LA PROTECCIÓN DE DATOS PERSONALES Y LAS RELACIONES LABORALES EN ESPAÑA Y FRANCIA: ANÁLISIS DE LAS RECOMENDACIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y LA *COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS* COMO EJERCICIO DE DERECHO COMPARADO PREVIO A UNA TRADUCCIÓN JURÍDICA

María Cristina TOLEDO BÁEZ*

Para citar este artículo puede utilizarse el siguiente formato:

María Cristina Toledo Báez (2010): "La protección de datos personales y las relaciones laborales en España y Francia: análisis de las recomendaciones de la Agencia Española de Protección de Datos y la *Commission Nationale de l'Informatique et des Libertés* como ejercicio de Derecho comparado previo a una traducción jurídica", en *Revista Crítica de Historia de las Relaciones Laborales y de la Política Social*, n.os 1-2 (diciembre 2010/enero 2011), pp. 36-56. En línea: www.eumed.net/rev/historia/01/mctb.htm.

RESUMEN: Desde el prisma de una traductora profesional, el presente artículo se centra en el estudio de la protección de datos personales en las relaciones laborales en España y Francia. Para ello, como ejercicio de derecho comparado previo a una traducción jurídica, se analizan de forma contrastiva tres objetos de estudio: en primer lugar, la normativa jurídica sobre la protección de datos personales desde una perspectiva general en ambos países; en segundo término, la normativa jurídica sobre el tratamiento de los datos personales de los empleados dentro de la empresa en los dos países implicados, y, en tercer lugar, las recomendaciones en materia de protección de datos personales de los empleados en el ámbito de los recursos humanos de la Agencia Española de Protección de Datos y su homóloga francesa la *Commission Nationale de l'Informatique et des Libertés* a través de, por un lado, la *Guía de protección de datos en las relaciones laborales* y, por otro, la *Guide pour les employeurs et les salariés*.

PALABRAS CLAVE: Protección de datos de carácter personal, Relaciones Laborales, España, Francia, Derecho comparado, Traducción jurídica.

RESUME: L'article fait référence à l'étude de la protection des données à caractère personnel dans le domaine des relations du travail en Espagne et en France, mais avec la particularité d'être abordé par une traductrice professionnel. Par conséquent, on fait un exercice de droit comparé préalable à une traduction juridique en analysant contrastivement trois objets d'étude : d'abord, le cadre juridique général de la protection des données à caractère personnel de chaque pays ; deuxièmement, le cadre juridique du traitement des données à caractère personnel obligatoire pour les

* Departamento de Didáctica de la Lengua y la Literatura. Universidad de Málaga. toledo@uma.es.

entreprises espagnoles et françaises ; troisièmement, les recommandations concernant la protection des données à caractère personnel des employés à être adoptées par le secteur des ressources humaines et qui ont été fixées par deux organismes homologues : d'une part, la *Guide pour les employeurs et les salariés*, publié par la Commission Nationale de l'Informatique et des Libertés ; d'autre part, la *Guía de protección de datos en las relaciones laborales*, écrite par l' Agencia Española de Protección de Datos.

MOTS CLE: Protection de données à caractère personnel, Relations du travail, Espagne, France, Droit comparé, Traduction juridique.

1. *Introducción*

A la hora de definir la traducción como proceso en Traductología, es lugar común considerar que traducir no se limita única y exclusivamente a trasvasar contenido de una lengua a otra, sino que implica la realización de otras actividades, entre las cuales destaca la fase de documentación, de forma que ciertos autores defienden que «el trabajo de traducción es en gran medida un problema de documentación»[1]. De esta forma, la capacidad para documentarse por parte del traductor, también denominada "subcompetencia heurística"[2], "competencia profesional e instrumental"[3] o "infocompetencia"[4], posee una importancia capital en el conjunto de destrezas o competencias que se le suponen al traductor[5]. Además, esta competencia cobra aún mayor relevancia en la traducción especializada, como es el caso que nos ocupa, ya que trabajaremos con textos jurídicos y, en este caso, «toda traducción jurídica requiere un ejercicio previo de derecho comparado»[6].

De este modo, el presente artículo[7] tiene como objeto realizar, desde el prisma del traductor profesional, un ejercicio de derecho comparado previo al siguiente encargo de traducción jurídica: la traducción de francés a español de la *Guide pour les employeurs et les salariés*[8] elaborada por la "Commission Nationale de l'Informatique et des Libertés" (CNIL)[9]. En España contamos con un texto oficial

[1] R. Mayoral Asensio, "La documentación en la traducción", en J. de Agustín (ed.), *Traducción, interpretación, lenguaje*, Fundación Actilibre, Madrid, 1994, p. 118.

[2] G. Corpas Pastor, "La competencia traductora. A propósito del texto médico", en C. Valero Garcés e I. de la Cruz Cabanillas (eds.), *Traducción y nuevas tecnologías. Herramientas auxiliares del traductor. Encuentros en torno a la Traducción 4*, Servicio de Publicaciones de la Universidad de Alcalá de Henares, Alcalá de Henares, 2001, p. 39.

[3] R. Rabadán y P. Fernández Nistal, *La traducción inglés-español: fundamentos, herramientas, aplicaciones*, Servicio de publicaciones de la Universidad de León, León, 2002, p. 396.

[4] D. Sales Salvador, *Documentación aplicada a la traducción: presente y futuro de una disciplina*, Ediciones Trea, Gijón, 2006, p. 13.

[5] A. Hurtado Albir, "La enseñanza de la traducción directa 'general'. Objetivos de aprendizaje y metodología", en A. Hurtado Albir (ed.), *La enseñanza de la traducción*, Universitat Jaume I, Castellón, 1996, p. 62.

[6] G. Corpas Pastor y J. Solís Becerra, "El contrato de aprovechamiento por turno en España y Reino Unido: un enfoque comparado", en *Revista Europea de Derecho de la Navegación Marítima y Aeronáutica*, XXI-XXII (2005), p. 3.212.

[7] El presente artículo ha sido realizado en el seno del proyecto *Ecoturismo: Espacio único de sistemas de información ontológica y tesauros sobre el medio ambiente* (Ref. n.º FFI2008-06080-C03-03/FILO. Ministerio de Ciencia y Tecnología. Dirección General de Investigación. VI Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica 2008-2011).

[8] Puede consultarse la *Guide pour les employeurs et les salariés*. [En línea: http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf].

[9] Para más información sobre la CNIL, visítese su sitio web oficial. [En línea: http://www.cnil.fr/].

similar, redactado por el organismo homólogo de la CNIL, la Agencia Española de Protección de Datos (AEPD)[10], que se denomina *Guía de protección de datos en las relaciones laborales*[11] y que nos servirá como texto comparable. Sin embargo, en lugar de proceder a traducir directamente, resulta imprescindible, por un lado, comprobar hasta qué punto coincide el marco jurídico de la protección de datos personales en ambos países y, por otro, llevar a cabo el necesario cotejo entre ambos documentos oficiales en aras de determinar sus similitudes y diferencias; en definitiva, una fase documental completa que nos permita acercar los rasgos terminológicos, fraseológicos, léxicos, morfosintácticos, semánticos, pragmáticos, conceptuales y textuales de las dos guías orientativas.

En consecuencia, en las páginas posteriores, como parte de la fase documental del encargo de traducción con temática jurídica, nos aproximaremos a la protección de datos personales en las relaciones laborales en España y Francia mediante el análisis contrastivo de nuestros tres objetos de estudio: en primer lugar, la normativa jurídica sobre la protección de datos personales desde una perspectiva general; en segundo lugar, la normativa jurídica sobre el tratamiento de los datos personales de los trabajadores dentro de la empresa; en tercer lugar, las recomendaciones de las autoridades de control española y francesa, esto es, la AEPD y la CNIL, en materia de protección de datos personales de los empleados en el ámbito de los recursos humanos. Hemos de precisar que nos limitaremos al apartado concerniente a los recursos humanos debido, de una parte, a que constituye uno de los temas abordados en las que coinciden las dos guías y, de otra, a que sería excesivo para un artículo de investigación analizar ambas guías en su totalidad ya que implicaría un ejercicio de Derecho comparado de mayor extensión.

