IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

Primer congreso sobre Internet, derecho y política: las transformaciones del derecho y la política en la sociedad de la información

Intercambio de datos entre administraciones públicas

Maria del Mar Pérez Velasco

Resumen

Las administraciones públicas recogen gran cantidad de datos personales. El ordenamiento jurídico ha definido el derecho fundamental a la protección de datos de carácter personal. En este artículo se plantea el intercambio de datos entre las administraciones públicas, cuando estos tengan carácter personal, partiendo de la constatación de que no hay una regulación general de los flujos informativos de las administraciones públicas, lo cual plantea dudas respecto a la necesidad de que haya una previsión legal y, en su ausencia, sea suficiente el consentimiento del interesado. Se expone la utilidad del proyecto de eDNI. Finalmente, se proponen mecanismos alternativos a la interconexión generalizada de las bases de datos de las administraciones públicas.

Palabras clave

administración electrónica, información del sector público, intercambio de datos entre administraciones públicas, datos de carácter personal

Tema

Democracia y administración electrónica

Abstract

Public administrations collect large amounts of personal data. By law, the protection of such personal data is defined as a fundamental right. This article looks at the exchange of personal data among public administrations in the absence of regulations governing the flow of data from public administrations. This gives rise to serious doubts regarding the need for there to be legal provision and, in its absence, whether the consent of the interested party should suffice. The article also looks at the usefulness of the "eDNI" (electronic National Identity Card) project. Finally, it makes some proposals for mechanisms that could offer alternatives to the generalised interconnection of public administration databases.

Keywords

e-administration, public sector information, data exchange among public administrations, personal data

Topic

e-Democracy and e-administration

El desarrollo de la e-Administración es una de las prioridades de las políticas de modernización de las administraciones en la mayoría de países de la Unión Europea. La mayoría de los proyectos consisten en el suministro de información y la posibilidad de tramitar en línea, total o parcialmente, algunos procedimientos administrativos. La eficacia gubernamental y administrativa, la reducción de costes y de molestias para los ciudadanos, la simplificación, etc., forman parte del argumentario que justifica y legitima la adopción de los diferentes planes y programas al respecto.

Para llevar a cabo estas funciones que tienen constitucionalmente encomendadas, los poderes públicos recogen,

almacenan y procesan –de forma masiva– los datos personales de millones de ciudadanos, por lo que los flujos de información, también masivos, entre particulares y poderes públicos, y entre los mismos poderes públicos, son una realidad ineludible.

En nuestro estado ya son numerosos los planes y proyectos que las diversas administraciones públicas están desarrollando en el ámbito de la administración electrónica. En el ámbito de la administración del Estado el «Plan Conecta para el desarrollo de la administración electrónica en España 2004-2007» trata de potenciar, una vez más, los servicios de la e-Administración y su relación con los ciudadanos y las empresas a través de las TIC.[1]

En el ámbito de la Administración de la Generalitat de Catalunya, se han anunciado ocho proyectos en los que trabaja el consorcio Administració Oberta de Catalunya (AOC) y que tienen por objetivo mejorar la relación entre los ciudadanos y las administraciones públicas y consolidar un sistema que permita «ahorrar tiempo y dinero».[2]

La gran cantidad de datos personales que se recogen a una escala cada vez más amplia de bases de datos, dan una información fragmentaría pero múltiple de perfiles relativos a las personas. Con esta información se nos admite o excluye de las relaciones jurídicas, administrativas, económicas o sociales, incidiendo sobre el principio de igualdad, el derecho a la salud, el derecho al trabajo, el acceso a la educación, al crédito, a los seguros, a las prestaciones sociales, etc.[3]

Todo tipo de datos son útiles para la identificación y la clasificación, así, el uso de técnicas biométricas comporta que el propio cuerpo o partes de él se configuren como *password*, que se pueden utilizar para cualquier tipo de transacción pero que pueden tener ulteriores usos de control.

