se comprometan a adecuar su propio tratamiento a los requisitos legalmente previstos en materia de protección de datos. Esta circunstancia facilita que, como esta Agencia ha tenido oportunidad de verificar, una entidad pueda inscribirse como usuaria de un portal de forma fraudulenta haciéndose pasar por otra, o identificándose como una sociedad en realidad inexistente. En el caso denunciado, la entidad reclamada tuvo acceso a los datos de contacto de un número considerable de demandantes de empleo, a los que posteriormente invitó a informarse sobre un supuesto empleo a través de una línea telefónica de tarificación adicional, con el consiguiente beneficio económico para el contratante de la línea.

En algunos de los sitios *web* analizados se incluyen cláusulas informativas acerca de la posible cesión de datos a otras compañías del mismo grupo empresarial. De acuerdo con los requisitos legales antes mencionados, esta comunicación, que debería contar con el consentimiento previo del demandante de empleo, tiene que justificarse en el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, por lo que es preciso que, en el momento de prestar su consentimiento, el interesado haya sido convenientemente informado de los fines concretos con los que se comunicarán sus datos. En este sentido, sería oportuno identificar cuál es el objeto social del resto de compañías del grupo a las que se prevé realizar la cesión de datos.

Por otra parte, la Inspección ha tenido conocimiento de algunas iniciativas que pretenden aglutinar la información contenida en distintas bases de datos de CV. También se ha verificado que ciertas empresas, en particular aquéllas cuya actividad se centra en la selección de personal o consultoría de RRHH o las grandes compañías, publican ofertas de empleo en distintos portales, ocasionando la recepción de CV por múltiples vías, con el consiguiente riesgo de que los datos facilitados a unos y otros puedan ser fácilmente contrastados.

6.6. DERECHOS DE LAS PERSONAS.

6.6.1. Acceso, rectificación, cancelación y oposición.

Aunque la mayor parte de las entidades inspeccionadas han manifestado no haber recibido un número significativo de solicitudes de los demandantes de empleo en ejercicio de sus derechos de acceso, rectificación, cancelación u oposición, se ha detectado, que en



numerosas ocasiones, las organizaciones no habían previsto aún procedimientos específicos para la atención de estas solicitudes.

No obstante, tal y como se ha mencionado en el apartado 6.1.3, cuando los sitios *web* permiten la inscripción o registro de usuarios, éstos tienen en cualquier momento (no sólo en el intervalo de doce meses previsto en el artículo 15 de la LOPD) la facultad de consultar directamente sus datos curriculares, mantenerlos actualizados e incluso cancelarlos o expresar su oposición al tratamiento de los mismos con determinados fines (generalmente comerciales).

Aunque algunos sitios *web* prefieren borrar definitivamente los datos tras recibir una solicitud de cancelación, en general los inspeccionados han reconocido que los datos son bloqueados durante un tiempo, de acuerdo con la previsión contenida en el apartado 3 del artículo 16 de la LOPD, a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento.

6.6.2. Impugnación de valoraciones.

Como ya se ha comentado en el apartado 6.1.1, en el ámbito que nos ocupa es habitual realizar evaluaciones sobre la idoneidad de los candidatos basadas exclusivamente en la información por ellos aportada, así como en el resultado de los tests realizados en algún caso para valorar su carácter o personalidad. Gran parte de esta información se conserva en los propios ficheros automatizados del empleador o del intermediario. Sin embargo, a pesar de la trascendencia de estos actos, ninguna de las entidades inspeccionadas ha reconocido haber recibido alguna solicitud de impugnación sobre los parámetros o criterios utilizados para la valoración. No obstante, algunos de los inspeccionados se han mostrado reticentes a facilitar a los interesados el resultado de estos tests, en el caso de que así lo solicitaran.

6.7. PRINCIPIO DE SEGURIDAD DE LOS DATOS.

Salvo que entre los datos recogidos a través de los sitios *web* que son objeto de análisis se incluya alguno de los mencionados en el artículo 7 de la LOPD, parece claro que el nivel de seguridad exigible a este tipo de ficheros es el nivel básico, definido en el apartado 1 del artículo 4 del *Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal*, aprobado mediante Real Decreto 994/1999, de 11 de junio. En este sentido, las medidas de seguridad que deben garantizarse son las que se establecen en el capítulo II del Reglamento (artículos 8 al 14).

No obstante, en el ámbito analizado puede entenderse que ciertos ficheros contienen “*un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo*”, siendo exigible en tales casos la adopción de las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20 del Reglamento, de acuerdo con la previsión del apartado 4 del mencionado artículo 4.

Puede decirse que la práctica totalidad de las entidades inspeccionadas disponen de un Documento de Seguridad que, en mayor o menor medida, contiene los aspectos detallados en el artículo 8 del Reglamento. No obstante, se aprecia en ocasiones que la redacción de determinados apartados es en exceso estándar y constituye una mera declaración de intenciones, no respondiendo a una implantación específica de las medidas de seguridad en la organización. Es decir, se expone lo que debería hacerse en lugar de lo



que se hace y, por tanto, el documento no es un reflejo de las medidas efectivamente implantadas.