2. *Protección de datos personales: definición, alcance y legislación*

En lo que respecta a nuestro primer objeto de estudio, la protección de datos de carácter personal constituye un asunto jurídico a la orden del día[12] en el que el conflicto entre la libertad de información y de tratamiento de los datos –junto con la libertad de expresión y la intimidad– emerge como uno de los grandes temas de nuestro tiempo y, además, provoca grandes y graves discrepancias doctrinales como consecuencia del hecho de que las tecnologías de la información y comunicación permiten nuevas maneras de injerencia en este ámbito protegido que no se habían planteado hasta la fecha[13]. Davara Rodríguez[14] ilustra este hecho con

[10] Véase la dirección URL de la AEPD. [En línea: https://www.agpd.es/portalwebAGPD/index-ides-idphp.php].

[11] La *Guía de protección de datos en las relaciones laborales* al completo se encuentra disponible en Internet. [En línea: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_relaciones_laborales.pdf].

[12] Consideramos que la protección de datos es uno de los grandes temas candentes desde el punto de vista jurídico junto con el tratamiento de la propiedad intelectual, en torno a la cual han reflexionado, entre otros, A. Castán, *La propiedad intelectual e industrial: garantía para la economía del conocimiento*, Círculo de Empresarios, Madrid, 2009; V. L. Montes Penadés y C. Becerra Bermejo, *Propiedad intelectual: aspectos civiles y penales*, Consejo General del Poder Judicial, Centro de Documentación Judicial, Madrid, 2008; E. Serrano Gómez (coord.), *El registro de la propiedad intelectual*, Sociedad de Gestión de España, Madrid, 2008.

[13] Al respecto, consúltese M. C. Toledo Báez, "Aproximación a la protección de datos personales en España, Inglaterra y Francia como ejercicio de Derecho comparado previo a una traducción", en *Contribuciones a las Ciencias Sociales*, marzo 2010. [En línea: http://www.eumed.net/rev/cccss/07/mctb.htm].

la siguiente afirmación: «La llamada protección de datos, entendida como la protección jurídica de las personas en lo que concierne al tratamiento de sus datos de carácter personal […] es un tema que ha adquirido enorme actualidad, casi diríamos protagonismo, y que afecta directamente a un derecho fundamental de elevado contenido».

Antes de abordar la legislación sobre la protección de datos personales, resulta preciso definir este concepto y para ello, recurriremos a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que en su artículo 3.a) da el siguiente concepto de datos de carácter personal: «Cualquier información concerniente a personas físicas identificadas o identificables». Como puede constatarse, se trata de una definición amplia, donde son dos los elementos esenciales: uno objetivo, la información, y otro subjetivo, relativo a la persona física. Tendrán, por tanto, la condición de dato personal no sólo el nombre, los apellidos, el número de afiliación, etc. de una persona física, sino «también imágenes, sonidos y voces». En esta dirección apunta la definición de datos de carácter personal desarrollada por el artículo 5.1.f) del Real Decreto 1729/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999: «Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo concerniente a personas físicas identificadas o identificables».

Por su parte, Davara Rodríguez[15] entiende por protección de datos: «El amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad».

En lo que concierne a la legislación sobre la protección de datos personales, como Estados miembros de la Unión Europea, España y Francia se rigen por el Derecho de la Unión Europea, orden jurídico *sui generis* que prevalece sobre el Derecho nacional. En consecuencia, estos Estados comparten la normativa reguladora europea sobre la legislación en torno a la protección de los datos personales a través de la transposición de directivas emanadas del Parlamento Europeo y del Consejo. Sin embargo, dentro de sus competencias y siempre que no se incumpla el Derecho de la Unión Europea, cada Estado puede crear sus propios instrumentos de regulación.

Con estos rasgos como telón de fondo, pasamos a continuación a analizar la legislación de la protección de los datos de carácter personal en España y Francia.

2.1. *Normativa jurídica en España*

Desde el punto de vista legal, el punto de partida en nuestro país de la protección de datos personales lo marca el artículo 18.4 de la Constitución española, el cual establece que «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». Partiendo de este precepto, nos encontramos ante un bloque normativo[16] que se

[14] M. A. Davara Rodríguez, *La protección de datos personales en el sector de las comunicaciones electrónicas*, Universidad Pontificia Comillas, Madrid, 2003, p. 14.

[15] M. A. Davara Rodríguez, *Manual de derecho informático*, Aranzadi, Cizur Menor, 2002, p. 47.

[16] Al respecto, véanse M. Vilasau Solana, "Derecho de intimidad y protección de datos personales", en M. Peguera Poch (coord.), *Derecho y nuevas tecnologías*, Universitat Oberta de Catalunya, Barcelona, 2005, pp. 98-99; E. Santos Pascual e I. López-Vidriero Tejedor, *Protección de datos personales: Manual práctico para empresas*, Fundación Confemetal, Madrid, 2005, pp. 27-28; R. Tascón López, *El tratamiento por la empresa de datos personales de los trabajadores: análisis del estado de la cuestión*, Thomson-Civitas, Cizur Menor, 2005; N. N. Tur Faúndez, "Deberes de

aplica de forma más o menos inmediata y que se inicia con la Ley General para la Defensa de los Consumidores y Usuarios, de 19 de julio de 1984, modificada en diferentes ocasiones y de la que resulta de interés, en particular, el régimen de las cláusulas abusivas.

A continuación, surge la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, que vino a regular el citado artículo 18.4 de la Constitución y por la que se creó en 1993 la Agencia de Protección de Datos, con respecto a la cual hemos de destacar el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba su Estatuto.

Otro elemento importante es el Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el Título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunicaciones, derogado en 2003 para satisfacer la exigencia de la Directiva europea 2002/58/CE, CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Dentro de este marco jurídico, en materia de protección de datos emergen como piedras angulares, por un lado, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que derogó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automático de Datos de Carácter Personal, y, por otro, el Real Decreto 994/1999, de 11 de junio, que aprobó el Reglamento de Medidas de Seguridad. La LOPD constituye la transposición al ordenamiento jurídico español 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; además, el artículo 79 de la LOPD establece que la Agencia de Protección de Datos pasará a denominarse Agencia Española de Protección de Datos (AEPD). Cabe apuntar que la LOPD ha sido modificada en parte por la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, si bien la LOPD sigue siendo el texto de referencia en lo que a protección de datos se refiere. Atañe también a la LOPD el 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, capital en la materia que nos ocupa ya que especifica los principios de protección de datos, los derechos de acceso, rectificación, cancelación y oposición y las disposiciones aplicables a determinados ficheros de titularidad privada, de lo cual daremos cuenta más adelante (cf. apartado 3.1.).

Otros hitos significativos en esta materia lo constituyen, de una parte, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), de la cual algunos preceptos han sido modificados por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y, de otra, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones y que supone la transposición a nuestro ordenamiento jurídico de la Directiva 2006/24/CE del Parlamento Europeo

información y documentación", en S. Cavanillas Múgica, M. N. Tur Fáundez, M. T. Benito Roser y C. S. Romero de Terreros, *Turismo y comercio electrónico. La promoción y contratación* on line *de servicios turísticos*, Comares, Granada, 2001, p. 32; R. De Rosselló Moreno, *El comercio electrónico y la protección de los consumidores*, Cedecs, Barcelona, 2001, p. 24; S. Cavanillas Múgica, "La protección del consumidor y la sociedad de la información: una revisión estratégica", en *Revista General de Legislación y Jurisprudencia*, 4 (1999), p. 438.

y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

Asimismo, destaca el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, y que cumple con la previsión recogida en la disposición final quinta de la Ley 44/2006, de 29 de diciembre, de mejora de la protección de los consumidores y usuarios, que habilita al Gobierno para que, en el plazo 12 meses, proceda a refundir en un único texto la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios y las normas de transposición de las directivas comunitarias dictadas en materia de protección de los consumidores y usuarios.

Como última ratio resultan aplicables el Código penal, en concreto los artículos 197 a 201 y 417, que sancionan aquellas conductas que se consideran más graves, y el Código Civil, cuyo art. 1.280 establece un listado de contratos sujetos a ciertas formalidades.

