10593/02/ES
WP 73

Documento de trabajo sobre la administración en línea

Adoptado el 8.5.2003

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[1],

Visto el artículo 29, así como la letra a) del apartado 1 y el apartado 3 del artículo 30 de dicha Directiva,

Visto su reglamento interno, y en particular sus artículos 12 y 14,

HA ADOPTADO EL PRESENTE DOCUMENTO DE TRABAJO:

INTRODUCCIÓN

El desarrollo de la administración en línea constituye hoy en día uno de los ejes de acción prioritarios de la política de modernización de la administración de la mayoría de los Estados miembros. Tal prioridad se expresa asimismo a escala europea con la adopción por el Consejo Europeo de Feira de junio de 2000 del «plan de acción eEurope 2002», que incluye un capítulo sobre «administración en línea».

De momento podemos observar el desarrollo de diferentes tipos de proyectos de administración en línea que consisten en la creación y la promoción del suministro de procedimientos administrativos en línea. El éxito de algunos de ellos depende de complejas cuestiones relacionadas con la protección de datos que se habrán de estudiar atentamente.

A título de ejemplo podemos mencionar el establecimiento de puntos de entrada únicos a los servicios de administración en línea, la creación de identificadores únicos y la interconexión de las bases de datos públicas.

Este documento tiene por objetivo presentar la situación de la administración en línea y la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales en la Unión Europea y pretende contribuir a la reflexión sobre este tema. El documento, elaborado por la delegación francesa, sintetiza las respuestas dadas por las Autoridades de protección de datos representadas en el Grupo de trabajo a un cuestionario sobre el tema.

Teniendo en cuenta la evolución constante de los servicios de administración en línea y las conclusiones extraídas de las experiencias desarrolladas en este ámbito, el Grupo de trabajo podría retomar en el futuro estas cuestiones para seguir ofreciendo orientación sobre la aplicación de las normas de la Directiva 95/46/CE en este contexto.

[1] DO L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

A. CONSULTA E INICIATIVAS DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS RELATIVAS A LA ADMINISTRACIÓN EN LÍNEA

Todas las Autoridades europeas de protección de datos expresaron sus opiniones sobre las cuestiones relacionadas con la administración en línea.

1. En la inmensa mayoría de los casos, las autoridades públicas habían realizado consultas oficiales a las Autoridades de protección de datos. En general, cuando la administración toma medidas legislativas o reglamentarias con repercusiones en la protección de los datos o en la aplicación de determinados procedimientos administrativos en línea, obliga a que se realicen estas consultas, para cumplir los procedimientos establecidos en su legislación sobre protección de datos. A este respecto, diversas Autoridades mencionaron que las autoridades no respetan sistemáticamente esta obligación de consulta a la Autoridad. En ocasiones la administración consulta a la Autoridad espontáneamente en cuestiones relativas a la administración en línea.

2. Las Autoridades pueden asimismo expresar su opinión en debates públicos o con motivo de reflexiones sobre el tema planteadas por las autoridades públicas. Así se hizo en Francia, donde la CNIL (Comisión nacional de informática y libertades) participó, a petición del gobierno, en el debate público sobre estas cuestiones y publicó en su informe anual sus primeros elementos de reflexión sobre el tema, o en el Reino Unido, cuyo Delegado de información, al que las autoridades públicas no habían consultado oficialmente, manifestó su opinión comentando diversas propuestas del gobierno y participando en consultas públicas.

3. Las Autoridades de protección de datos pueden expresar también su opinión en relación con la administración en línea por iniciativa propia. En los Países Bajos, por ejemplo, la Autoridad tomó la iniciativa de expresar sus opiniones sobre el tema sin ningún motivo especial.

4. Por último, algunas Autoridades forman parte de grupos de trabajo sobre proyectos concretos centrados en la administración en línea (Finlandia, Países Bajos, Francia) o han pedido que se les informe de la evolución de determinados proyectos (Portugal).

Las consultas e iniciativas de las Autoridades se pueden referir al marco general del desarrollo de la administración en línea o a cuestiones específicas.

Las contribuciones de las diferentes delegaciones dan una idea de la gran diversidad de los temas tratados por las Autoridades. Puede tratarse, por ejemplo, de una opinión sobre proyectos globales, como, en España, la creación de una tarjeta de identidad electrónica o la ejecución de un proyecto general de promoción de la administración en línea; en Suecia, la ejecución de una «política común» de la Asociación de Banqueros Suecos y Correos relativa a la tarjeta de identidad electrónica; en Italia, además de la emisión de una tarjeta de identidad electrónica, la ejecución de un proyecto nacional de creación de

una «red de la administración pública unificada», esto es, una red electrónica que conectará a todas las autoridades administrativas del país.

Por otra parte, algunas Autoridades de protección de datos han intervenido en la aplicación de procedimientos administrativos en línea específicos, como, en relación con la imposición a las personas físicas, la declaración del impuesto sobre la renta en línea y el pago en línea; en relación con la seguridad social, la declaración en línea y el reembolso de los costes sanitarios (España, Francia), etc. En estos casos, las Autoridades de protección de datos insisten especialmente en la cuestión de la seguridad de los datos.

Por último, otro desencadenante de la expresión de opiniones puede ser la introducción de ciertos textos en la legislación nacional, tales como la Directiva Europea sobre la firma electrónica (en particular en Finlandia, donde la ley que la transpone entrará en vigor el 1 de febrero de 2003, en Dinamarca, donde la Autoridad de protección de datos ha expresado su opinión sobre el proyecto legislativo correspondiente, y en España, donde la Autoridad de protección de datos ha publicado un informe sobre el proyecto legislativo).

B. SITUACIÓN DE LOS PROCEDIMIENTOS ADMINISTRATIVOS EN LÍNEA

Con esta pregunta se pretendía averiguar el nivel de desarrollo alcanzado en cada país por los procedimientos administrativos en línea, así como el nivel de seguridad correspondiente aplicado, teniendo en cuenta la lista de los 20 procedimientos básicos que se han de ofrecer en línea con arreglo al plan de acción eEurope establecido con vistas al Consejo Europeo de Feira de junio de 2000. Sólo 8 países cumplimentaron el cuadro.

Excepto Bélgica y Alemania, se consultó a todas las Autoridades de protección de datos sobre los proyectos de procedimientos administrativos en línea ejecutados en su país.