Por otra parte, como ya se ha apuntado en el apartado 6.3, se ha detectado que el responsable del tratamiento o del fichero no siempre es plenamente consciente de que entre los datos recabados a través de estos sitios *web* pueden figurar algunos que por su naturaleza requieran un especial nivel de protección, de acuerdo con lo que establece el artículo 7 de la LOPD y los capítulos III y IV del Reglamento (artículos 15 al 26).

La Inspección ha detectado que, por ejemplo, cuando se recaban datos relativos a la discapacidad del demandante, aunque a veces se cifran mediante el protocolo HTTPS o utilizando herramientas como PGP, no siempre se han previsto mecanismos que garanticen que la información no sea inteligible o que eviten que pueda ser manipulada por terceros durante su transmisión a través de internet, de conformidad con lo que establece el artículo 26 del Reglamento.

En relación con el registro de accesos previsto en el artículo 24, se ha podido verificar que, cuando está implantado, no siempre guarda constancia de la totalidad de usuarios que tienen acceso a datos especialmente protegidos, siendo frecuente que sólo se considere el acceso por parte de los usuarios externos inscritos en la *web* (es decir, los candidatos a sus propios datos y los empleadores), dejando así sin registro el posible acceso que realicen los usuarios de la propia organización.

Al hilo de lo expuesto en el último párrafo del apartado 6.1.3, se ha comprobado que en muchas ocasiones los documentos que se imprimen a partir de los datos recabados por internet pasan a formar parte del archivo manual del empleador al que se incorporan los CV procedentes de otras vías. Se ha observado, sin embargo, que las organizaciones no son del todo conscientes de que, cuando tales documentos van a ser desechados, han de aplicarse procedimientos de destrucción que garanticen que la información no pueda ser recuperada posteriormente, de acuerdo con lo exigido por el artículo 20 (apartado 3) del Reglamento, evitándose así hechos como los que desgraciadamente se han hecho públicos con cierta frecuencia en los últimos años a través de los medios de comunicación.

Se han observado deficiencias por parte de los portales de empleo en el nivel de cumplimiento del artículo 11 (identificación y autenticación), en particular en lo que respecta al almacenamiento de las contraseñas de acceso de los usuarios inscritos en el portal, que no siempre se realiza de forma inteligible, lo cual tiene especial trascendencia en aquellos casos en los que el fichero contiene datos especialmente protegidos. Por otra parte, el procedimiento previsto para la distribución de esas contraseñas, cuando son remitidas por correo electrónico a los interesados (tras la inscripción o como “*recuerdo de clave*”), no puede decirse que garantice su confidencialidad e integridad, pues los mensajes remitidos no son cifrados en ningún caso.

También se ha verificado que algunos portales utilizan “*cookies*” como método rápido para la identificación de los usuarios, los cuales no son autenticados pues no se les solicita la contraseña de acceso, con el riesgo de que se puedan producir accesos indebidos, especialmente cuando el ordenador desde el que se realiza la conexión a internet no es de uso privado.

Se ha comprobado que al realizar una búsqueda de candidatos a través de un determinado sitio *web*, aunque los resultados mostrados al público en general estaban anonimizados, era posible, sin embargo, visualizar en la barra de herramientas del navegador el número del D.N.I. de cada candidato, pues se utilizaba internamente como parámetro en el acceso. Una vez comunicada esta deficiencia, fue subsanada por los responsables del portal, destinado a personas con discapacidad.



Finalmente, cuando es exigible el sometimiento de los sistemas de información y las instalaciones de tratamiento a una auditoría interna o externa, es decir, cuando se tratan datos especialmente protegidos o cuando nos hallamos en el escenario expuesto en el segundo párrafo de este apartado, se ha detectado que las organizaciones no siempre disponen del informe preceptivo previsto en el artículo 17 del Reglamento, el cual debe emitirse con una periodicidad máxima de 2 años.

6.8. MOVIMIENTO INTERNACIONAL DE DATOS.

Se han hallado *webs* de empleo que son responsabilidad de compañías ubicadas en nuestro país y que, al igual que los ficheros a los que se incorporan los datos curriculares, se alojan fuera del territorio español, lo cual constituye en sí mismo una transferencia internacional de datos. En tales casos, es preciso recordar que, excepto en el caso de que el destino de la transferencia sea un Estado miembro de la Unión Europea o un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado⁴, se requiere la autorización previa del Director de la Agencia Española de Protección de Datos, según prevé la norma general establecida por el artículo 33 de la LOPD.

Se ha comprobado que algunos sitios, de conformidad con la excepción prevista en el apartado e) del artículo 34 de la LOPD (que “*el afectado haya dado su consentimiento inequívoco a la transferencia prevista*”), incluyen entre las condiciones generales de prestación del servicio una mención específica al hecho de que los datos curriculares recabados se almacenarán en un servidor ubicado en otro país (generalmente Estados Unidos), entendiéndose que de esta forma se obtiene el consentimiento preciso. No obstante, siguen siendo numerosos los sitios que no informan de esta circunstancia y que, por tanto, no cuentan con el consentimiento de los interesados, por lo que en estos casos es evidente que la transferencia internacional no se adecua a los requisitos legalmente previstos.