En este contexto es preocupante que el poder de las administraciones públicas pueda disponer de cualquier información personal, recogida de cualquier manera y con independencia de la finalidad originaria que motivó la recogida.[4]

El derecho fundamental a la protección de datos de carácter personal es un derecho de configuración reciente con unas especificidades que lo hacen singular. Este derecho ha evolucionado desde una concepción que podía coincidir con el ámbito propio de la intimidad, que se caracteriza por la posibilidad de excluir a otros del ámbito privado, a una perspectiva diferente como es el

1. Se presenta como una iniciativa nueva pero no supone una ruptura total con el «Plan de choque para impulsar la administración electrónica», de 8 de mayo de 2003, elaborado por el gobierno anterior para paliar las críticas que suscitó el anterior Plan Info XXI de enero de 2001. Por otro lado, la Comisión de Estudio creada el 27 de noviembre de 2002 para evaluar el grado de desarrollo y ejecución del plan (conocida por el nombre de Comisión Soto por el nombre de su presidente) elaboró un informe que se hizo público en la página web de la propia comisión y que presentó un panorama bastante negativo.

2. El primer proyecto es el llamado TRAM, creado para facilitar que todos los ayuntamientos dispongan de una solución para gestionar sus trámites por canales telemáticos (36 trámites municipales más solicitados y comunes), prueba piloto en Castellar del Vallès y ahora en fase de extensión. Con el segundo proyecto se pretende evitar pedir a los ciudadanos documentos acreditativos de que ya disponga la Administración. Para ello se desarrolla una plataforma que permita la interconexión de bases de datos de las administraciones y facilite el intercambio de información de manera segura y legal (volantes de padrón, títulos de familia numerosa, certificados de hacienda). El tercer proyecto es facilitar el intercambio entre administraciones, con garantías, de volantes telemáticos de padrón (acreditación del domicilio entre un distrito de Barcelona y Cat salud). El cuarto proyecto es el georreferenciador, una herramienta mediante la cual los ciudadanos pueden conocer la oferta pública de equipamientos y localizar lo que más les interese. El quinto proyecto es la plataforma eaCat que pasa a situarse en el Consorcio AOC. El sexto proyecto consiste en desarrollar soluciones tecnológicas a partir de módulos comunes que responden a necesidades comunes. El séptimo proyecto responde a la necesidad de integrar la información para facilitar la consulta mediante un metabuscador de las webs de la Administración. El último proyecto es la convocatoria de ayudas para adaptar las herramientas al conjunto de las administraciones (incorporación de la firma electrónica).

3. RODOTÁ, Stefano. «Prefacio». En: David LYON (2003). *La società sorvegliata. Tecnologie di controllo della vita quotidiana.* Roma: Feltrinelli Editore.

4. WHITAKER, Reg (1999). *El fin de la privacidad. Cómo la vigilancia total se está convirtiendo en realidad.* Barcelona: Paidós.

reconocimiento de un poder sobre los demás consistente en conocer quién dispone de la información que le concierne. Este cambio de perspectiva, consecuencia de las transformaciones tecnológicas que han determinado la posibilidad de realizar transacciones informativas a gran escala, comporta también que las tutelas tradicionales se vean necesitadas de algún complemento como puede ser la creación de instituciones de garantía específicas.

La Constitución europea reconoce el derecho fundamental a la protección de datos, tanto en lo que se refiere a las instituciones de la Unión (título VI de la primera parte de la Constitución) como en la Carta de los Derechos fundamentales de la Unión (título II de la segunda parte de la Constitución). En ambos casos se distingue este nuevo derecho fundamental del tradicional derecho al respeto a la vida privada y familiar, que es objeto de reconocimiento en otro precepto del mismo cuerpo jurídico.

Es, por lo tanto, un hecho bastante importante el que se reconozca con el máximo rango jurídico posible un derecho fundamental que ya disponía de una regulación propia en la Unión Europea, manifestada en la Directiva 95/46/CE, del Parlamento Europeo y el Consejo de la Unión Europea, de 24 de octubre de 1995, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, pero que ahora se constitucionaliza con su incorporación al texto del Tratado. Pasa de ser una materia armonizada para el cumplimiento de un objetivo del mercado interior, a recibir el reconocimiento de un ámbito propio de la libertad de las personas, es decir, a ser un aspecto recogido junto con los máximos valores democráticos.

De todas maneras, en el ámbito internacional europeo este derecho también dispone de reconocimiento en virtud del Convenio n.º 108 del Consejo de Europa de 28 de enero de 1981.