En general, las observaciones de las Autoridades de protección de datos se referían principalmente a las medidas de seguridad, y más concretamente a las de identificación y autenticación de los usuarios, así como de los agentes o profesionales autorizados a acceder a aplicaciones de procedimientos administrativos en línea. Asimismo, el cifrado de los datos durante su transmisión se recomienda en general, además, aunque en menor medida, del cifrado durante el almacenamiento de los datos y el uso de registradores de datos y ficheros históricos (Portugal, Países Bajos, Francia, Austria).

Además, las Autoridades de protección de datos convienen en que el desarrollo de los procedimientos administrativos en línea debe ir acompañado de medidas de información a los ciudadanos, en particular acerca de los derechos que les confieren las leyes sobre protección de datos.

1. En primer lugar, todos los países mencionados más arriba ofrecen a las personas físicas la posibilidad de recurrir a un procedimiento de declaración del impuesto sobre la renta en línea, que a menudo va unido a la posibilidad de pago en línea (6 países) y de consulta del expediente personal en línea (también 6 países).

Igualmente, entre los procedimientos administrativos en línea que se ofrecen a las empresas, el servicio que se menciona con mayor frecuencia es el de la declaración del IVA (8 países) o los impuestos directos (6 países).

Así pues, el sector de las finanzas públicas constituye sin lugar a dudas el ámbito de intervención privilegiado de la administración en línea. Conviene señalar que, por lo general, los procedimientos administrativos en línea que se ofrecen en este ámbito se caracterizan por un nivel de seguridad más elevado, pues varios países declaran contar con sistemas de firma electrónica (Finlandia, España, Francia) o de cifrado de los datos (Francia, Portugal, España). En Austria la seguridad se controla únicamente con el uso de contraseñas.

2. La notificación administrativa de cambio de dirección, que constituye una gestión administrativa habitual (e incluso obligatoria) en un gran número de países, es, por detrás de las gestiones fiscales, el procedimiento administrativo en línea más mencionado: 6 países indican que ofrecen tal servicio[2], en 3 de ellos (España, Finlandia, Noruega) asociado a la posibilidad de consultar en línea el expediente personal. Dependiendo de los países, a estos servicios se les aplican diferentes niveles de seguridad, que en algunos casos (España, Finlandia) consisten en sistemas de firma electrónica.

3. El siguiente procedimiento en línea es la búsqueda de empleo, que también está disponible en 6 países[3], en algunos casos completado con la posibilidad de consultar en línea el propio expediente (3 países). Normalmente se accede a estos procedimientos mediante nombres de usuario y contraseñas, es decir, con procedimientos de seguridad tradicionales.

   Se mencionaron otros procedimientos en línea, como las solicitudes de permisos de obras, los préstamos en bibliotecas públicas, la solicitud de documentos al registro civil, los procedimientos de registro de nuevas empresas, las cargas sociales, las relaciones de los usuarios con los profesionales de los centros sanitarios, la matrícula en escuelas y universidades, las inscripciones en exámenes, la matriculación de coches, el reembolso de gastos médicos y, por último, el registro de demandas (policía, justicia, etc.), éste último asociado, en general, a un servicio de envíos por correo.

   El análisis de las respuestas aportadas por las Autoridades de protección de datos sobre la seguridad de los procedimientos mencionados muestra una gran disparidad de situaciones, excepto en el caso de algunos servicios, sin duda considerados más «delicados» (por ejemplo, la matriculación de coches, la validación del reembolso de gastos médicos, etc.) y que parecen requerir medidas de seguridad específicas. Por lo tanto, no se puede extraer ninguna conclusión significativa, excepto la de que de momento ningún país (salvo, quizás Finlandia y Dinamarca) tiene una idea clara de qué requisitos de seguridad son necesarios en las aplicaciones de la administración en línea.

[2] Dinamarca, España, Finlandia, Italia, Noruega, Países Bajos.

[3] Dinamarca, Finlandia, Francia, Italia, Noruega, Portugal.

C. CREACIÓN DE UN PUNTO DE ENTRADA ÚNICO, O «PORTAL», A LOS PROCEDIMIENTOS ADMINISTRATIVOS EN LÍNEA

1. Generalidades

En casi todos los países estudiados existe o está previsto crear un portal o punto de entrada único a los procedimientos administrativos en línea. Esta tendencia general se da en los países que ya contaban con sitios que funcionan como portales más o menos independientes y en aquéllos en los que no existía ningún sistema previo.

En algunos casos hay un Ministerio concreto a cargo del portal, por ejemplo, el portal finlandés http://www.suomi.fi y el del gobierno federal austriaco, http://www.help.gov.at, ambos gestionados por sus correspondientes Ministerios de Hacienda.

Normalmente, estos portales son de información general y contienen vínculos a los diferentes servicios públicos e institucionales, listas de direcciones de las administraciones y las instituciones públicas, documentación informativa, extractos de boletines oficiales relativos a diferentes procedimientos (formularios, información sobre procedimientos administrativos, información sobre ayudas financieras, solicitudes de financiación, licitaciones, ofertas de empleo público), información sobre la legislación nacional, acontecimientos, «buzón de sugerencias», publicaciones, etc.

Cada vez es más frecuente que estos portales se usen también para acceder a procedimientos administrativos en línea relacionados con los ciudadanos o con las empresas. Surge así la cuestión de la posible retención de datos personales en el portal. En la actualidad, estos sitios no retendrían datos personales en Dinamarca, Alemania, España, Portugal y Suecia. En cambio, pueden o podrán retenerlos en Bélgica, Italia, Noruega, Finlandia, Austria (sólo si el ciudadano está entrando en un procedimiento para el cual sea indispensable que se identifique) e Irlanda.

En este último país, el sistema, que preverá el registro en línea, consiste en la autenticación de la identidad mediante un número personal atribuido por el servicio público (PPSN, *person's Public Service Number*) y la prestación de los servicios públicos mediante un agente que almacenará los datos personales en una especie de cámara central de seguridad (*data vault*). La identidad de una persona se autenticará a través de la base de datos de identificación para los servicios públicos del Ministerio de Asuntos Sociales y Familiares, que contiene detalles identificativos básicos. El sistema impondrá otros requisitos de autenticación para transacciones más seguras y confidenciales.