Algunos de los sitios analizados disponen de versiones distintas dependiendo del país desde el que accede el usuario, de forma tal que se configura una base de datos de CV organizada por países (generalmente, aunque no siempre, del ámbito hispanohablante), facilitándosele al usuario la posibilidad de optar por puestos de trabajo ofertados por compañías ubicadas en esos países. Aunque parece evidente que en tales casos (independientemente del país donde se ubica el fichero) pueda tener lugar una transferencia de datos a terceros países, siempre que sea de aplicación la legislación española, sería preciso advertir explícitamente al usuario de la existencia de ese movimiento internacional de datos.

Se ha verificado también que desde algunos sitios *web*, generalmente pertenecientes a multinacionales, se recaban datos curriculares que son transferidos a las filiales de esas compañías ubicadas en otros países, circunstancia ésta de la que suele informarse adecuadamente en el momento de la recogida de los datos.

⁴ La decisión de la Comisión Europea 2000/518/CE, de 26 de junio, considera adecuado el nivel de protección de datos personales en Suiza. Así mismo, la Decisión 2000/520/CE, de igual fecha, efectuó la misma declaración respecto de las empresas de los Estados Unidos de América acogidas al sistema de “*puerto seguro*”. Posteriormente, la Decisión 2002/2/CE, de 20 de diciembre de 2001, consideró adecuado el nivel garantizado por Canadá, respecto de las entidades canadienses de ámbito federal. La Decisión 2003/490/CE, de 30 de junio, ha considerado que Argentina garantiza también un nivel adecuado. Las Decisiones 2003/821/CE, de 21 de noviembre, y 2004/411/CE, de 28 de abril, han declarado el carácter adecuado de la protección de datos en Guernsey y en la Isla de Man, respectivamente. En su Decisión de 14 de mayo de 2004, la Comisión consideró que el Servicio de aduanas y protección de fronteras de los Estados Unidos (CBP) garantiza una protección adecuada de los datos PNR transferidos por la Comunidad sobre los vuelos con destino o procedentes de Estados Unidos.



7. RECOMENDACIONES.

Con fecha 12 de agosto de 2005 se puso en conocimiento de las entidades investigadas el informe elaborado por la Inspección de Datos, con el fin de que, en el plazo de veinte días hábiles, pudieran formular las observaciones que al respecto estimasen necesarias, partiendo de los hechos ya constatados.

Una vez recibidas las observaciones formuladas y teniendo como referencia el resultado de las actuaciones de Inspección llevadas a cabo, el Director de la Agencia Española de Protección de Datos, en virtud de las potestades que le otorga el art. 5, c) y d) del *Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia*, dicta las siguientes recomendaciones, que deberán ser observadas por todas aquellas entidades que, a través de internet, recaban datos de carácter personal de los demandantes de empleo, al objeto de adecuar su funcionamiento a los principios de la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal* (LOPD), y a la normativa que la desarrolla.

7.1. DERECHO DE INFORMACIÓN EN LA RECOGIDA DE LOS DATOS.

RECOMENDACIÓN PRIMERA

1. De conformidad con lo establecido por el artículo 5 de la LOPD, los demandantes de empleo a los que se soliciten datos personales a través de internet deberán ser previamente informados de modo expreso, preciso e inequívoco:
 - a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información;
 - b) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas;
 - c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos;
 - d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición;
 - e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
2. En todas y cada una de las páginas web desde las que se recaben datos de carácter personal, tanto si la recogida se realiza mediante un formulario como si se habilita un buzón electrónico, se incluirá claramente visible la información a la que hace referencia el artículo 5 de la LOPD, a la que el usuario deberá poder acceder con facilidad y de forma directa y permanente.

A pesar de que se pueda incorporar en todas esas páginas un texto o un botón adecuadamente etiquetado que, al ser seleccionado mediante un “click”, permita obtener la citada información, se considera más adecuado propiciar la lectura de dicha información de modo ineludible (y no optativa) dentro del flujo de acciones que deba ejecutar el usuario para expresar la aceptación definitiva de la transmisión de sus datos a la entidad que los está recabando.



En particular, se especificará claramente el nombre o denominación social y el domicilio del responsable del fichero al que se incorporarán los datos personales solicitados, así como una referencia al código de inscripción asignado por el Registro General de Protección de Datos. Deberá indicarse también la dirección ante la cual pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición, en el caso de que sea distinta del domicilio especificado, así como el procedimiento que deberán seguir los usuarios, ya sea electrónico, postal, telefónico o cualquier otro que se considere válido.

En el caso de que los datos personales vayan a ser inicialmente incorporados a los ficheros de distintos responsables, se referirá toda la información anterior a cada uno de ellos.

Cuando el responsable no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España.