En el contexto de Internet y también en materia de protección de datos en las relaciones laborales, es preciso hacer referencia a los elementos de autorregulación que surgen. Un ejemplo de esta actividad lo constituyen los denominados *códigos tipo*, una clase de códigos de conducta que pueden acordar un grupo de empresas o las administraciones públicas. Se establece una serie de reglas, condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad, políticas en el tratamiento de los datos personales, etc. En nuestro país se dividen en códigos inscritos en el Registro General de Protección de datos, como el Farmaindustria, firmado el 17 de junio de 2009, o el de la Universidad de Castilla, con fecha 16 de noviembre de 2009, y en códigos tipo inscritos en Registros Autonómicos de Protección de Datos e incluidos en el Registro General de Protección de Datos, ejemplo de los cuales es el Código Tipo para las entidades locales adheridas a EUDEL (Asociación de Municipios Vascos-Euskadiko Udalen Elkartea)[17].

2.2. *Normativa jurídica en Francia*

El manejo de datos personales constituye un tema de gran interés en el país galo y, por ello, el marco jurídico que lo protege es bastante amplio, en parte herencia del ordenamiento jurídico de Derecho continental al que pertenece. Las normativas de mayor relevancia[18] comienzan, como no podía ser de otra forma, con la anteriormente nombrada ley n.º 78-17 de 6 de enero de 1978 «relative à l'informatique, aux fichiers et aux libertés», la cual marca el inicio de la protección legislativa de los datos personales y que refleja, además, el carácter precursor francés en materia de protección de datos al aprobarse con tanta antelación en comparación con el resto de países europeos. Por ende, constituye el texto de referencia para la protección de datos de carácter personal en Francia y fue

[17] Más códigos tipo disponibles. [En línea: https://www.agpd.es/portalweb/canaldocumentacion/códigos_tipo/index-ides-idphp.php#rgpd].

[18] Para más información consúltense A. Debet, "Mesure de la diversité et protection des données personnelles", en Informe para la *Commission Nationale de l'Informatique et des Libertés*, 2007. [En línea: http://www.egaltraitement.net/modules/xfsection/article.php?articleid=67&category=1]; J. King, *Sécurité informatique et protection de la vie privée - Je vous dépanne en 5 minutes*, First Interactive Éditions, Paris, 2006; A. Belleil, *E-privacy: le marché des données personnelles: protection de la vie privée à l'âge d'Internet*, Dunod, Paris, 2001.

modificado posteriormente por la ley n.º 2004-801 de 6 de agosto de 2004 sobre la protección de las personas físicas en lo que respecta a tratamiento de datos personales, ley que reguló disposiciones no recogidas en la ley n.º 78-17 y que hacían referencia, entre otras cosas, al tratamiento de datos en medios electrónicos.

Son de aplicación también en esta materia el artículo 1316 del *Code civil*, que vela por el cumplimiento de la legalidad en documentos y firmas electrónicas, y los artículos 287 y 288-1 del *Code de procédure civile*, los cuales se ocupan de la verificación y validez de escritos en papel o electrónicos en función de la firma de las partes.

En protección de datos resulta imprescindible, como veremos más adelante, la labor de la ya citada *Commission Nationale de l'Informatique et des Libertés*, cuyas funciones quedan estipuladas a instancias del Decreto n.º 2005-1309 de 20 de octubre de 2005, por el que se fijan las formalidades obligatorias previas a cualquier tratamiento de datos, como son la notificación de ficheros o las solicitudes de autorización de tratamiento de datos, así como así como los poderes de control, investigación, injerencia y sanción de la CNIL. El reglamento interno de dicho organismo queda fijado mediante la *délibération* n.º 2006-147 de 23 de mayo de 2006.

Otros tres elementos fundamentales en protección de datos en la sociedad de la información son, en primer lugar, el Decreto n.º 2007-1527, de 24 de octubre de 2007, concerniente al derecho de respuesta aplicable a los servicios de comunicación en línea y que modifica en parte, en concreto el art. 6, de la ley n. º 2004-575; en segundo lugar, la Ley n.º 2008-3, de 3 de enero de 2008, que se ocupa del desarrollo de la competencia a la hora de ofrecer servicios a los consumidores, en la cual el capítulo I del título II está consagrado a las medidas específicas para las comunicaciones electrónicas, y que constituye la transposición de la Directiva 2001/95/CE relativa a la seguridad general de productos; en tercer lugar, la Ley n.º 2008-696, de 15 de enero de 2008, relativa a los archivos y protección de datos de distinta índole. Por último, es aplicable el Decreto de 7 de abril de 2009 relativo a la comunicación por vía electrónica ante los *tribunaux de grande instance*[19].

3. *Protección de datos personales en las relaciones laborales*

Sobre nuestro segundo objeto de estudio, comenzaremos apuntando que son numerosos los agentes que intervienen en las relaciones laborales y que manejan datos de carácter personal de trabajadores. Cabría destacar, por ejemplo, a intermediarios de la colocación, la Seguridad Social y entidades colaboradoras, mutuas de accidentes, aseguradoras, representantes de los trabajadores, gestorías, abogados. En el marco de estas relaciones, se recoge gran cantidad de información de los empleados que afecta tanto a la vida profesional como a la personal.

López Vidriero Tejedor y Santos Pascual[20] recalcan que la obligación del cumplimiento de la normativa sobre protección de datos personales está

[19] El *Tribunal de Grande Instance* equivaldría en el sistema jurídico español a la Audiencia Provincial, si bien existe una diferencia fundamental entre ambos organismos: mientras que la Audiencia Provincial puede conocer asuntos en segunda instancia (recurso de apelación), en Francia esta segunda instancia es competencia de la *Cour d'Appel*, que tiene una única sede por región. Ver N. A. Campos Plaza, J. Cantera Ortiz de Urbina, A. M. García Calero, M. D. Espinosa Sansano y E. Ortega Arjonilla, *Diccionario jurídico-económico francés-español/español-francés*, Editorial Comares, Granada, 2005, p. 20.

[20] *Op. cit.* p. 20.

especialmente ligada con la actividad cotidiana de las empresas, dado que constituyen un activo importante. Una de las implicaciones graves a la hora de tratar datos personales son los importantes riesgos económicos y de imagen que se ocasionan como consecuencia del incumplimiento de la normativa vigente en materia de protección de datos personales.

Por todo lo anterior, es deber, obligación y responsabilidad del titular de una empresa salvaguardar los datos personales de sus trabajadores y, a continuación, estudiaremos las medidas adoptadas al respecto en nuestros dos países objeto de estudio.

3.1. *En España*

En nuestro país, en el momento en el que se constituye una empresa y trata datos de carácter personal de los clientes, proveedores y empleados, dicha empresa será la responsable de los ficheros a los efectos previstos en la anteriormente citada LOPD. Cabe apuntar que, de acuerdo con el artículo 3 de dicha ley, se entiende por fichero «todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso». Tal y como especifican Santos Pascual y López Vidriero-Tejedor[21], dependiendo de quién sea el titular del fichero, entidad pública o privada, serán denominados de forma diferente –ficheros de titularidad pública o ficheros de titularidad privada– y su creación, modificación o supresión deberán seguir pautas distintas. La AEPD especifica en el artículo 24.1 de su Estatuto los distintos titulares de ficheros que se encuentran en pleno derecho para la inscripción de sus ficheros, a saber: la Administración General del Estado, las entidades y organismos de la Seguridad Social, los órganos autónomos del Estado, las sociedades estatales y entes del sector público, las Administraciones de las Comunidades Autónomas y de sus Territorios Históricos, las entidades que integran la Administración local y los entes y organismos dependientes de la misma, cualesquiera otras personas jurídico-públicas, así como las personas privadas, físicas o jurídicas. En consecuencia, queda patente que toda institución pública o privada que posea un fichero de datos de carácter personal relativo a personas físicas, ya sea automatizado o no, tiene la obligación de solicitar su inscripción en el Registro General de Protección de Datos.