El acceso a los servicios a través del agente exigirá el consentimiento individual, y no se podrá exigir a nadie que utilice el sistema para acceder a los servicios. El agente almacenará en una cámara de seguridad los datos personales que se usen con frecuencia (por ejemplo, los relativos al nacimiento, el pasaporte, los ingresos, las relaciones familiares, etc.) y los gestionará y protegerá en beneficio del usuario. Los datos sólo se darán a conocer a una agencia de servicios públicos cuando el usuario dé instrucciones concretas, en caso de transacción, con motivo de un servicio en el que intervenga el agente. Se desarrollarán políticas de seguridad adecuadas para los diferentes servicios y los datos personales de la cámara de seguridad se cifrarán.

Una vez desarrollado el sistema, el agente podrá prever ciertos sucesos (una pensión, por ejemplo) y cada categoría del sistema podrá sugerir cuestiones de interés para el individuo. Por medio del portal, el agente ofrecerá una «ventanilla única» a las personas que hagan uso de los servicios públicos. Paulatinamente, a medida que se sucedan las visitas, los servicios se podrán ir personalizando. La administración podrá garantizar que la vida privada del usuario se respeta, pues éste habrá dado su consentimiento para que sus datos se utilicen y almacenen de este modo con miras a la prestación del servicio de que se trate. La Autoridad irlandesa ha aprobado el uso de este modelo siempre y cuando se apliquen condiciones estrictas de protección de datos relativas al consentimiento y al uso de los datos para determinados fines.

La Autoridad neerlandesa también trató la cuestión y llamó la atención de la administración sobre las repercusiones, en la protección de los datos, de la distinción operativa entre los servicios de contacto con el ciudadano (atención al público) y los encargados del manejo de los ficheros. Los primeros recogen todos los datos necesarios para la prestación de los servicios solicitados por el ciudadano y los segundos los usan para estimar la posición del ciudadano en relación con cada uno de ellos. De este modo, la administración puede establecer una ventanilla única para prestar varios servicios. La administración recurre cada vez más a esta estructura organizativa, cuyos servicios de portal y «ventanilla única» son emblemáticos. En su informe anual, la Autoridad neerlandesa insistió en que en estas circunstancias las administraciones deben definir estrictamente las responsabilidades de cada departamento en relación con los datos tratados, con el fin de evitar que los servicios encargados de su manejo los utilicen o difundan ilegalmente.

2. Recurso a proveedores externos privados que puedan almacenar datos personales de los usuarios o tener acceso a ellos

La proximidad entre la administración en línea y los procedimientos comerciales en línea y, por consiguiente, la posibilidad de que los procedimientos administrativos en línea se encarguen a empresas privadas, llevan a considerar diversos elementos relacionados con la organización técnica de los servicios públicos en línea. Por ejemplo, ¿cómo pueden las empresas privadas garantizar la igualdad de trato en los procedimientos públicos? ¿cómo cobran? ¿implica esto que habría que pagar por ciertos procedimientos administrativos en línea?

Estas preguntas no obtuvieron las mismas respuestas en los diferentes países de la Unión Europea.

Alemania, Italia, España, los Países Bajos, Suecia y Noruega se decantaban por no recurrir a proveedores privados con acceso a los datos personales de los usuarios. No obstante, en la mayor parte de dichos países, y sobre todo en España, las autoridades públicas recurren a proveedores externos privados para el desarrollo de los productos o los portales, por ejemplo. En España, además, se pide la cooperación de proveedores privados para llevar a cabo planes de auditoría del desarrollo de la planificación del portal.

En Bélgica, Dinamarca, Francia (ocasionalmente), Finlandia y Austria se opta por lo contrario: cualquier proveedor privado puede solicitar el reconocimiento tras demostrar su capacidad de garantizar la seguridad necesaria, especialmente en relación con la protección de los datos. En cambio, la cuestión no está clara en Portugal y el Reino

Unido, donde, sin embargo, no existen objeciones de principio al recurso a proveedores externos privados.

Ningún país ha recurrido al servicio sobre pasaportes ofrecido por Microsoft en el marco de los proyectos de administración en línea, y algunas Autoridades carecen de información concreta al respecto.

3. Dictamen de la Autoridad sobre estos temas y reacción de la administración

No todas las Autoridades de protección de datos se han tenido que enfrentar con cuestiones relacionadas con la creación de un portal en su país, principalmente porque no todos los proyectos en curso exigen el registro de datos a través del portal.

Antes al contrario, las Autoridades de los países en que el tratamiento de los datos personales se realiza a través del portal respondieron insistiendo en que el recurso a proveedores externos sólo se podría plantear una vez puestas en práctica las garantías específicas necesarias. Así pues, en los diferentes requisitos resultantes de las recomendaciones de las diferentes autoridades se mencionan las garantías siguientes: contrato adecuado con las entidades encargadas del tratamiento de los datos; determinación exacta de las misiones de los proveedores externos privados; determinación de los requisitos de seguridad (entorno protegido y totalmente automatizado); cumplimiento de requisitos jurídicos específicos (acreditación) por los proveedores externos privados, incluida en particular la prohibición de utilizar los datos para fines distintos de aquéllos para los que fueron recogidos, o la prohibición de revelarlos; determinación precisa de los datos registrados; posible creación de un comité inspector, etc.

D. SISTEMAS NACIONALES DE IDENTIFICACIÓN DE PERSONAS (USO DE IDENTIFICADORES ÚNICOS O SECTORIALES PARA ACCEDER A CIERTOS SERVICIOS ADMINISTRATIVOS EN LÍNEA)

En primer lugar, conviene recordar que, hasta ahora, sólo Bélgica, Dinamarca, España, Finlandia, Irlanda, Italia, Luxemburgo, Noruega y Suecia han implantado un identificador único y general a escala nacional. En otros países existen proyectos de desarrollo de identificadores únicos, en particular en Austria, pero únicamente como un número de origen oculto para los identificadores sectoriales (véase más abajo). En Dinamarca, Bélgica y España, este identificador único convive con los sectoriales, mientras que en los otros países sólo existen identificadores sectoriales: Alemania (número de la seguridad social, número del pasaporte), Francia y Portugal (básicamente, número de la seguridad social) y Grecia y los Países Bajos (identificador relativo a los impuestos sociales, en particular). Recordemos que en países como Alemania y Portugal se considera inconstitucional recurrir a un identificador único.