En nuestro ordenamiento jurídico interno, el derecho a la protección de datos se ha deducido de la redacción del artículo 18.4 de la Constitución de acuerdo con la interpretación realizada por el Tribunal Constitucional (STC 290/2000 y 292/2000 de 30 de noviembre) y se ha desarrollado tanto en la primera Ley orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (conocida por el nombre de LORTAD, derogada) como actualmente por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD ahora vigente). En Cataluña la Ley 5/2002, de 19 de abril, crea la Agencia Catalana de Protección de Datos.

Para plantear de forma adecuada los intercambios de bases de datos entre las administraciones públicas, se hace necesario hacer dos precisiones.

La primera hace referencia al concepto de interconexión. Ni la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal ni la Directiva 95/46/CE definen lo que se tiene que entender por interconexión. Tanto en una como en otra, las interconexiones aparecen asociadas a las cesiones o comunicaciones de datos. De acuerdo con la redacción de la Directiva 95/46/CE, la interconexión se menciona como una específica operación de tratamiento de datos personales (artículo 3.c).

En términos generales, la interconexión podría aludir a la conexión física, lógica y funcional de las bases de datos utilizadas por el mismo o diferentes operadores, de manera tal que los usuarios de estas bases de datos puedan comunicarse entre sí.

La segunda precisión se refiere al concepto de base de datos que se podría entender como sinónimo de fichero y que se define como «conjunto estructurado de datos personales, accesibles, de acuerdo con criterios deter-

minados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica» (artículo 2.c Directiva 95/46/CE). El Convenio Europeo de 1981 también utiliza el concepto de fichero.

Para las administraciones públicas hay unas especificidades, tanto en la recogida como en la cesión de los datos, donde se excepciona el principio del consentimiento para desarrollar sus competencias (artículo 6.2 y 21.1 LOPD).

Estas previsiones, junto con la posibilidad de que mediante habilitación legal se sustituya el consentimiento y el hecho de tener que elaborar una disposición de carácter general para la creación de los ficheros públicos, son las únicas previsiones que la LOPD dedica a los tratamientos de la información por las administraciones públicas.

No hay una regulación general de los flujos informativos de las administraciones públicas. Únicamente algunas normas sectoriales han incorporado recientemente esta perspectiva (regulación del historial clínico, normativa tributaria, etc.).

Por todo ello se hace necesaria una reflexión sobre el alcance de una interconexión generalizada de las bases de datos de información pública y del mayor intercambio de datos personales entre las administraciones públicas.

Esto es importante para no desvirtuar la cadena de control informativo de los datos personales, consistente en que los datos, para poder ser tratados, han de ser adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas. La finalidad de la recogida y tratamiento de los datos personales aparece como uno de los aspectos fundamentales del derecho a la protección de datos, que adopta más relevancia en el ámbito de los tratamientos de las administraciones públicas donde, como se ha comentado, normalmente el consentimiento del ciudadano no está presente. La determinación de qué grupos de finalidades pueden ser compatibles a efectos de una interconexión de datos personales, así como qué garantías de adecuación y pertenencia tienen que reunir los datos interconectados parecen cuestiones que no tendrían que decidirse al margen de un planteamiento general. La interconexión pormenorizada y exenta del debido debate y decisión del legislador podría conculcar la debida transparencia y correlativo deber de información de este desarrollo informativo a gran escala, que es la tendencia actual.

Tiene que establecerse un equilibrio entre las interconexiones de bases de datos públicas (que en ningún caso pueden ser generalizadas, como se ha distinguido por la CNIL) y la protección de los usuarios en relación con el tratamiento de sus datos. Aquí tiene importancia analizar el criterio de compatibilidad de las finalidades para las cuales se tratan los datos personales y que pueden legitimar una interconexión. En este nuevo contexto, de gran capacidad de los poderes públicos para disponer de cualquier información personal, recogida de diversas formas e independientemente de la finalidad originaria que la motivó, es esencial examinar los supuestos que legitiman una interconexión generalizada.

La interconexión entre bases de datos plantea múltiples problemas y una de las líneas de actuación de las administraciones electrónicas tiene como objetivo último la sustitución de los certificados en soporte papel por el intercambio de certificados telemáticos y transmisiones de datos entre los diversos registros y ficheros administrativos. Naturalmente, para hacer posible el intercambio de certificados y las transmisiones de datos será necesario establecer la interconexión entre los diferentes ficheros o bases de datos de las administraciones públicas.