En estrecha relación con los ficheros al tratarse de su contenido, es necesario recalcar que no todos los datos personales contenidos en ficheros gozan del mismo estatus de acuerdo con la LOPD ya que diferenciamos tres niveles: 1. En primer lugar, los datos altos, datos de nivel alto o datos especialmente protegidos, que incluyen datos de ideología, datos de religión, datos de creencias, datos de origen racial, datos de salud, datos de vida sexual, así como los datos recabados para fines policiales sin consentimiento de las personas afectadas. 2. En segundo lugar, los datos medios o de nivel medio, dentro de los cuales encontramos una doble diferenciación: por un lado, información general, que alude al conjunto de datos respecto de los cuales podemos obtener un perfil del afectado, ejemplo de los cuales serían los currículos gestionados y organizados por una determinada empresa; por otro lado, información específica, a través de la cual se muestran datos relativos o que hagan referencia a infracciones administrativas o penales de acuerdo con el artículo 29 de la LOPD, Hacienda Pública, servicios financieros, ficheros de morosos o impagados, etc. 3. Por último, los datos bajos o de nivel básico, para los cuales la normativa en materia de protección de datos no establece un listado cerrado o

[21] *Op. cit.* pp. 32-33.

numerus clausus de los datos que la misma considera como básicos o de sensibilidad mínima. Por ende, en aras de poder dilucidar éstos, es preciso delimitar los datos de nivel medio y alto y, una vez realizado, podemos concluir que pertenecerán al nivel básico el resto de datos de carácter personal que almacenemos y tratemos, tales y como el nombre, los apellidos, el documento nacional de identidad, la dirección postal, el correo electrónico, la edad, etc.

La pertenencia de un dato a un nivel o a otro determinará la adopción de medidas de seguridad de distinta índole atendiendo a la naturaleza de la información tratada en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma.

En lo que respecta a los deberes y las obligaciones del responsable del fichero, se regulan a través del título II de la LOPD y se concretan en siete principios, si bien destacaremos cinco de ellos: los principios de consentimiento, información, calidad de datos y finalidad, seguridad y deber de guardar secreto. En cuanto al primero, el consentimiento se constituye como un derecho inherente al afectado y, conjuntamente, como deber del responsable del tratamiento. Como regla general, la inclusión de datos de carácter personal en un fichero supondrá que el posterior tratamiento de los mismos requerirá, en principio, el consentimiento del afectado, excepto en supuestos tasados por la LOPD. Los cuatro requisitos inherentes para la legalidad de este principio son que el consentimiento sea libre, específico, informado e inequívoco.

Respecto al principio de información, bajo este principio descansa uno de los pilares más importantes de la normativa en materia de producción de datos de carácter personal[22]. La información que debe prestar o facilitar el responsable, en este caso las empresas, a los afectados o interesados, no sólo es un deber sino que se configura como un derecho inherente de aquéllos.

En cuanto al principio de calidad de los datos y finalidad, sobre él se sustentan la recogida, el almacenamiento y el tratamiento de los datos de carácter personal. La exigencia de calidad de los datos conlleva la necesidad y pertinencia de los mismos respecto a la finalidad para la cual fueron recabados, debiendo proceder a la cancelación de los mismos, sin previo consentimiento del afectado, cuando los datos sean inexactos o fueran recabados con otra finalidad[23]. De esta forma, el principio de calidad de los datos se basa en cuatro requisitos o parámetros, a saber, finalidad, utilización no abusiva ni excesiva, exactitud y legalidad en la recogida.

En lo que concierne al principio de seguridad, señalamos que el responsable de los ficheros debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos. Debe atenderse a lo establecido en el Real Decreto 994/1999, de 11 de junio, que establece las concretas medidas de seguridad para cada uno de los niveles (básico, medio o alto). Normalmente, a los ficheros de personal se les deberá aplicar medidas de seguridad de nivel alto, ya que la AEPD ha indicado que los partes de baja, confirmación y alta son considerados datos de salud, y por tanto el nivel de protección aplicable es el alto. El

[22] Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional: «En primer lugar, debe tenerse en cuenta que nos hallamos ante la regulación del derecho a la información a la recogida de datos, derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos […]».

[23] Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 9 de marzo de 2001, en la interpretación de los artículos 4.4 y 4.5 de la LOPD: «La norma establece la obligación del responsable del fichero de proceder de oficio y con la debida diligencia a cancelar los datos inexactos o que han dejado de ser necesarios para la finalidad del fichero y sin necesidad de solicitud previa del afectado».

mismo nivel de seguridad es exigido si se tratan datos relativos a la afiliación sindical. Recordamos que el responsable debe elaborar, mantener e implantar de forma efectiva un Documento de Seguridad.

Por último, el principio del deber de guardar secreto se fundamenta en el artículo 10 de la LOPD, el cual exige a quienes intervengan en cualquier fase del tratamiento de los datos a guardar secreto profesional sobre los datos, subsistiendo la obligación aún después de finalizar su relación con el responsable del fichero.

En este orden de cosas, es importante destacar que un despacho profesional que gestiona, por ejemplo, las nóminas del personal de una empresa (responsable del fichero) es considerado como encargado del tratamiento. Éste no decide sobre la finalidad, el contenido y el uso de los ficheros, sino que es el responsable del fichero el que, a través de la suscripción obligatoria de un contrato escrito entre ambos, establece las directrices, instrucciones y finalidades a las que se debe de atener dicho encargado.

En lo que respecta a los derechos de los afectados, resumiremos brevemente que la LOPD, como garante de nuestra privacidad e intimidad, reconoce los siguientes: derecho de acceso, que podrá ser ejercitado cuando el afectado quiera conocer con exactitud los datos personales que dispone de él un tercero; derecho de rectificación cuando el afectado desee que sus datos sean modificados bien porque hayan sufrido un cambio, bien porque se encuentren incompletos; derecho de cancelación, si el afectado desea que sus datos, o parte de ellos, no vuelvan a ser tratados por el responsable del fichero; y, por último, derecho de oposición, el cual ofrece la posibilidad de negarnos a que un tercero recabe, o que posteriormente trate, nuestros datos de carácter personal.

Para concluir este apartado, especificaremos que, tal y como detallaremos más adelante (cf. apartado 4), la protección de datos en el ámbito laboral se proyecta en tres momentos: 1) en el tratamiento de datos en la fase de contratación o proceso de selección de personal, 2) en el desarrollo de la relación de trabajo y 3) en el momento de cesar la relación laboral. Y en todos ellos el empresario ha de atenerse a la LOPD con el fin de ser consciente de los riesgos que pueden afectar al derecho de la intimidad del trabajador.

3.2. *En Francia*

A tenor del marco normativo especificado en el apartado 2.2., es notorio que Francia constituye uno de los países precursores en materia de protección de datos personales gracias a la ley de 6 de enero de 1978, modificada posteriormente por la ley de 6 de agosto de 2004. En cuanto a las obligaciones del empresario como responsable del tratamiento de los datos personales, tanto la CNIL como la ley de 1978 establecen los siguientes parámetros: seguridad de los ficheros, confidencialidad de los datos, duración de la conservación de los datos, información a los afectados, autorización por parte de la CNIL y finalidad del tratamiento de datos. Respecto al primero de ellos, la seguridad de los ficheros, en virtud del artículo 34 de la ley de 1978 y de la *délibération* n.º 02-017[24] de la CNIL, los responsables del tratamiento informático de los datos personales están obligados a adoptar medidas de seguridad físicas (seguridad de los locales), lógicas (seguridad de los sistemas de información) y adaptadas a la naturaleza de los datos y a los posibles riesgos del tratamiento de los mismos. En caso de no respetar la obligación

[24] *Délibération* n.º 02-017, de 21 de marzo de 2002, sobre la adopción de una recomendación relativa a la recogida y tratamiento de datos nominativos durante el procedimiento de selección de personal. [En línea: http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/15/].

de seguridad, el responsable de los datos será sancionado con cinco años de prisión y con 300.000 euros de multa a tenor de lo estipulado en el artículo 226-17 del *Code pénal* francés.

El segundo principio, la confidencialidad de los datos, se asegura que únicamente podrán acceder a los datos personales contenidos en un fichero las personas autorizadas, ya sean los destinatarios designados explícitamente, ya sean terceros autorizados como Hacienda o la Policía. El artículo 226-22 del *Code pénal* establece que la comunicación de datos a personas no autorizadas se castiga con cinco años de prisión y con 300.000 euros de sanción; asimismo, la divulgación de datos realizada por imprudencia o negligencia se sanciona con tres años de prisión y 100.000 euros de multa.