En todo caso, la información deberá proporcionarse en el mismo idioma en que se recaban los datos personales.

3. El demandante de empleo deberá estar convenientemente informado en todo caso del momento en que desde una web se transfiere el control a otra web, de tal forma que no pueda albergar dudas al respecto. En este sentido, se considera una buena práctica que el responsable de la web se cerciore de que las webs a las que se transfiere el control cumplen también los términos expresados en la presente Recomendación.

7.2. CONSENTIMIENTO DEL INTERESADO.

RECOMENDACIÓN SEGUNDA

1. De acuerdo con lo que dispone el apartado 1 del artículo 6 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa o sean de aplicación las excepciones previstas en el apartado 2 del mismo artículo.
2. Cuando un demandante de empleo facilita voluntariamente sus datos curriculares de carácter personal a través de internet, se entenderá que consiente en el tratamiento de los mismos en los términos en los que haya sido convenientemente informado en el momento de la recogida.
3. Siempre que la Ley no lo impida, y el afectado puede revocar su consentimiento para el tratamiento de sus datos de carácter personal, en cuyo caso el responsable del fichero habilitará los correspondientes medios, sencillos y gratuitos, para excluir del tratamiento dichos datos.

7.3. USOS Y FINALIDADES.

En el año 1996, el Grupo de Trabajo Internacional de Protección de Datos en Telecomunicaciones⁵ elaboró el documento *“Telecommunications and Privacy in Labour*

⁵ Grupo de Trabajo creado en 1983, a iniciativa de la autoridad de protección de datos del Lander de Berlín, donde tiene su sede, y que agrupa, junto a representantes de las autoridades de control de un gran nmero de Estados (entre ellos Espaa), a representantes de organizaciones internacionales pblicas y privadas, y a representantes de los sectores industriales implicados.



Relationships”, en el que recomendaba al empleador restringir la recogida de datos que pudieran considerarse no directamente relevantes en la relación profesional, como el comportamiento personal, determinadas características personales o los contactos internos y externos del trabajador.

Por otra parte, en su Recomendación 1/2001, de 22 de marzo, sobre los datos de evaluación de los trabajadores, el Grupo de Trabajo de Autoridades Europeas de Protección de Datos⁶ argumentaba: *“según la definición incluida en la letra a) del artículo 2 de la Directiva 95/46/CE, los datos personales son toda información sobre una persona física identificada o identificable, tal como los datos relacionados con su identidad física, fisiológica, psíquica, económica, cultural o social. El alcance de dicha definición implica que los datos personales incluyen, además de los datos de los registros de población o información resultante de factores objetivos que se pueden verificar o rectificar, cualquier otro elemento, información o circunstancia que incluya un contenido informativo tal que se sume al conocimiento de una persona identificada o identificable. Así, se pueden encontrar datos personales en evaluaciones y juicios subjetivos que, en realidad, podrían incluir elementos específicos de la identidad física, fisiológica, psíquica, económica, cultural o social de los interesados. Esto sucede igualmente si un juicio o evaluación se resume en una puntuación o clasificación, o si se expresa mediante otros criterios de evaluación”*.

Cabe citar también la Recomendación 2/1989 del Comité de Ministros del Consejo de Europa⁷, sobre la protección de datos personales usados con fines de empleo, que en su artículo 4.3 establece que *“en el proceso de selección de trabajadores los datos recogidos han de limitarse a aquellos necesarios para evaluar la aptitud de los eventuales candidatos y sus perspectivas de promoción. A lo largo de este proceso, sólo se obtendrán datos personales del propio interesado. De conformidad con lo previsto en las Leyes nacionales, se podrán consultar otras fuentes sólo con el consentimiento del interesado o si éste ha sido previamente informado de esta posibilidad”*. Así mismo, en su artículo 4.4 se prevé que *“el recurso a tests, análisis y procesos similares diseñados para evaluar el carácter o la personalidad del individuo no debería tener lugar sin el consentimiento de éste, a menos que las Leyes nacionales prevean otras garantías apropiadas”*.

RECOMENDACIÓN TERCERA

1. Tal y como dispone el apartado 1 del artículo 4 de la LOPD, los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

⁶ Órgano con carácter consultivo e independiente creado por el artículo 29 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y, por este motivo, también conocido como Grupo del artículo 29. Está integrado por representantes de las Autoridades de protección de datos de la UE y la Comisión Europea. La Agencia española forma parte del mismo desde su inicio, en febrero de 1997. Se reúne con periodicidad bimensual, habiendo aprobado hasta ahora casi una centena de documentos, en forma de Decisiones, Dictámenes, Documentos de Trabajo, Informes o Recomendaciones sobre todas aquellas cuestiones relevantes que afectan a la protección de datos personales.

⁷ La protección de datos personales en el Consejo de Europa es un objetivo político y jurídico de esta Organización europea, como una manifestación más del respeto a los derechos humanos. Consecuencia de ello fue precisamente el *Convenio 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos personales*, de 1981, completado por un Protocolo relativo a las autoridades de control. Fue ratificado por España por Instrumento de 27 de enero de 1984.