Eso comporta atender varias cuestiones de carácter tecnológico, organizativo y jurídico que de una forma u otra inciden en el modelo de protección de los datos de carác-

ter personal según cuál sea la solución adoptada por la interconexión de bases de datos.

Desde el punto de vista tecnológico, se plantean cuestiones sobre la interoperabilidad de los sistemas.[5] Con respecto a los aspectos organizativos supone un esfuerzo por superar prácticas y rutinas burocráticas (el *back office*) y se ha de tener en cuenta, además, la propia complejidad de la organización de las administraciones públicas, estructuradas en nuestro caso en tres niveles políticos de gobierno claramente diferenciados.

Finalmente, con respecto a los aspectos jurídicos algunas cuestiones aparecen solucionadas en el Real Decreto 209/2003, de 21 de febrero, que regula los registros y notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por parte de los ciudadanos. No obstante, las previsiones de esta disposición plantean algunos interrogantes.

En primer lugar, los protocolos y criterios técnicos para la solicitud y recepción de los certificados telemáticos y las transmisiones de datos se establecen por el órgano titular de la base de datos,[6] pero tanto estos criterios como los elaborados con carácter general por el «Consejo Superior de Informática» son aplicables únicamente en el ámbito de la Administración General del Estado y no establecen unos protocolos de interconexión entre bases de datos claros y precisos.[7]

Por otra parte, el diseño del Real Decreto se basa en el consentimiento del ciudadano para que los organismos de la Administración recojan los certificados que necesitan para tramitar un expediente, directamente de los organismos terceros que los expiden, o bien que sea el propio ciudadano el que obtenga estos certificados de forma telemática. Es decir, en todos los casos de transferencia electrónica de los datos entre administraciones se exige el previo consentimiento de los afectados o, en su caso, una ley que autorice esta transferencia.

Pero lo que pone de relieve la regulación actual es la ausencia de un marco general que regule la interconexión y eso plantea dudas respecto de que, en ausencia de una expresa habilitación legal de las interconexiones de las bases de datos públicas, el consentimiento del interesado sea cobertura adecuada y suficiente de las interconexiones entre cualquier fichero público.

También es importante tener en cuenta que el proyecto «eDNI» pretende dotar a los ciudadanos de identidad digital y firma electrónica, tal como se establece en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. Esta ley establece en su artículo 15.1, que *«El DNI electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos».* La identidad digital se configura así como el conjunto de elementos que proporcionan capacidad jurídica para actuar en un medio

5. Se hace necesario un programa de intercambio de datos como el EDI, *Electronic Data Interchange*, establecer estándares de interoperabilidad entre diferentes sistemas, como por ejemplo el XML, Extensible Markup Language, que es un estándar ratificado por el World Wide Web Consortium (W3C).
6. En el marco de los criterios de seguridad, normalización y conservación, aprobados por el Ministerio de la Presidencia, previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica. La última versión de los «Criterios» es de fecha 24 de junio de 2004 (http://www.csi.map.es).
7. Quizás sea ésta la razón de que el propio Real Decreto prevea en su disposición transitoria única que todos los departamentos ministeriales y organismos públicos tienen que aprobar en el plazo máximo de un año la relación de certificados en soporte papel que pueden ser sustituidos por certificados telemáticos o transmisiones de datos y de que el «Plan de choque» antes mencionado establezca que el MAP, en coordinación con el Ministerio de Ciencia y Tecnología y la entidad empresarial RED.es, tiene que desarrollar los aspectos técnicos relativos a la arquitectura y estándares de intercambio necesarios para posibilitar el uso generalizado de certificados telemáticos y transmisiones de datos entre departamentos y organismos de la Administración estatal.

electrónico, es decir, en las transacciones que se efectúan en línea.

El DNI Electronico se configura así como una poderosa herramienta de identidad en el entorno digital. A las funcionalidades del DNI «analógico» se incorporan las funcionalidades de la biometría digitalizada y de la firma electrónica. Ha de tenerse en cuenta que, a diferencia de la mayoría de países de nuestro entorno en los que no existe un documento identificador único o universal, el DNI es un elemento presente en la mayoría de las relaciones entre los ciudadanos.[8]

En el documento de trabajo de la administración en línea, adoptado por el «Grupo de Trabajo sobre protección de datos del artículo 29,» de 8 de mayo del 2003, se efectúa un análisis comparado del estado de implantación de las tarjetas de identidad electrónicas en el ámbito de la UE y se relacionan los aspectos problemáticos a juicio de las autoridades europeas de protección de datos.