En cuanto a la duración de la conservación de los datos, se estima que los datos personales poseen fecha de caducidad y, en consecuencia, el responsable de los ficheros ha de fijar un período razonable de conservación de los datos en función del objetivo del fichero. En este caso, el artículo 226-20 del Código Penal de nuestro país vecino sanciona la conservación de los datos por un período superior al estipulado con cinco años de prisión y con una sanción de 300.000 euros.

La información a los afectados constituye un principio fundamental en protección de datos y, a tenor de lo estipulado en el artículo 7 de la ley de 1978, el responsable de un fichero está obligado a permitir que los afectados ejerzan sus plenos derechos en lo que concierne a sus datos. Por ello, el responsable ha de comunicar a los afectados sobre los siguientes aspectos de los ficheros: la identidad, la finalidad del tratamiento, el carácter obligatorio o facultativo de las respuestas, los destinatarios de la información, la existencia de derechos, entre otros. A este respecto, el artículo 131-13 del *Code pénal* castiga con 1.500 euros, y con 3.000 en caso de reincidencia, toda obstaculización al ejercicio de los plenos derechos de los afectados. Si fundamental es la información a los afectados, igual relevancia adquiere el principio de autorización por parte de la CNIL, ya que el tratamiento informático de los datos personales que presenten mayor riesgo de abuso en lo que concierne a los derechos y las libertades de los empleados estará sometido a la autorización de la CNIL antes de su ejecución. En caso de no cumplir lo ordenado por la CNIL, se sanciona al responsable del fichero con cinco años de prisión y con 300.000 euros de multa de acuerdo con el artículo 226-16 del Código Penal francés.

Para terminar, cabe resaltar la importancia de la finalidad del tratamiento de datos, para la cual el artículo 6 de la ley de 1978 determina que los ficheros de datos han de tener un objetivo concreto y, en consecuencia, la información contenida en los mismos ha de ser coherente con el objetivo marcado. Los datos personales no podrán emplearse fuera de la finalidad para la que han sido recabados y cualquier infracción en lo que respecta a la finalidad del tratamiento de los datos se sancionará con cinco años de prisión y 300.000 euros de multa en virtud de lo estipulado en el artículo 226.21 del *Code pénal*.

Huelga decir que, si se compara este apartado con el anterior, tanto España como Francia, al seguir directivas europeas, poseen obligaciones comunes para el responsable del fichero de datos, en este caso el empresario. Asimismo, el afectado posee los mismos derechos que en España tal y como queda reflejado en el artículo 40 de la ley de 1978, el cual reproducimos a continuación: «Cualquier persona física que acredite su identidad tiene derecho a exigir al responsable del tratamiento que sus datos sean, según el caso, rectificados, completados, actualizados, ocultados o

borrados si son inexactos, incompletos, erróneos, obsoletos, o cuya recogida, utilización, comunicación o conservación esté prohibida»[25].

Queda comprobar cuáles son las recomendaciones emitidas por autoridades de control española y francesa encargadas de velar por la protección de datos y comprobar hasta qué punto coinciden o discrepan, a lo cual dedicaremos el apartado siguiente.

4. *Las recomendaciones de la Agencia Española de Protección de Datos y de la "Commission Nationale de l'Informatique et des Libertés" en materia de protección de datos personales en recursos humanos*

Una vez detallados la normativa y el marco jurídico de la protección de datos personales y las relaciones laborales en España y Francia, pasamos a continuación a analizar nuestro tercer objeto de estudio y, al mismo tiempo, encargo de traducción jurídica: las guías elaboradas en la materia de protección de datos en las relaciones laborales por parte de dos organismos homólogos, los cuales, hasta este punto, se han nombrado pero sin detallar sus características. Nos referimos, claro está, a la Agencia Española de Protección de Datos, por un lado, y a la *Commission Nationale de l'Informatique et des Libertés*, por otro. Ambos organismos se regulan a instancias 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 en todos los Estados de la Unión Europea se han ido creando organismos similares, de forma que actualmente los 27 Estados miembros, así como los países del Espacio Económico Europeo (Islandia, Liechtenstein y Noruega), disponen, de una parte, de una ley sobre la protección de los datos personales y, de otra, de una autoridad independiente de control. El conjunto de los organismos encargados de velar por la protección de los datos personales, agrupados bajo el nombre "Grupo de trabajo sobre protección de datos del artículo 29"[26], se reúne con frecuencia en Bruselas para aconsejar a la Comisión Europea en materia de iniciativas legislativas en aras de armonizar las prácticas o recomendaciones relativas a la protección de datos y otras cuestiones relacionadas con las tecnologías de la información.

La AEPD constituye un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada y que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se creó en 1993[27] y lleva a cabo numerosas funciones, siendo la general y prioritaria velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y

[25] El texto original en lengua francesa queda como sigue: « Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ».

[26] La AEPD facilita en su sitio web los documentos adoptados por el grupo del artículo 29 en lengua española [En línea: https://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/index-ides-idphp.php]. La Comisión Europea de Justicia ofrece más información al respecto en su sitio web. [En línea: http://ec.europa.eu/justice/policies/privacy/index_en.htm].

[27] El Real Decreto 428/1993, de 26 de marzo, aprobó el Estatuto de la Agencia Española de Protección de Datos, si bien su creación se aprobó a instancias de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, referida anteriormente en el apartado 2.1.

cancelación de datos. En relación con los afectados, la agencia se ocupa de atender a sus peticiones y reclamaciones, informar de los derechos reconocidos en la Ley y promover campañas de difusión a través de los medios. Por su parte, en relación con quienes tratan datos, la AEPD está en la obligación de emitir autorizaciones previstas en la Ley, requerir medidas de corrección, ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos, ejercer la potestad sancionadora, recabar la ayuda y la información que precisa y autorizar las transferencias internacionales de datos. Su labor en lo que concierne a la elaboración de normas es informar los Proyectos de normas de desarrollo de la LOPD, informar los Proyectos de normas que incidan en materias de protección de datos, dictar instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD y dictar recomendaciones en materia de seguridad y control de acceso a los ficheros. Asimismo, en materia de telecomunicaciones, la AEPD tutela los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente. Otras funciones dignas de mención son velar por la publicidad en los tratamientos, publicando anualmente una lista de los mismos, cooperación internacionalmente, representar a España en los foros internacionales sobre protección de datos, controlar y observar lo dispuesto en la Ley reguladora de la Función Estadística Pública y elaborar una memoria anual que se presenta por conducto del Ministro de Justicia a las Cortes.

Por su parte, la CNIL se creó a instancias de la ley de 1978 que le otorga el estatus de autoridad administrativa independiente. Su misión principal es proteger la vida privada y la libertad en la actual sociedad de la información y sus funciones específicas son, entre otras, informar de los derechos que reconoce la ley de 1978, desarrollar iniciativas de formación y de sensibilización, recibir las quejas de ciudadanos sobre abusos o prácticas irregulares, proponer al gobierno medidas legislativas o reglamentarias en aras de adaptar la protección de la libertad y la vida privada a la evolución de la tecnología, informar a los responsables de los datos personales sobre sus obligaciones, regular e informar de los ficheros de datos y ejercer la potestad sancionadora.

Tras exponer las características principales de las dos agencias y tras determinar que ambas se ocupan de velar por el cumplimiento de la protección de datos, nos centraremos en las recomendaciones de ambas en materia de protección de datos en el seno de la empresa, esto es, en las relaciones laborales.

La *Guía de protección de datos en las relaciones laborales*, elaborada por la AEPD en 2009 con motivo de la celebración de la 31 Conferencia Internacional de la Privacidad[28], se redactó con el fin de examinar aspectos de la protección de datos que, o bien resultan fundamentales desde el punto de vista de la aplicación y el cumplimiento normativo, o bien han planteado dificultades de interpretación o aplicación práctica. Por ello, la *Guía* se planteó como objetivo primordial considerar un conjunto de aspectos prácticos a los que las empresas deben enfrentarse habitualmente. El documento se divide en cuatro apartados: recursos humanos, prevención de riesgos laborales, controles empresariales y relaciones con los sindicatos.

[28] La página de información de la 31 Conferencia Internacional de la Privacidad está disponible en Internet. [En línea: http://www.privacyconference2009.org/home/index-iden-idweb.html].