2. No se recabarán a través de internet datos personales cuyo conocimiento por parte del responsable no esté justificado por la finalidad para la que se recaban y de la cual el usuario no haya sido previamente informado.
3. Los datos personales de los demandantes de empleo no se usarán para finalidades incompatibles con la de facilitar a éstos la búsqueda de un puesto de trabajo, por lo que el tratamiento de tales datos con otros fines requerirá el consentimiento de los interesados, a los que se informará previamente de modo expreso, preciso e inequívoco de tales fines. Para recabar este consentimiento en internet, se considerará válido un procedimiento en el que el usuario tenga una participación activa, de tal forma que, a través de la web, pueda manifestar su voluntad en uno u otro sentido.
4. Para que la ausencia de manifestación de la voluntad del usuario pueda producir alguna consecuencia respecto del tratamiento de sus datos, deberá habersele advertido expresamente de esta circunstancia, así como de los efectos de la misma.
5. No se recogerán de forma indiscriminada datos que pudieran considerarse no directamente relevantes para la relación profesional con el candidato. Así, se requerirán tan sólo en el momento en que el aspirante solicite un puesto de trabajo para cuyo desempeño esté suficientemente justificado su conocimiento por parte del empleador.
6. Los responsables del tratamiento y los responsables de ficheros realizarán un control exhaustivo de las cuestiones que se plantean a los candidatos para evaluar su idoneidad en determinados puestos de trabajo, con objeto de respetar los principios legales de adecuación, pertinencia y no exceso, asegurándose en todo caso de que a través de las mismas no se recaban de los interesados datos especialmente protegidos sin su consentimiento expreso y, cuando sea preciso, por escrito.
7. Estas mismas garantías se respetarán así mismo respecto de los datos de valoración que los empleadores o intermediarios consignan en campos de texto de libre cumplimentación.
8. El mantenimiento en los ficheros de los resultados de los tests y demás pruebas de selección realizadas por los solicitantes de empleo se realizará en todo caso con el consentimiento informado de éstos.
9. Los candidatos serán convenientemente informados acerca del posible acceso por parte de empleadores o intermediarios a datos que les conciernen relativos a su trayectoria profesional y que no hayan sido obtenidos directamente de los mismos.
10. Se respetarán también las garantías legales respecto de los datos personales de terceros (por ejemplo, referencias profesionales) que pudieran ser obtenidos durante el proceso de selección laboral.
11. El apartado 1 del artículo 21 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, establece que *“queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas”*. No obstante, el apartado 2 del mismo artículo, particulariza que *“lo dispuesto en el apartado anterior no será de aplicación cuando exista un relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente”*.



De conformidad con este precepto, el envío por parte del responsable del fichero de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente, se realizará únicamente cuando medie la solicitud previa de los solicitantes de empleo o cuando éstos las hayan autorizado expresamente, salvo que tales comunicaciones se refieran a servicios del propio responsable similares al que ocasionó la recogida de los datos, es decir, el servicio de búsqueda de empleo.

12. El artículo 22.2 de la Ley 34/2002 establece que *“cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito”*, aunque también aclara que *“lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida en que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario”*.

Si, aparte de los datos personales que facilita voluntariamente el interesado a través de internet, se utilizan procedimientos automáticos invisibles de recogida de datos relativos a una persona identificada o identificable (*“cookies”*, datos de navegación, información proporcionada por los navegadores, contenidos activos,...), antes de comenzar la recogida a través de ellos o de desencadenar la conexión del ordenador del usuario con otro sitio web, se informará al usuario de manera clara y completa sobre su utilización, finalidad y tiempo de permanencia, ofreciéndosele la posibilidad de rechazar su tratamiento mediante un procedimiento sencillo y gratuito.

13. Así mismo, se deberá informar al usuario del nombre de dominio del servidor que transmite o activa los procedimientos automáticos de recogida, de la finalidad de los mismos, de su plazo de validez, de si es necesaria o no la aceptación de dichos procedimientos para visitar el sitio web y de la opción de que dispone todo usuario de oponerse a esta modalidad de tratamiento, además de las consecuencias de desactivar la ejecución de dichos procedimientos, cuando dicha opción esté disponible para el mismo.
14. El artículo 38.3. a) de la Ley General de Telecomunicaciones establece que los abonados a los servicios de comunicaciones electrónicas, entre los que cabe incluir a los usuarios de internet, tendrán el derecho *“a que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación”*. También, en el apartado b) del citado artículo, prevé que los usuarios tendrán el derecho *“a que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello”*.

Los datos de tráfico, relativos a las visitas recibidas por los sitios web de empleo, que se almacenan en ficheros históricos de *“log”*, se harán anónimos o se cancelarán cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Estos datos podrán ser utilizados con fines comerciales o para la prestación de servicios de valor añadido, únicamente, cuando los usuarios visitantes hubieran prestado su consentimiento informado para ello.