El desarrollo de la administración electrónica constituye a veces una ocasión adecuada para volver a diseñar este sistema de identificadores o ampliar el alcance de un identificador sectorial. De momento, sólo Portugal y Austria han indicado que esta evolución haya supuesto una revisión de sus sistemas nacionales de identificación personal.

1. La tendencia general para acceder a los procedimientos administrativos en línea es recurrir a identificadores preexistentes, ya sean únicos (Bélgica,

Dinamarca, España, Irlanda) o sectoriales (Francia, Países Bajos, Portugal, Italia). En algunos de los países en que no existen identificadores únicos, se sostuvo que la creación por la administración de un portal personalizado no debería constituir una ocasión para establecerlos (Francia, en particular). Austria representa un caso particular a este respecto, pues próximamente creará un número de identificación único (el número del registro de residentes) que no se deberá almacenar fuera del registro de residentes y sólo se usará para definir identificadores sectoriales por medio de un procedimiento especialmente protegido. Ninguna autoridad pública está autorizada a almacenar números de identificación de sectores ajenos a sus competencias.

2. En algunos países se consideraron, o aún se están considerando, proyectos de ampliación de identificadores sectoriales con fines de acceso a procedimientos administrativos en línea. El gobierno de los Países Bajos renunció a un proyecto de generalización del identificador fiscal social, tras la emisión de un dictamen negativo por la Autoridad. En la actualidad, tal proyecto sólo existe en Italia, donde está previsto generalizar el identificador fiscal para obtener un identificador único que permita acceder a determinados procedimientos administrativos en línea. En Irlanda, el PPSN (número personal atribuido por el servicio público) es un identificador único estatutario que permite acceder a los servicios públicos y, con arreglo a la legislación, se puede utilizar para servicios fiscales y sociales, además de para otros servicios de las autoridades públicas y locales.

3. En Italia tuvo lugar un debate incidental sobre el riesgo de la generalización *de facto* de un identificador sectorial (en este caso, el número de identificación fiscal) una vez integrado en una tarjeta de identidad electrónica: la Autoridad italiana recordó al gobierno que en virtud del apartado 7 del artículo 8 de la Directiva 95/46, relativo a la creación de un identificador único, era aconsejable determinar rigurosamente las condiciones en que tal número se usaría para el tratamiento. El gobierno italiano aseguró a la Autoridad que lo tendría en cuenta, pero la situación aún no se ha fijado definitivamente.

4. La liberalización del uso de un identificador único es efectiva en Irlanda y se espera que llegue a serlo en Bélgica, donde el uso del número del registro nacional (y por defecto, para quienes no son titulares de un número del registro nacional, del identificador de la seguridad social) como identificador único ya es obligatorio en todos los sistemas de información de las autoridades públicas. La Autoridad de protección de datos debe emitir de modo inminente un dictamen sobre la cuestión.

5. El recurso a identificadores sectoriales sólo se mantiene en Alemania, Portugal, el Reino Unido y Francia. Estos identificadores sectoriales sólo se usarán para sus fines originales.

6. Siguiendo la misma lógica de evitar riesgos de interconexión, otras Autoridades pidieron o sugirieron que se recurriera a identificadores sectoriales derivados, en particular en los Países Bajos, donde el anteproyecto del gobierno se modificó de acuerdo con esta petición, y en Austria, donde se

usará el número de identificación único (oculto) combinado con la firma electrónica en una función especial (la llamada «Bürgerkarte» o «tarjeta del ciudadano») para garantizar el acceso en línea a todas las aplicaciones de la administración e incluso a algunas especialmente estructuradas del sector privado.

7. Específico:

- En Finlandia se ha previsto un proyecto de revisión de los sistemas de identificación personal en el contexto de la administración en línea, lo que implica recurrir sólo a un identificador único creado especialmente a efectos de la firma electrónica y la identificación electrónica para el Centro de registro de la población. No está previsto que tal identificador se use para acceder a procedimientos administrativos en línea. El identificador único previo, el número de la seguridad social, no se debe usar para estos fines.
- En Bélgica, el desarrollo de la administración en línea dio lugar a la creación de un identificador único para las empresas: el número de IVA (ampliado a las empresas y organizaciones exentas de tal impuesto) se convirtió en un identificador único para todas las empresas y organizaciones. Este número sustituirá a todos los números específicos restantes y se introducirá como identificador único para las empresas y organizaciones en relación con todos los sistemas de información de las autoridades.

E. INTERCONEXIONES NECESARIAS PARA EL DESARROLLO

Una cuestión a la que la Autoridad británica presta un interés especial es que la administración en línea no funcione como una pantalla de humo que oculte una interconexión generalizada de las bases de datos de información pública y un mayor intercambio de datos personales entre administraciones. Por su parte, con motivo de las consultas organizadas por los autores del informe escrito por encargo del gobierno francés sobre la administración en línea y la protección de los datos personales, la CNIL recordó también su doctrina global, consistente en rechazar una interconexión generalizada de los ficheros. Cuando la CNIL hizo entrega de dicho informe al gobierno, se entabló un debate público sobre los principales puntos abordados en su elaboración. Una de las conclusiones más destacadas del debate, que concuerda perfectamente con la doctrina de la CNIL, fue que la administración en línea no debería suponer un aumento del control ejercido en los individuos, que deriva principalmente de las interconexiones.

Por otra parte, conviene señalar que la conocida teoría del Tribunal Supremo alemán del derecho de los individuos a la autodeterminación en materia de información se refiere precisamente a la cuestión de las interconexiones. Con arreglo a tal derecho, cada individuo ha de poder decidir sobre la comunicación y el uso de sus datos por terceras partes. Aunque su reconocimiento no equivale a una prohibición absoluta de las interconexiones, limita en gran medida sus posibilidades.