En lo que respecta a la *Guide pour les employeurs et les salariés*, redactada por la CNIL en 2010, aspira a informar a los empleados de los derechos de los que dispone y a los empresarios de las medidas que se han de adoptar conforme a la ley de 1978. En suma, se marca como fin dar las claves prioritarias a la hora de manejar ficheros con datos en recursos humanos y en otros aspectos de las relaciones laborales. La organización de la *Guide* difiere de la de su homóloga española ya que se estructura en torno a 12 apartados, a saber: proceso de selección de personal, anuarios de personal, acceso a archivos profesionales, gestión de obras sociales y culturales, transferencia internacional de datos, control de la utilización de Internet, administradores de red, videovigilancia en el trabajo, gestión de la telefonía, dispositivos de geolocalización, utilización de aparatos de fichar en el trabajo y biometría en la empresa.

En nuestro caso, como ya hemos aclarado anteriormente (cf. Introducción), nos centraremos en los apartados de recursos humanos de ambas guías, sección en la que las dos coinciden (la otra sección en las que ambas trabajan aborda los controles biométricos en la empresa), si bien es preciso señalar que, con el fin de lograr una traducción fructífera, sería necesario cotejar las recomendaciones en su totalidad, labor que no realizaremos en el presente artículo por ser de mucha enjundia para nuestro objetivo prioritario. Además, somos conscientes de que dicha labor implicaría un ejercicio de Derecho comparado de mayor extensión que englobase, entre otros temas, las relaciones sindicales, los controles en la empresa, la prevención de riesgos laborales, la transferencia internacional de datos o la biometría empresarial. En consecuencia, compararemos ambas guías centrándonos en dos aspectos de los recursos humanos: de una parte, selección de personal; de otra, contratación y desarrollo de la prestación laboral.

4.1. *Selección de personal*

Ambas guías se centran en la gestión de personal en lo relativo a los procesos de captación y uso de su información. No obstante, hemos de remarcar que la guía francesa es más exhaustiva que la guía española, si bien, con el fin de conocer al detalle las recomendaciones ofrecidas en cada ámbito, comenzamos por resumir las especificaciones de la CNIL: 1. Los datos que pueden recogerse. Se especifica que la información recabada ha de tener por finalidad considerar si el candidato posee la capacidad necesaria para ocupar el empleo en cuestión, motivo por el cual dicha información ha de guardar relación directa y necesaria con el puesto vacante o con las aptitudes profesionales del candidato. Se detalla que, salvo en determinados casos plenamente justificados, no es pertinente la recogida de los siguientes datos: fecha de la entrada al país; fecha de obtención de la nacionalidad francesa; modalidad de adquisición de la nacionalidad francesa; nacionalidad de origen; número de afiliación al régimen de la Seguridad Social; detalles sobre la situación militar (por ejemplo, si se es objetor de conciencia); dirección postal anterior; entorno familiar del candidato (apellido, nombre, nacionalidad y profesión del cónyuge ni apellido, nombre, nacionalidad y profesión de padres, suegros, hermanos e hijos); estado de salud, altura, peso, vista, etc.; si se es propietario o inquilino de una vivienda; vida asociativa y, por último, datos bancarios: domiciliaciones, préstamos, retrasos en pagos, etc. A continuación, se especifica la información que no puede recogerse por tratarse de datos especialmente protegidos como son datos sobre orígenes raciales o étnicos; opiniones políticas, filosóficas o religiosas; pertenencia a sindicatos; datos relativos a la salud y la vida sexual. Asimismo, en la *Guide*, en concreto en su página 9, se explica que en la zona “comentarios” destinada a

recoger información sobre el trabajador, ha de contener datos pertinentes, adecuados y relacionados con el fin del tratamiento. De acuerdo con la CNIL, en 2006 se llevó a cabo una inspección laboral y se constató la existencia de comentarios subjetivos sobre empleados de una empresa que no habían cumplido su trabajo de forma satisfactoria tales como "demasiado pesado", "problemas de higiene (olor nauseabundo)", "persona sin dientes y que bebe", etc. Conforme a los artículos 45 y siguientes de la ley de 6 de 1978 modificada en 2004, la CNIL sancionó el 11 de diciembre de 2007 a la empresa en cuestión con una multa que ascendía a los 40.000 euros[29]. 2. Información a los candidatos: En la página 9 de la *Guide* se detalla que, a la hora de recoger datos, se ha de informar a los candidatos sobre: la identidad del responsable de tratamiento de los datos (por ejemplo, departamento de selección de personal X, servicio de recursos humanos de la empresa Y); la finalidad del tratamiento de los datos (por ejemplo, la gestión de candidatos); el carácter obligatorio o facultativo de las respuestas (por ejemplo, la recogida de información sobre actividades de tiempo libre es facultativa); las consecuencias en el caso de obviar una respuesta; las personas físicas o morales destinatarias de la información (por ejemplo, otros departamentos de personal) y las condiciones del ejercicio de su derecho de acceso y rectificación así como el derecho de oposición (por ejemplo, indicación del servicio en el cual pueden ejercer estos derechos). En este punto, la CNIL recomienda que los trabajadores encargados de seleccionar personal informen al candidato, dentro de un plazo razonable de su situación como candidato (es decir, si ha sido seleccionado, rechazado, etc.), de la duración de la conservación de los datos que le conciernen así como de la posibilidad de exigir su restitución o destrucción, de cualquier cesión de información a otros organismos de selección de personal y de la posibilidad de oponerse a tal acto y de los métodos y técnicas de ayuda a la selección de personal que le atañen. La CNIL recomienda que, en los casos en los que la identidad de la empresa permanezca oculta durante una oferta de empleo, se obtenga el consentimiento del candidato antes de enviar su currículo a dicha empresa. 3. Ejercicio de los derechos por parte del empleado: Cualquier candidato o empleado, tras solicitud en forma y dentro de un plazo razonable, tiene derecho a disponer de los resultados de los análisis y test psicológicos, grafológicos, etc. así como de la evaluación profesional practicada. El derecho de acceso se aplica, asimismo, a la información que dispongan terceros implicados en la relación laboral. La CNIL aconseja que la comunicación de la información contenida en el fichero del candidato se efectúe por escrito. 4. Período de conservación de los datos de un candidato: La CNIL detalla que el período de conservación de toda información en soporte electrónico o en papel no exceda de los dos años tras el último contacto con el candidato en cuestión.

En lo que respecta a la *Guía de protección de datos en las relaciones laborales*, dentro de la sección "Recursos Humanos", el apartado "Información sobre el tratamiento de los datos personales. Modalidades" (p. 8), especifica las siguientes recomendaciones:

1. En procedimientos de selección de personal: El primer tratamiento de datos personales puede producirse cuando el futuro trabajador sea un simple candidato a un puesto. Para ello deben tenerse en cuenta algunas cautelas:
   - Es conveniente, cuando los recursos lo permitan, disponer de modelos de impresos tipo para la formalización del currículo y de un procedimiento de

[29] Se trata de la *délibération* de la CNIL n.°2007-374 de 11 de diciembre de 2007 .

formalización y entrega de los mismos por los candidatos, ya que ello permite no sólo informar adecuadamente sino definir con precisión el tipo de datos a tratar, establecer las medidas de seguridad, etc.
- Si para la selección de personal se realiza algún tipo de anuncio o convocatoria pública debería incluirse en ella la información del artículo 5 de la LOPD.
- Si el currículo se presenta directamente por el candidato sin habérsele solicitado deben fijarse procedimientos de información que supongan algún acuse o confirmación de conocer las condiciones en las que se desarrollará el tratamiento.
- En casos de grupos de empresas o de cualquier otra fórmula de colaboración empresarial debe tenerse en cuenta que la cesión de los datos contenidos en el currículum o del propio documento debe contar con el consentimiento del candidato[30].