15. Cuando el procedimiento utilizado para la recogida de datos personales del solicitante de empleo suponga el envío de un mensaje electrónico con la dirección electrónica por defecto del solicitante, se informará adecuadamente a éste con objeto de obtener su consentimiento.



7.4. CANCELACIÓN DE DATOS.

Al respecto de la conservación de los datos contenidos en los CV conviene reproducir las consideraciones que realizaba el Consejo de Europa en el artículo 14 de su Recomendación 2/1989. En primer lugar, este organismo consideraba que *“los datos personales obtenidos a través de una solicitud de empleo deberían normalmente borrarse tan pronto como se decida que, a ese respecto, no se realizará una oferta de empleo”*. Por otra parte, aconsejaba que *“cuando tales datos se hayan conservado con vistas a un posterior proceso de selección, deberían borrarse si el candidato así lo solicita”*, aunque especificaba que *“si es necesario conservar éstos últimos para la realización de acciones legales, se almacenarán durante un período de tiempo razonable”*.

RECOMENDACIÓN CUARTA

1. Según prevé el apartado 5 del artículo 4 de la LOPD, los datos de carácter personal serán cancelados a propia iniciativa del responsable del fichero cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados. Igualmente serán cancelados cuando así lo solicite el interesado.
2. No obstante, la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.
3. Los datos personales de los solicitantes de empleo, que hubieran sido facilitados por éstos o hubieran sido obtenidos con su consentimiento para una oferta concreta de empleo, serán cancelados por el empleador tan pronto como éste haya resuelto negativamente la solicitud, salvo que el solicitante exprese explícitamente su voluntad en sentido contrario.
4. Los datos personales de los solicitantes de empleo no serán tratados por los intermediarios, a los que los hubiesen facilitado, desde el mismo momento en que aquéllos soliciten su cancelación.

7.5. DATOS ESPECIALMENTE PROTEGIDOS.

El artículo 10 de la Recomendación 2/1989 del Consejo de Europa prevé que a los trabajadores y a los demandantes de empleo se les pueden plantear cuestiones relacionadas con su estado de salud para: a) determinar su adecuación al puesto de trabajo; b) cumplir los requisitos de la medicina preventiva; o c) garantizar determinados beneficios sociales.

RECOMENDACIÓN QUINTA

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución Española, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.
2. Tal y como prevé el apartado 2 del artículo 7 de la LOPD, sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias.



3. De conformidad con lo establecido en el apartado 3 del artículo 7 de la LOPD, los datos de carácter personal de los demandantes de empleo que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando el afectado consienta expresamente.

A estos efectos, se considerará válido un procedimiento en el que el usuario tenga una participación activa, de tal forma que, a través de la web, pueda manifestar expresamente su voluntad de que tales datos sean recabados y tratados.

4. Los datos relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual de los demandantes de empleo sólo podrán ser tratados por los empleadores e intermediarios cuando este tratamiento esté suficientemente justificado en relación al proceso de la contratación laboral de que se trate.

7.6. ACCESO A LOS DATOS POR CUENTA DE TERCEROS.

RECOMENDACIÓN SEXTA

1. De conformidad con lo dispuesto en el apartado 1 del artículo 12 de la LOPD, la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
2. En el citado contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de la LOPD y que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En particular, estas obligaciones se extenderán a todas aquellas entidades que, como encargados del tratamiento, precisen intervenir en el desarrollo de la relación establecida con los usuarios de la web. A este respecto, el prestador del servicio no podrá utilizar los datos para fin distinto del que conste en el contrato, ni subcontratar la gestión del servicio con terceros, salvo que lo haga en nombre y por cuenta del responsable.
5. Los responsables de ficheros o de tratamientos se asegurarán de que, las entidades con las que establecen relaciones contractuales y que alojan temporalmente en sus ficheros datos personales de los demandantes de empleo, no realizan accesos indebidos a esta información.

7.7. COMUNICACIÓN DE DATOS.

RECOMENDACIÓN SÉPTIMA

1. Según dispone el apartado 1 del artículo 11 de la LOPD, los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Se tendrán en cuenta, sin embargo, las excepciones previstas en el apartado 2 del citado artículo, y en particular, la referida a la situación en la que el tratamiento responda



a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este último caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

Se entenderá en todo caso que la comunicación de datos de los demandantes de empleo a los empleadores por parte de los intermediarios requiere el consentimiento previo de aquéllos.

2. De acuerdo con lo que establece el apartado 3 del mismo artículo, será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad del cesionario a quien se pretenden comunicar.

En este sentido, cuando los datos personales recabados a través de internet vayan a ser comunicados a otras compañías (incluso cuando éstas pertenezcan al mismo grupo empresarial) deberá informarse al usuario, de tal forma que éste pueda conocer explícitamente las finalidades determinadas a las que se destinarán los datos.

3. Se considera más adecuada en este contexto la obtención del consentimiento del demandante mediante un procedimiento que le permita a éste ejercer un control sobre la identidad de los destinatarios de la comunicación o, al menos, determinar qué ofertas de empleo concretas son las que pueden ocasionar el acceso a sus datos personales.