A este respecto, en algunos países la motivación básica del establecimiento de interconexiones provocó un deseo de simplificar los procedimientos. Esta innovación afecta a las empresas y a los individuos, en particular, en el caso de estos últimos, cuando

se trata de cambios de dirección. También se mencionó el objetivo de la lucha contra el fraude (en particular en Irlanda y el Reino Unido)

En general, las interconexiones aún se encuentran en proceso de definición. Los campos afectados varían de unos países a otros. A título de ejemplo podemos citar el sector sanitario (España, Finlandia), la gestión de las relaciones entre las administraciones y las empresas (Bélgica), la indexación de los ficheros públicos (Italia) y la aplicación de procedimientos de información en las administraciones públicas (España, referida concretamente a la llamada «ventanilla única», que permite coordinar la actuación de diferentes departamentos administrativos en el curso de procedimientos basados en el intercambio de documentación).

Diversas Autoridades de protección de datos participan en grupos de trabajo centrados en estas cuestiones (por ejemplo, en los Países Bajos y en Finlandia); otras, como las CNIL, tratan estas cuestiones a resultas de su facultad de verificación previa del tratamiento de los datos personales en el sector público.

Estos proyectos plantean las mismas dificultades en todos los países donde se desarrollan:

- A nivel jurídico, las interconexiones se tratan en el marco de una autorización estatutaria (Francia) o bien en el de las disposiciones que exigen un consentimiento personal. En España, por ejemplo, la Autoridad de protección de datos consideró que el proyecto de reglamento de la promoción de la administración en línea cumplía los requisitos de la ley general de protección de datos, pues exigía el consentimiento de los afectados previo a la transferencia electrónica de los datos entre administraciones. Este reglamento fue adoptado por el Real Decreto de 28 de febrero de 2003 relativo a la regulación de los registros, notificaciones, certificados y transmisiones telemáticos. El Decreto establece asimismo los procedimientos que se han de aplicar para utilizar estos sistemas, en particular en el contexto de las comunicaciones con los ciudadanos o para el intercambio de información dentro de los departamentos de la administración pública. En este último caso se exige el consentimiento previo del titular de los datos. También conviene mencionar que una cláusula del Decreto obliga a la administración pública a cumplir la ley de protección de datos.
- En cuanto a los principios de protección, los países insistieron especialmente en los relativos a la calidad de los datos, la legitimidad del tratamiento y la información a las personas afectadas, así como al nivel de seguridad aplicado.

Las cuestiones relativas a la necesidad de interconexiones generales y las condiciones generales de éstas se trataron en el Reino Unido en 2002, con ocasión de la publicación de un informe encargado por el gobierno británico a la «*Performance and Innovation Unit*» (una organización del gobierno británico encargada de la reflexión estratégica que ahora se denomina «Strategy Unit»). El informe, titulado «*Privacy and data sharing: the way forward for public services*», presenta la interconexión como algo aparentemente promovido por el desarrollo de la administración en línea y las expectativas de los ciudadanos en este ámbito, pero insiste en la necesidad igualmente importante de sus expectativas en cuanto a la protección de la vida privada. Por lo tanto, conviene equilibrar las interconexiones (y la supuesta mejora que conllevan en los servicios de la administración) y la protección de los usuarios en relación con el tratamiento de sus datos

personales. La búsqueda de este equilibrio pasaría, obligatoriamente, por los siguientes pasos de análisis:

- ¿Qué ventajas se espera que tenga el uso de los datos y sus interconexiones, teniendo en cuenta los objetivos del gobierno?
- ¿Existe algún enfoque alternativo que permita alcanzar el mismo objetivo?
- ¿Qué riesgos y qué costes conlleva la interconexión?
- ¿Qué garantías se podrían precisar para gestionar estos riesgos (ejemplo: tecnologías destinadas a reforzar el respeto de la vida privada)?
- Al final de este análisis, ¿quedan equilibrados los beneficios y los riesgos inducidos por la interconexión?

Por último, uno de los intereses básicos del informe es recordar que las interconexiones no son indispensables para mejorar los servicios de la administración.

F. FIRMA ELECTRÓNICA E INFRAESTRUCTURA DE CLAVE PÚBLICA

La mayor parte de las delegaciones indican que en sus respectivos países está o estaría permitida la participación de operadores privados, «proveedores de servicios de certificación», en el marco de la aplicación de los mecanismos de firma electrónica en ciertos procedimientos administrativos en línea. En estos casos, el estatuto del proveedor de servicios de certificación está dotado de un marco jurídico (por ejemplo, condición de acuerdo). Estas cuestiones se resolverían con frecuencia en el momento de la trasposición de la Directiva sobre la firma electrónica al derecho nacional.

En los casos restantes es imposible recurrir a proveedores externos privados, pues este papel está reservado al Estado (Alemania, España). En Francia, la cuestión funciona por defecto: hasta ahora, los operadores externos privados sólo intervienen en la certificación de la declaración del IVA en línea. En todos los casos restantes, el Estado actúa como autoridad certificadora.

En general se señala que en la actualidad el recurso a mecanismos de firma electrónica no está muy desarrollado, en algunos casos porque se carece de un marco jurídico adecuado, en otros porque los costes y la complejidad de tales sistemas aún son demasiado elevados. A este respecto, la CNIL subraya que el recurso sistemático a estos procesos no puede constituir un requisito indispensable para la aplicación de procedimientos administrativos en línea: en la situación actual del derecho, la técnica y el mercado de las infraestructuras de clave pública, sería prematuro imponer tal requisito. De hecho, se menciona que ciertos procedimientos administrativos aún no están en línea porque precisarían medios de firma electrónica y cifrado. Así pues, la mayor parte de las administraciones siguen sin contar con un procedimiento público general que lleve asociado un mecanismo de firma electrónica. Una de las excepciones es Dinamarca, donde ya se han desarrollado mecanismos de firma electrónica. Las firmas electrónicas son gratuitas para los ciudadanos y son muchos los portales de Internet que ya están preparados para prestar servicios públicos en línea.

Las prioridades de estas aplicaciones varían de unos países a otros, desde los sectores social y fiscal (Francia), al registro de la población (Finlandia), por ejemplo. En la mayor parte de los casos, estos mecanismos se refieren por igual a los individuos, las empresas y los agentes de la administración. A veces se centran principalmente en las personas (Alemania), otras en los empleados, las organizaciones y los servidores, y no tanto en los individuos (Dinamarca), y en ocasiones se refieren principalmente a los agentes de la

administración (Noruega). Sobre este último punto se presentó una distinción: las firmas electrónicas de los agentes públicos no precisan tanto la identificación de su propietario como establecer si posee las facultades necesarias para tomar una decisión o realizar la acción de que se trate.