2. Consideración de los datos especialmente protegidos: En aras de garantizar la correcta protección de datos que, bien por su naturaleza religiosa o ideológica, bien por pertenecer al núcleo más íntimo de la persona, resultan merecedores de una especial protección, se ha de disponer de procedimientos:
   - Una adecuada información en la recogida de datos. A este respecto aluden los procedimientos de la AEPD n.º 0029/2004[31] y 00525/2007, en los que se especifica que «la posibilidad de admitir un consentimiento expreso que no conste por escrito para el tratamiento de los datos de salud, se encuentra condicionada a que pueda acreditarse que es una manifestación de voluntad libre, inequívoca y específica» (p. 12).
   - Antes de recabar este tipo de datos es necesario analizar la proporcionalidad del tratamiento y la legitimación para el mismo. A este respecto, la AEPD especifica que es posible que para la adaptación de un puesto deban conocerse algunos datos de salud; sin embargo, ello no legitima al empresario para incorporar y tratar los datos de salud en sus sistemas de información salvo que cuente con un servicio de prevención de riesgos laborales o un servicio médico de empresa (p. 13).
   - El tratamiento de este tipo de datos se proyecta sobre la organización ya que exige adoptar medidas de seguridad de nivel alto, salvo en las excepciones previstas por el Reglamento de desarrollo de la Ley Orgánica de protección de datos. No obstante, debe recordarse que la normativa permite adaptar las medidas a la estructura real del sistema de información.

Dado que el objetivo de nuestro artículo es ofrecer un análisis contrastivo de las recomendaciones de las dos autoridades independientes de control, resumimos a continuación las características más significativas de los aspectos estudiados por cada una de ellas en materia de selección de personal. En lo que concierne a las características de las recomendaciones de la CNIL, hemos de resaltar que se centra en el dato específico ya que se concretan los datos personales cuya recogida no es

[30] A este respecto, véase el Procedimiento n. PS/00239/2007 de la AEPD. [En línea: https://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2007/common/pdfs/PS-00239-2007_Resolucion-de-fecha-21-12-2007_Art-ii-culo-10-LOPD.pdf].

[31] Se puede consultar en su sitio web. [En línea: https://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2004/common/pdfs/PS-00029-2004_Resolucion-de-fecha-03-11-2004_Art-ii-culo-7.3-LOPD.pdf].

pertinente mediante un listado exhaustivo. Asimismo, se detalla el tipo de datos que pueden ofrecerse en la zona “comentarios”, pues no ha de tratarse de información subjetiva o incluso denigrante y se especifica la información que se le debe ofrecer al candidato cuando se recojan datos. Es significativa la especificación de la información que se ha de aportar al candidato sobre la candidatura, la conservación de los datos, la cesión de información y los métodos y técnicas de ayuda a la selección de personal que le atañan; en relación con lo anterior, se indica el derecho de información que tiene el candidato a un puesto de disponer de los resultados de los análisis y tests psicológicos, grafológicos, etc., o de la evaluación profesional practicada.

Otras recomendaciones dignas de destacarse son, por un lado, la recomendación de obtener el consentimiento del candidato cuando se envíe su currículo a una empresa cuya identidad haya permanecido oculta y, por otro, la recomendación de conservar la información en soporte electrónico o en papel por un período que no exceda de los dos años. En este orden de cosas, la CNIL determina que el derecho de acceso se aplica a la información que dispongan terceros implicados en la relación laboral y declara que la comunicación de la información contenida en un fichero se comunique preferentemente por escrito.

En lo que respecta a las características de las recomendaciones de la AEPD, cabe recalcar que se centran en aspectos muy concretos de selección de personal y, en particular, en acciones que han de llevarse a cabo cuando se traten datos que pertenezcan al currículo de un candidato. En concreto, se aconseja disponer de modelos de impresos tipo para la formalización del currículo y de un procedimiento de formalización y entrega de los mismos por parte de los candidatos, se especifica que los anuncios o las convocatorias públicas de empleo han de contener la información del artículo 5 de la LOPD, se debe acusar recibo de la entrega del currículo por parte del candidato, se detalla que la cesión de datos contenidos en un currículo debe contar con el consentimiento del candidato y, para terminar, se concretan los procedimientos de tratamiento de datos especialmente protegidos, a saber, una adecuada información en la recogida de datos incluso con consentimiento, una análisis de la proporcionalidad del tratamiento y legitimación para el mismo, una organización de medidas de seguridad de nivel alto, salvo en las excepciones previstas por el Reglamento de desarrollo de la LOPD.

Por tanto, podemos determinar que, en lo que selección de personal se refiere, las recomendaciones de la CNIL son más concretas y más centradas en el dato que las ofrecidas por la AEPD, la cual se limita a reiterar lo estipulado en la LOPD añadiendo información contenida en diversos procedimientos. En el caso de la guía francesa, hallamos incluso ejemplos específicos de mala praxis en lo que concierne a comentarios vertidos por el departamento de selección de personal. Asimismo, se especifican dos elementos clave: por un lado, el derecho que tiene el candidato a un puesto de disponer de los resultados de los análisis y evaluaciones de su candidatura; por otro, la recomendación de obtener el consentimiento del candidato cuando se envíe su currículo a una empresa cuya identidad haya permanecido oculta, lo cual coincide en parte con la recomendación de la AEPD de obtener el consentimiento del candidato para la cesión de datos contenidos en un currículo. Un aspecto primordial en el que coinciden las guías de la AEPD y de la CNIL es en el tratamiento de los datos especialmente protegidos, aunque la CNIL presenta una lista más detallada.

4.2. *Contratación y desarrollo de la prestación laboral*

Las recomendaciones que emite la CNIL en cuanto a la contratación y al desarrollo de la prestación laboral aluden, por un lado, a las bases de datos profesionales y, por otro, a los datos profesionales de cada trabajador.

En cuanto a las bases de datos profesionales, la CNIL recomienda lo siguiente (p. 12):

1. Las bases de datos tanto internas (disponibles únicamente para el personal de una empresa) como externas (accesible a más usuarios al publicarse, por ejemplo, en Internet) con información del personal de una empresa no deben emplearse para fines comerciales o políticos.
2. Previamente a la constitución de la base de datos, el empresario debe informar a sus empleados por escrito (sea en papel, sea por vía electrónica) de sus derechos de acceso, rectificación y oposición.
3. La difusión en Internet de los datos de carácter personal (por ejemplo, apellido, nombre, datos profesionales, etc.) implica que cualquier usuario de la Red puede acceder a dicha información, de ahí que el empleado pueda oponerse en todo momento a tal difusión.
4. En caso de que se pretenda publicar en Internet una fotografía de un empleado, la CNIL recomienda que la difusión de dicha fotografía esté sujeta a un acuerdo previo entre el empleado y el empresario.
5. Las bases de datos profesionales internas han de notificarse a la CNIL mediante una declaración de conformidad en virtud de la norma 46[32] relativa a la gestión del personal de organismos públicos y privados, excepción hecha de si se ha designado en el seno de la empresa un *correspondant informatique et libertés* (CIL)[33], esto es, un enlace o corresponsal entre la CNIL y la empresa. Respecto a las bases de datos profesionales externas, se notifican mediante una declaración normal, salvo si, como en el caso anterior, dicha empresa posee un CIL.

Respecto a los datos profesionales de cada trabajador, la CNIL presenta las recomendaciones que siguen a continuación (p. 13):

1. Derecho de acceso a determinados datos: Cualquier empleado o antiguo empleado puede acceder a sus datos profesionales como trabajador y, en concreto, puede consultar, entre otra, información relativa a su entrevista de trabajo y posterior selección, su historial laboral, su remuneración, la evaluación de sus competencias profesionales y su expediente disciplinario.
2. Límites del derecho de acceso: Por el contrario, un empleado o antiguo empleado no tiene el derecho de acceder a datos que atañen a la situación personal de terceros, en particular de otros empleados y a datos sobre su promoción profesional, salvo si dichos datos se han tenido en cuenta para un aumento de salario.
3. Ejercicio del derecho de acceso: El derecho de acceso puede ejercerse tanto en persona como por escrito. El empresario está obligado a responder inmediatamente si la petición se realiza en persona o en un período de dos meses si se efectúa por escrito. Un eventual rechazo del derecho de acceso ha de manifestarse por escrito y mencionar las posibles vías de recurso.

Por su parte, las recomendaciones que propone la AEPD en cuanto a la contratación y el desarrollo de la prestación laboral son las siguientes:

[32] Disponible para su consulta. [En línea: http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/169/].

[33] La *Guide du Correspondant Informatique et Libertés* puede consultarse en su sitio web. [En línea: http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Guide_correspondants.pdf].