7.8. DERECHOS DE LAS PERSONAS.

En consonancia con las previsiones de la LOPD, cabe mencionar el criterio adoptado más específicamente en su día por el Consejo de Europa en la ya citada Recomendación 2/1989, sobre la protección de datos personales usados con fines de empleo, que en su artículo 4.4 prevé que *“si el interesado así lo desea, debería informársele de los resultados de los tests, análisis y procesos similares”* diseñados para evaluar su carácter o personalidad.

En relación con el ejercicio del derecho de impugnación en el ámbito que nos ocupa, interesa traer a colación las observaciones realizadas en el estudio *“Utilización y control de datos laborales automatizados”*⁸: *“mientras permanezca incontrovertido el derecho del trabajador a conocer la existencia de un fichero automatizado, a poder o no poder suministrar los datos personales, a exigir seguridad y reserva e, incluso, a controlar la cesión a terceros, no resulta tan clara en el marco de una relación laboral la exclusión del poder de dirección empresarial de la posibilidad de tratar como estime conveniente los datos obtenidos legalmente –siempre sin violar los derechos de intimidad del trabajador o de fuentes paralelas legítimas–, siendo de muy difícil demostración, además, que determinadas decisiones hayan sido adoptadas por el empresario atendiendo en exclusiva a tales ficheros, dada la habitual pluralidad de puntos de referencia en orden a adoptar decisiones concretas sobre los trabajadores sometidos a una evaluación permanente. Una solución a tal problema podría encontrarse aplicando la doctrina elaborada por los Tribunales en torno al despido nulo por vulneración del principio de no discriminación o de otros derechos fundamentales, de forma tal que, por ejemplo, el candidato rechazado únicamente debería demostrar unos hechos a partir de los cuales derivar la sospecha fundada de haber adoptado la decisión en virtud de valoraciones fundadas exclusivamente en datos automatizados, mientras al*

⁸ Op. cit.



empresario le correspondería cargar con la prueba de que en su decisión han primado otra serie de factores serios y razonables”.

RECOMENDACIÓN OCTAVA

1. Los responsables de ficheros o del tratamiento de datos de carácter personal de los demandantes de empleo atenderán las solicitudes de acceso, rectificación, cancelación y oposición realizadas por éstos de conformidad con lo previsto en los artículos 15 y 16 de la LOPD y en el capítulo IV del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continua en vigor a tenor de la disposición transitoria tercera de la LOPD.
2. De acuerdo con lo especificado en el artículo 13 de la LOPD, los demandantes de empleo tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

Así mismo, el demandante de empleo podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

El demandante de empleo también tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

7.9. SEGURIDAD DE LOS DATOS.

RECOMENDACIÓN NOVENA

1. De acuerdo con lo establecido por el artículo 9 de la LOPD, el responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones determinadas en el Reglamento de Medidas de Seguridad, aprobado mediante el Real Decreto 994/1999, de 11 de junio, las cuales se clasifican de acuerdo a los niveles de seguridad establecidos en su artículo 4.
3. A los ficheros con datos personales que permitan obtener una evaluación de la personalidad del demandante de empleo, les será de aplicación, al menos, lo establecido en el apartado 4 del artículo 4 del citado Reglamento, es decir, en tal caso deberán garantizarse las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20 del mismo.
4. Los ficheros con datos que puedan revelar circunstancias relativas a la ideología, afiliación sindical, creencias, religión, salud, origen racial o vida sexual de los demandantes de empleo reunirán, además de las medidas de nivel básico y medio detalladas en los capítulos II y III del Reglamento, las calificadas como de nivel alto en su capítulo IV.



5. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

Este documento contendrá los aspectos detallados en el apartado 2 del artículo 8 del Reglamento y, en caso de ser aplicable, los especificados en el artículo 15.

En todo caso el documento reflejará con fidelidad las medidas efectivamente implantadas por la organización y se mantendrá en todo momento actualizado, debiendo ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

6. Cuando los usuarios registrados en una web tengan acceso on-line a los datos curriculares de que dispone el responsable del fichero respecto a su persona, deberán establecerse procedimientos de identificación, autenticación y control de accesos, de acuerdo con lo establecido en los artículos 11, 12 y, cuando sea aplicable, 18 del citado Reglamento.

Siempre que el mecanismo de autenticación se base en la existencia de contraseñas se utilizará un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad, de tal forma que se minimice el riesgo de acceso no autorizado a través de internet.

Se considera que la identificación de los usuarios mediante “cookies”, sin la aplicación de métodos complementarios de autenticación, no cumple las garantías previstas en los mencionados artículos del Reglamento.

7. Cuando se proceda a la destrucción de cualquier tipo de soporte que contenga datos personales de los demandantes de empleo, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él.
8. Las organizaciones que traten datos personales de los demandantes de empleo y a las que les sean de aplicación las medidas especificadas en los apartados 3 y 4 de la presente Recomendación, someterán a los sistemas de información e instalaciones de tratamiento de datos a una auditoría interna o externa, que verifique el cumplimiento del Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

La redacción de los correspondientes informes de auditoría se adecuará a lo previsto en los apartados 2 y 3 del artículo 17 del Reglamento.