Las Autoridades de protección de datos informaron a las autoridades públicas de sus posturas en diversas ocasiones. En algunos casos, el gobierno les consultó con motivo de la adopción de medidas estatutarias y reglamentarias sobre la definición de actividades que precisaban el uso de las firmas electrónicas; en otros decidieron emitir un dictamen a raíz de la presentación de su examen previo de determinadas aplicaciones.

La actitud general de las Autoridades de protección de datos en relación con los mecanismos de firma electrónica es positiva, pues se considera que éstos podrían contribuir a la protección de los datos personales. Sin embargo, algunas de ellas son partidarias de incluir cuestiones de protección de los datos en el desarrollo de tales mecanismos. En particular se recomendó que los proveedores de servicios de certificación facilitaran al usuario información clara acerca de la comunicación de los datos, en cumplimiento de las normas de comunicación de datos personales. La Comisión austriaca de protección de datos considera además que una identificación clara y única de las personas que pidan acceso en línea a datos personales constituye una aportación importante a la protección de los datos en el marco de la administración en línea.

G. TARJETAS DE IDENTIDAD ELECTRÓNICAS

1. Actualmente, la mayoría de las tarjetas de identidad electrónicas de los individuos de los países europeos son sectoriales: principalmente, tarjetas de la seguridad social en algunas de las cuales está previsto registrar, a largo plazo, los datos sanitarios (por ejemplo en Austria). A veces, estas tarjetas sectoriales conviven con las tarjetas de identidad generales, como sucede en particular en Bélgica y Finlandia.

2. Debería haber tantos países con tarjetas de identidad generales como únicamente con tarjetas sectoriales. De hecho, aunque las tarjetas de identidad electrónicas sólo se utilizaban en Bélgica, Italia y Finlandia, se espera que se lleguen a usar en Alemania, Suecia, Francia, España y el Reino Unido (donde serán «tarjetas de autorización», pues no servirán para comprobar la identidad, sino para identificar a las personas que deseen acceder a determinados servicios administrativos en línea y también como tarjetas de la seguridad social). En Portugal también hay un proyecto de tarjeta única: se registrarán en una sola tarjeta varios tipos de datos con varios identificadores asociados, y cada administración sólo podrá acceder a los datos que relacionados con ella. Se está realizando un estudio de la viabilidad técnica de esta tarjeta. La Autoridad portuguesa de protección de datos pidió que se le informase de la evolución de este trabajo, para garantizar el respeto de las disposiciones constitucionales que prohíben la institución de un identificador único en el país.

3. Los proyectos sobre tarjetas de identidad electrónica más avanzados son los de Italia y Finlandia.

    - En Finlandia consiste en una tarjeta de identidad con una fotografía del titular y un chip en el que se registra su certificado de autenticación, el de no

repudio, necesario para las aplicaciones de firma electrónica, y el del Centro de registro de la población, que emite el «número electrónico» del titular: un número único que se utiliza principalmente en transacciones comerciales. La tarjeta no contiene información sobre el identificador universal de la persona (determinado al nacer), su dirección ni su fecha de nacimiento. Está protegida por un identificador personal (PIN) que el usuario puede utilizar también para acceder a redes de información como Internet. Además de ser una tarjeta de identidad (y pasaporte y permiso de conducción), esta tarjeta es útil con fines de identificación y firma electrónicas. Es útil en las transacciones comerciales, pero también en las relaciones con la administración. Así, por ejemplo, la tarjeta se puede usar para validar un cambio de dirección en línea utilizando la aplicación creada a tal fin por el Centro de registro de la población y Correos. En noviembre de 2002, el gobierno propuso que esta tarjeta de identidad se asociara a la de la seguridad social. A petición del Defensor del pueblo en materia de protección de datos, el proyecto tiene en cuenta el derecho de cada persona a decidir si sus datos sanitarios y de la seguridad social se incluyen en ella.

En la actualidad la tarjeta cuesta 29 euros y es válida durante 3 años. Está previsto aumentar su precio a 40 euros y ampliar su periodo de validez a 5 años. No sólo se emite para ciudadanos finlandeses: también puede ser titular de una de ellas cualquier individuo que viva permanentemente en Finlandia y pueda demostrar su identidad.

Estas tarjetas las emiten las comisarías de la policía local contra presentación de la tarjeta de identidad, el pasaporte o el permiso de conducción. El Centro de registro de la población, que la administración finlandesa utiliza como proveedor de servicios de certificación, aporta los certificados necesarios para la identificación electrónica. Además de la tarjeta, es necesario un lector de tarjetas inteligentes, que los usuarios pueden tener en casa. Sin embargo, la identificación también es posible desde un aparato móvil, como un teléfono móvil equipado con un chip especial. Existe un sistema de declaración de pérdida o robo que funciona las 24 horas del día.

La tarjeta de identidad finlandesa no ha obtenido el éxito previsto. De momento sólo la han adoptado 13 000 finlandeses. Algunas de las principales razones de su falta de popularidad son que se ha de pagar tanto por la tarjeta como por el lector que sus usuarios han de tener en casa para realizar con ella transacciones comerciales a través de Internet y que los finlandeses no tienen una idea clara de los beneficios que puede reportarles. Por lo tanto, dado que se trata de una tarjeta opcional, han preferido, en general, mantener los documentos de identidad tradicionales.

- En cambio, está previsto que la tarjeta de identidad electrónica italiana sustituya a la de papel y que sea obligatoria para todos los ciudadanos. De acuerdo con el proyecto que se está desarrollando, además de ser una tarjeta de identidad en sentido estricto, un documento de acreditativo de la nacionalidad y un documento que autorizará el libre movimiento dentro de la Unión Europea, la tarjeta de identidad italiana dará acceso a los servicios públicos nacionales y locales, incluirá una función de firma electrónica y

permitirá a los ciudadanos votar en línea. Y podría ofrecer más funciones, como la posibilidad de pedir hora al médico en línea, por ejemplo.