1. Respecto a la contratación, el contrato es un medio adecuado para informar al trabajador respecto del tratamiento que se realizará respecto de sus datos. No obstante, no debe confundirse la información con la manifestación del consentimiento. Por ello, el contrato de trabajo constituye un medio adecuado para ofrecer información sobre los tratamientos directamente relacionados con la prestación laboral, si bien no es así para otros tratamientos (p. 10). Además, no exime del deber información sobre todos aquellos nuevos tratamientos de datos personales que la empresa decida realizar con carácter posterior al nacimiento de la relación laboral (p. 13).
2. Durante el desarrollo de la prestación laboral, dado que las relaciones laborales son dinámicas y pueden estar sujetas a cambios sobrevenidos tanto desde el punto de vista del trabajador como desde la perspectiva de la empresa, será necesario informar al trabajador en todos aquellos casos en los que se produzcan cambios que afecten al tratamiento de los datos personales como la aparición de nuevas finalidades o de nuevos tratamientos (p. 13).

Como ocurre con la selección de personal, las recomendaciones de la CNIL son más detalladas que las emitidas por la AEPD y, de hecho, casi podríamos afirmar que ambas guías se centran en la contratación y la prestación laboral pero desde dos perspectivas distintas: la CNIL, desde el prisma de la responsabilidad del titular de una empresa, presta una mayor atención a los datos del trabajador que dicha empresa contiene en su base de datos o en su dossier y a su posterior tratamiento, mientras que la AEPD, reiterando lo articulado en la LOPD, toma como base la información que el empresario ha de proporcionarle al empleado sin ahondar en datos personales concretos ni en su ulterior tratamiento.

No obstante, la diferencia más significativa entre las recomendaciones de ambos organismos, y que además enfatiza en la superioridad francesa a la hora de proteger los datos personales, radica en la existencia en el país galo de un *correspondant informatique et libertés* (CIL), un enlace o corresponsal entre la CNIL y la empresa y cuya labor reside en proporcionar información a la empresa sobre las recomendaciones de la CNIL y de las exigencias de la ley francesa de 1978. Estimamos encomiable la creación de este tipo de corresponsal y consideramos que, a nuestro juicio, sería una gran aportación para la AEPD contar con esta figura en nuestro país.

Tras este cotejo del tratamiento de los datos personales en los departamentos de recursos humanos de las empresas, estamos en condiciones de afrontar con éxito la traducción de francés a español de la *Guide pour les employeurs et les salariés* elaborada por la CNIL ya que tendremos en cuenta las siguientes consideraciones: 1ª) El texto comparable de la *Guía de protección de datos en las relaciones laborales* es más exigua que el texto origen en francés y entra en menos detalles. 2ª) La guía francesa cuenta con un número mayor de apartados mejor definidos que la guía española, la cual centra su atención en los cuatro apartados anteriormente señalados: recursos humanos, prevención de riesgos laborales, controles empresariales y relaciones con los sindicatos. 3ª) En contraposición, la guía española aborda un abanico más amplio de temas que la guía española pasa por alto, como son la prevención de riesgos laborales y las relaciones con los sindicatos, ya que la *Guide* se centra, *grosso modo*, en recursos humanos, control empresarial y transferencia de datos personales. 4ª) La traducción al español de la *Guide* exige una traducción explicativa y detallada de la figura del *correspondant informatique et libertés* (CIL), al cual se le dedica un apartado de la guía francesa, dado que constituye una figura inexistente en nuestro país. 5ª) La guía francesa contiene al

final una serie de anexos en los que aparecen distintos formularios de gran utilidad sobre todo para el titular de una empresa y cuya traducción exigiría una adaptación o naturalización por parte del traductor.

4. *Conclusiones*

En el presente artículo nos hemos aproximado a la protección de datos personales en las relaciones laborales desde una perspectiva no jurista, sino en calidad de traductores profesionales que, ante un encargo de traducción jurídica, han de documentarse previamente y realizar un ejercicio de Derecho comparado.

Tres han sido nuestros objetos de estudio analizados de forma contrastiva. En lo que respecta al primero de ellos, la normativa jurídica sobre la protección de datos personales, hemos resaltado la importancia de la protección de datos personales como tema candente desde el punto de vista jurídico dado que las tecnologías de la información y comunicación permiten nuevas maneras de injerencia, tanto en lo laboral como en lo personal, que no se habían planteado hasta la fecha. A continuación, hemos definido, por un lado, el concepto de dato de carácter personal y, por otro, el de protección de datos de carácter personal para pasar, seguidamente, a detallar las principales normativas que regulan la protección de datos en España y Francia. En este punto, hemos de resaltar que ambos países comparten gran parte de la normativa jurídica debido a que ambos países se rigen por el Derecho de la Unión Europea, orden jurídico *sui generis* que prevalece sobre el Derecho nacional.

Respecto al segundo objeto de estudio, hemos resaltado que la protección de los datos de carácter personal en las relaciones laborales es de vital importancia debido a los numerosos agentes que intervienen en las relaciones entre empresas y que manejan datos personales de los trabajadores. Por ello, es deber, obligación y responsabilidad del titular de una empresa salvaguardar los datos personales de sus empleados. Tras el análisis contrastivo de las características de la protección de datos personales y las relaciones laborales en España y Francia, hemos comprobado que, al seguir directivas europeas, hallamos numerosos rasgos comunes: los afectados poseen los mismos derechos respecto a sus datos en la empresa y a los titulares de empresa o los responsables de ficheros de datos les corresponde las mismas obligaciones de cumplir los principios de consentimiento, información, finalidad, seguridad, deber de guardar un secreto y conservación de los datos. Otro aspecto en el que coinciden nuestros dos países objeto de análisis es en la necesidad que tienen las empresas de conseguir la autorización de la AEPD o de la CNIL respectivamente cuando se traten datos personales que presenten mayor riesgo de abuso en lo que concierne a los derechos y las libertades de los empleados.

En cuanto al tercer objeto de estudio, en primer lugar, hemos descrito tanto la AEPD como la CNIL en lo que respecta a sus procesos de creación y a sus funciones principales y, en segundo lugar, hemos comparado la *Guide pour les employeurs et les salariés* y la *Guía de protección de datos en las relaciones laborales*, texto origen y texto comparable respectivamente para el encargo de traducción encomendado. Hemos constatado que ambas guías presentan estructuras diferentes, siendo la francesa más prolija en apartados y la española más centrada en cuatro aspectos de las relaciones laborales. En concreto, en nuestro caso hemos estudiado los apartados dedicados a los departamentos de recursos humanos en las empresas y, más específicamente, en dos secciones: de

una parte, selección de personal; de otra, contratación y desarrollo de la prestación laboral.

El análisis comparativo de las recomendaciones de la CNIL y la AEPD con respecto a la selección de personal nos lleva a concluir que recomendaciones de la CNIL son más concretas y más centradas en el dato que las ofrecidas por la AEPD, la cual se limita a reiterar lo estipulado en la LOPD. Sin embargo, un aspecto primordial en el que coinciden las guías de la AEPD y de la CNIL es en el tratamiento de los datos especialmente protegidos, aunque la CNIL presenta una lista más detallada.

Por su parte, gracias al cotejo de las recomendaciones de las dos autoridades independientes de control en materia de contratación y desarrollo de prestación laboral, constatamos que, al igual que ocurre con la selección de personal, las recomendaciones de la CNIL son más detalladas que las emitidas por la AEPD e incluso cabría afirmar que cada organismo adopta una perspectiva distinta: la CNIL presta una mayor atención a los datos del trabajador que dicha empresa contiene en su base de datos o en su dossier y a su posterior tratamiento y la AEPD toma como base la información que el empresario ha de proporcionarle al empleado.

Como colofón del presente artículo, hemos detallado las precauciones que han de tomarse a la hora de afrontar con éxito la traducción de francés a español de la *Guide pour les employeurs et les salariés* de entre las cuales destacamos la necesidad de optar por una traducción explicativa y detallada de la figura del *correspondant informatique et libertés* (CIL) dado que constituye una figura inexistente en nuestro país. No obstante, somos conscientes de que habría que ampliar el estudio contrastivo entre ambas guías y sus correspondientes normas jurídicas en aras de completar una fase documental adecuada que permita traducir de forma efectiva.

Recibido el 15 de diciembre de 2010, corregido del 21 al 23 de diciembre de 2010 y aceptado el 24 de diciembre de 2010.