9. Los accesos a los datos de los demandantes de empleo, que requieran la adopción de las medidas especificadas en el apartado 4 de la presente recomendación, serán auditados mediante un Registro de Accesos en los términos previstos por el artículo 24 del Reglamento. Este requisito se extenderá tanto a los accesos efectuados por los demandantes a través de internet respecto de sus propios datos, como a los accesos realizados por cada una de las personas que participan de alguna forma en el tratamiento de tales datos.

10. Siempre que no sean exigibles de conformidad con el artículo 26 del Reglamento, se considera una buena práctica la adopción de medidas que eviten que la información circule por la red de forma inteligible y, por tanto, susceptible de ser conocida o manipulada por terceros. Del mismo modo, se considera buena práctica proporcionar al usuario información acerca del nivel de protección que proporciona la tecnología utilizada.



7.10. MOVIMIENTO INTERNACIONAL DE DATOS.

Con fecha 6 de noviembre de 2003, el Tribunal de Justicia Europeo resolvía una petición del Göta Hovrätt, órgano jurisdiccional sueco, destinada a obtener una interpretación de la Directiva 95/46/CE. En la sentencia se estimaba lo siguiente: “1) *La conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE. 2) Un tratamiento de datos personales de esta naturaleza no está comprendido en ninguna de las excepciones que figuran en el artículo 3, apartado 2, de la Directiva 95/46. [...] 4) No existe una «transferencia de datos a un país tercero» en el sentido del artículo 25 de la Directiva 95/46 cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por una persona física o jurídica que gestiona el sitio internet en el que se puede consultar la página web que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a internet, incluidas aquellas que se encuentren en países terceros.*

Por otra parte, el Grupo del artículo 29, en su Dictamen 8/2001, de 13 de septiembre, sobre el tratamiento de datos personales en el contexto laboral, expresa su convencimiento de que una significativa proporción de las transferencias internacionales que se realizan son las que precisamente llevan a cabo las multinacionales o los grupos empresariales con los datos de sus trabajadores. El Grupo de Trabajo muestra su preferencia por que los empleadores amparen legalmente esta actividad en la existencia de un nivel de protección adecuado en el país destinatario y que, sólo en su defecto, se haga uso de alguna de las excepciones previstas en la Directiva (artículo 34 de la LOPD), acudiendo en último término a la que prevé la obtención del consentimiento inequívoco del interesado.

RECOMENDACIÓN DÉCIMA

1. De conformidad con lo establecido por el artículo 33 de la LOPD, no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal, que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable al que presta la Ley Orgánica, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos.

A este respecto, se tendrán en cuenta las excepciones previstas en el artículo 34 de la LOPD:

- a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
- b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
- d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.



- f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
- h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquella sea acorde con la finalidad del mismo.
- k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.⁹

En particular, cuando sea de aplicación la legislación española sobre protección de datos, conforme al artículo 2.1 de la LOPD, y además el fichero que contiene los datos personales recabados a través de internet se halle ubicado en el territorio de un Estado no miembro de la Unión Europea o respecto del que no se haya declarado por la Comisión de las Comunidades Europeas la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo, será precisa la autorización previa del Director de la Agencia Española de Protección de Datos, a menos que la transferencia internacional se fundamente en alguna de las excepciones comprendidas en los apartados a) a j) del artículo 34 de la LOPD antes citados. En todo caso, la transferencia internacional se deberá notificar a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos.

2. De acuerdo con lo que establece el artículo 5 de la LOPD y se recoge en la Norma Segunda de la Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos, cualquier responsable de un fichero o tratamiento que se proponga transferir datos de carácter personal fuera del territorio español deberá haber informado a los afectados de quiénes serán destinatarios de los datos, así como de la finalidad que justifica la transferencia internacional y el uso de los datos que podrá hacer el destinatario.

El deber de información a que se refiere el párrafo anterior no será exigible, con carácter general, cuando la transferencia internacional tenga por objeto la prestación de un servicio al responsable del fichero por parte de un tercero, al que se le haya encargado el mismo en los términos establecidos por el artículo 12 de la LOPD.

En este último supuesto, para la redacción del correspondiente contrato de prestación de servicios el responsable del tratamiento podrá utilizar como referencia las cláusulas-tipo aprobadas por la Decisión 2002/16/CE, de la Comisión de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecido en terceros países de conformidad con la Directiva 95/46/CE.

⁹ Ver apartado 6.8 (nota 4).



3. Con independencia de lo anterior, en el caso particular de que la transferencia internacional se legitime mediante la obtención del consentimiento inequívoco del afectado, el responsable del fichero se asegurará de que éste ha sido previamente informado de los extremos citados en el apartado anterior.

Madrid, 17 de noviembre de 2005

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: José Luis Piñar Mañas