Esta tarjeta, que también se podrá emitir a nombre de menores, contiene datos sobre la identidad de su titular y también su identificador fiscal. A largo plazo contendrá las huellas dactilares y los datos sanitarios del titular (excepto el ADN), cuyo registro estará autorizado por éste (el requisito de autorización previa individual se estableció a petición de la Autoridad italiana de protección de datos). El gobierno pretende promover el uso de la tarjeta en Internet instalando terminales de uso público en bares, restaurantes y tiendas, y le conferirá una función de identificación en línea. Otro objetivo de esta acción es que los comerciantes puedan actuar como ventanillas administrativas, lo que, a largo plazo, permitirá reducir el coste de estas operaciones para la administración.

Una de las preocupaciones del Ministerio del Interior italiano en relación con la ejecución de este proyecto es la de centralizar de un modo lógico las autorizaciones de emisión de tarjetas, con el fin de garantizar la dependencia de las comunidades locales en la prestación de sus servicios en línea con los ciudadanos y de aplicar una política de seguridad para la propia tarjeta, tanto en el momento de su emisión como durante todo su ciclo de vida. Esta política de seguridad consistía, por ejemplo, en definir un complejo proceso de producción, inicialización, activación y emisión de la tarjeta. Esta última correspondería a las autoridades locales encargadas de recoger los datos personales del titular, incluida la fotografía, y registrarlos en la tarjeta.

La tarjeta incorpora dos tecnologías en un soporte tradicional de plástico: un microprocesador de 16 K y una banda láser. En la tarjeta de plástico se registrarán visiblemente una fotografía, el apellido, el nombre, el sexo y el lugar y la fecha de nacimiento del titular, además de un identificador único. En el reverso constarán la dirección, el número de identificación fiscal y el periodo de validez de la tarjeta y se incorporarán los dos componentes electrónicos (microprocesador y banda láser). En la banda láser, a modo de holograma, figurarán ciertos datos del titular, como las huellas dactilares y la firma.

Ambas tecnologías están justificadas: la banda láser como tarjeta de identidad y el microprocesador como tarjeta de servicios. El microprocesador se utilizará con fines de identificación y autenticación mediante claves simétricas y asimétricas. En la tarjeta se podrán almacenar hasta dieciséis claves distintas.

4. En los países donde existen proyectos de tarjeta de identidad electrónica, los fines de estos suelen coincidir.

En primer lugar se utilizan como certificados de identidad personal.

1. Se prevé casi sistemáticamente que la tarjeta se pueda usar para acceder a procedimientos administrativos en línea (excepto en Alemania, según la información disponible), para identificarse y autenticarse en las

transacciones de comercio electrónico (este punto aún no está definido en el caso de España).

2. Se prevé sistemáticamente la función de firma electrónica para procedimientos administrativos en línea y para aplicaciones de comercio electrónico (si bien este último punto aún no está definido en el caso de España).
3. Por otra parte, estas tarjetas sólo se podrán usar como tarjetas de pago en Alemania, Italia, Austria, Portugal y Suecia.
4. La función de «tarjeta sanitaria» sólo se aplicará en Alemania y Finlandia, y quizá en Portugal, Italia y Austria.
5. La función de «seguridad social» sólo se aplicará en Alemania y Finlandia. En el resto de los países, en principio se contará con una tarjeta sectorial que cubrirá esta función.
6. Por último, estas tarjetas se podrán usar para votar en Alemania, Italia, los Países Bajos y, posiblemente, Portugal y Suecia.

5. Se consultó sobre estas cuestiones a la mayor parte de las Autoridades europeas de protección de datos. Algunas de ellas aprobaron los proyectos de sus autoridades públicas (Finlandia, Suecia), otras están debatiendo los proyectos existentes y otras manifestaron opiniones diferentes a las de las administraciones encargadas del proyecto (Italia, los Países Bajos). En todos los casos se consideraron potencialmente problemáticos varios elementos:

    1. Determinación del carácter de los datos registrados en la tarjeta
    2. Determinación de los procedimientos de tratamiento de los datos
    3. Determinación de las organizaciones autorizadas a acceder a las diferentes categorías de información
    4. Respeto de los derechos individuales
    5. Determinación de las autoridades competentes para decidir sobre el carácter de los datos registrados en la tarjeta de identidad electrónica
    6. Uso potencial de la tarjeta de identidad electrónica con fines comerciales (pago en línea, monedero electrónico, etc.)
    7. Medidas de seguridad aplicadas (Italia subrayó a este respecto que actualmente sólo hay en el mundo una empresa capaz de ofrecer soluciones que respondan a las ambiciones tecnológicas del proyecto)
    8. Almacenamiento centralizado de datos sanitarios y biométricos (huellas dactilares)

H. CONTROL DEL USUARIO SOBRE SUS DATOS PERSONALES

Este punto no se resuelve del mismo modo en los diferentes países de la Unión Europea. En realidad, tal como indica la Autoridad británica, pueden surgir tensiones dentro de la administración entre el deseo de ofrecer al usuario servicios coherentes y prácticos y el de combinar fuentes de información sobre las personas de un modo que podría infringir la legislación sobre la protección de datos. El control de los ciudadanos sobre sus datos personales se encuentra en el centro de esta tensión. Al leer las respuestas de las Autoridades sobre esta cuestión se observan dos tendencias principales:

Una primera tendencia a la que varios países se adhieren expresamente, generalmente apoyados por sus autoridades de protección de datos (Irlanda, Dinamarca, España, Finlandia), consiste en considerar que los ciudadanos deben mantener sus datos bajo

control en todas las fases de los procedimientos administrativos y que se les debe informar de los intercambios de datos correspondientes a las decisiones que se han tomado acerca de ellos. Como consecuencia de esta tendencia, el intercambio de datos entre administraciones por medios telemáticos se puede ver sujeto al consentimiento de los afectados (por ejemplo, en España e Irlanda). En otros países (Reino Unido, Bélgica) la situación es más vacilante. Esta primera tendencia se ve respaldada por la idea de que tal control personal condicionaría la confianza que debe generar la administración en línea, así como su credibilidad. Del mismo modo, cuanto más confíen los ciudadanos en su administración, menos necesitarán ejercer tal control.

Sin embargo, aunque el ciudadano mantenga sus datos bajo control, también se deben aplicar los principios fundamentales de la protección de datos. Así pues, para satisfacer la condición de la recogida leal de datos, la Autoridad irlandesa recomienda no alimentar la base de datos con información facilitada para un fin distinto. En cambio, se recomienda y acepta que se dé a los ciudadanos una oportunidad de consentir su inclusión en el nuevo sistema y que se les informe acerca de los fines y usos de la base de datos central. También se ha de respetar el principio de la calidad de los datos: así pues, no se deberían pedir ni almacenar datos personales excesivos o fuera de propósito, que probablemente no tendrán aplicaciones legítimas y pertinentes en el servicio público. El individuo deberá decidir con libertad qué datos adicionales facilita para disponer de un conjunto de servicios más amplio. Del mismo modo, los individuos han de ser conscientes del abanico de usos potenciales de sus datos en el momento de su recogida, y los agentes administrativos deberían recibir información clara sobre las formas de uso legítimo de los datos a los que tienen acceso. Dicha información ha de ser lo suficientemente precisa como para que las personas puedan entender realmente los riesgos potenciales que conlleva la transmisión de sus datos y las consecuencias que ésta podría inducir. Sin tal información, el consentimiento personal sería ilusorio, pues no habría ninguna razón justificada para rechazar la comunicación de los datos frente al argumento de la simplificación de los procedimientos administrativos.

Es más, diversas Autoridades señalan también como cuestión esencial la necesidad de garantizar un nivel satisfactorio de seguridad de las aplicaciones correspondientes. No se trata de una cuestión teórica, tal como muestra un dictamen reciente de la Autoridad española: una autoridad local subcontrató en dos organizaciones financieras la ejecución de un procedimiento de solicitud de certificados de residencia utilizado por los solicitantes para obtener descuentos en sus billetes de transporte público. Las organizaciones financieras utilizaron las máquinas expendedoras de billetes para emitir los certificados. Sin embargo, durante el procedimiento de solicitud, la máquina expendedora permitía ver no sólo los datos personales propios, sino también los de las otras personas que vivían en la misma residencia, que también estaban registradas en la base de datos. La Autoridad española sancionó a la autoridad local por revelación ilegal de datos.

En cuanto a la segunda tendencia, consiste en considerar que la simplificación administrativa exige necesariamente cierta pérdida de control de los datos personales por parte del usuario. De este modo, no se podrán satisfacer al mismo tiempo las exigencias relativas a una mayor rapidez de la administración en línea y las relativas al suministro «tradicional» de información a los ciudadanos. Tres países (Portugal, Alemania e Italia) consideran que el control de los ciudadanos sobre sus datos no es una consecuencia necesaria del desarrollo de la administración en línea. Un argumento que la Autoridad francesa plantea a este respecto es el riesgo de que en la práctica ese control no sea más

que una ilusión. El usuario podría pensar, erróneamente, que controla sus datos, pero en realidad es evidente que la ley y los reglamentos pueden obligar a los individuos a facilitar datos a la administración. En esta misma línea, la Autoridad portuguesa de protección de datos considera que, aunque la administración en línea pueda soportar parcialmente el derecho de la persona a acceder a sus datos disponibles en línea, el usuario no ejercerá ningún control suplementario sobre sus datos, especialmente en relación con el consentimiento del titular a comunicarlos a terceras partes dentro de la administración.

I. ESTABLECIMIENTO DE UNA AUTORIDAD DE CONTROL DE LA PROTECCIÓN DE LOS DATOS ESPECÍFICA DE LOS PROYECTOS DE ADMINISTRACIÓN EN LÍNEA

Excepto en Bélgica y, en cierta medida, en Finlandia, la cuestión del establecimiento de una autoridad específica de protección de datos para las cuestiones relacionadas con la administración en línea no se ha planteado en absoluto. Las Autoridades preexistentes parecen dedicadas a ser las Autoridades competentes para emitir dictámenes sobre proyectos de administración en línea con repercusiones en la protección de datos.

Se puede pedir a otras autoridades distintas de las Autoridades de protección de datos que consideren las cuestiones relacionadas con este tema en el ámbito de la administración en línea. Por ejemplo, el Defensor del Pueblo del Reino Unido puede investigar quejas formuladas por individuos en relación con las actividades de la administración, incluida la administración en línea. Del mismo modo, en Finlandia, la autoridad reguladora de las telecomunicaciones se encarga de comprobar la conformidad de las autoridades certificadoras y las telecomunicaciones en general, así como las cuestiones relacionadas con el archivo electrónico que son competencia de las autoridades correspondientes. A veces, como en Dinamarca, la Autoridad de protección de datos asume expresamente, por petición de las autoridades públicas, competencias adicionales relativas a la autorización de las soluciones de seguridad en el ámbito de la administración en línea. De todas formas, en ninguno de estos casos se trata de dividir una competencia de comprobación del cumplimiento de la legislación sobre protección de datos entre las Autoridades de protección de datos y otra autoridad.

Por otra parte, en Bélgica se ha estudiado esta posibilidad de dividir las competencias. Está en curso un proyecto que consiste en establecer un Consejo de auditoría diferente de la Autoridad de protección de datos y que estaría formado por comités de autorización del acceso a datos no públicos contenidos en la base de datos de la administración llamada «base de datos empresarial» («banque carrefour des entreprises»). Al principio, dichos comités se iban a crear al margen de la Comisión. Sin embargo, ésta, en su decisión relativa a la creación de la base, pidió que se crearan dentro de ella. Insistía expresamente en que la creación de comités aparte resulta en perjuicio de la unidad de enfoque que debería caracterizar, especialmente a escala institucional, el control del respeto de la vida privada. Así, la Comisión belga recordó al gobierno la necesidad de evaluar las consecuencias de la elección tomada en aquel momento cuando intentase desarrollar una política de administración electrónica, incluidas todas sus aplicaciones futuras en todos los sectores de la administración, tales como, por ejemplo, la tarjeta de identidad electrónica. Dado que cabe esperar que estas cuestiones aumenten, la Comisión consideró importante que fuese una sola institución, en la medida de lo posible, la que estudiase los asuntos relacionados con los derechos y libertades fundamentales de los ciudadanos generados por la creación de esta nueva base de datos. El proyecto actual prevé que los comités se establezcan dentro de la Comisión y estén formados por cierto número

de miembros de ésta acompañados de representantes o expertos de los sectores relacionados.

Hecho en Bruselas, 8.5.2003
Por el Grupo
El Presidente
Stefano RODOTA