En este documento se mencionan los aspectos relevantes que cabe considerar para la implantación de estos documentos identificativos, que no se han sometido a un debate amplio en nuestro país y que son los siguientes: la determinación del carácter de los datos que se registran en la tarjeta; la determinación de los procedimientos de tratamiento de los datos; la determinación de las organizaciones autorizadas a acceder a las diferentes categorías de información; el respecto a los derechos individuales; la determinación de las autoridades competentes para decidir sobre el carácter de los datos que se registran en la tarjeta de identidad electrónica; el uso potencial de la tarjeta de identidad electrónica con finalidades comerciales (pago en línea, monedero electrónico, etc.); las medidas de seguridad aplicadas y el almacenaje centralizado de datos sanitarios y biométricos (huellas dactilares).[www1]

En cualquier caso la opción por un identificador único y general o por identificadores sectoriales es una opción estratégica por un modelo generalizado de interconexión de ficheros públicos o por un modelo de interconexión sectorializado y limitado.

¿Son indispensables las interconexiones entre bases de datos para mejorar los servicios de la Administración? El análisis de su conveniencia tendría que evaluar los riesgos y los costes, las alternativas que permiten el mismo objetivo y las garantías necesarias para gestionar estos riesgos.

La generalización del consentimiento de la persona concernida parece una garantía totalmente insuficiente en ausencia de una regulación equilibrada y general de las interconexiones de bases de datos.

Por otra parte, Lawrence Lessig ha señalado de manera original la estrecha relación entre el código jurídico y el código informático. De la misma manera que los principios de libertad y cooperación están «inscritos» en los programas de base de Internet, se podría inscribir directamente las reglas de protección de datos en los programas y aplicaciones. Con este enfoque se modificarían las formas de producción de reglas jurídicas y también de programas y, eventualmente, se considera que proporcionaría una garantía más fuerte para los ciudadanos.

Se pueden desarrollar dispositivos tecnológicos alternativos a la interconexión generalizada de bases de datos y así podría analizarse la oferta de grupos de servicios, que requerirían la selección previa de los servicios prioritarios –como el cambio de domicilio– y la puesta en marcha de dispositivos específicos.

Las cuentas administrativas personalizadas podrían ser una solución técnica y organizativa que tendría que analizarse.

8. Su número aparece como dato en el 97% de los registros de entidades y organizaciones y es referente obligado para la expedición de otros documentos o identificadores sectoriales (permiso de conducir, seguridad social, NIF, etc.).
[www1]: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/e-government_es.pdf

Es posible imaginar diferentes escenarios. Uno podría consistir en una especie de caja fuerte virtual que contiene los datos personales de los usuarios y que está ubicada en un portal de la Administración, pero en una zona neutra e inaccesible para ésta. El usuario podría cruzar ciertos datos, facilitar la transferencia de los mismos de una administración a otra, etc. Alternativamente, la caja fuerte virtual podría estar bajo el control directo del usuario, en forma de una tarjeta, o sobre su ordenador.

Una tercera posibilidad sería lo que los franceses denominan «la casa del servicio público virtual». Se trata de un servicio en el cual el usuario efectúa puntualmente mandatos precisos: recoger y facilitar ciertas informaciones, realizar transacciones, ejecutar órdenes. El usuario estaría orientado hacia un interlocutor polivalente.[9]

Cita recomendada

PÉREZ, Maria del Mar (2006). «Intercambio de datos entre administraciones públicas». En: «Primer congreso sobre Internet, derecho y política: las transformaciones del derecho y la política en la sociedad de la información» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 2. UOC. [Fecha de consulta: dd/mm/aa].
<http://www.uoc.edu/idp/2/dt/esp/perez.pdf>
ISSN 1699-8154

Maria del Mar Pérez Velasco
mperezv@gencat.net

Licenciada en Derecho por la Universidad de Barcelona. Abogada de la Generalitat de Catalunya. Profesora asociada del Departamento de Constitucional y Ciencia Política de la Facultad de Derecho de la Universidad de Barcelona. Actualmente es jefe de la Asesoría Jurídica de la Agencia catalana de Protección de Datos.

Publicaciones más relevantes: PÉREZ VELASCO, M. M. (1992). *La conflictivitat competencial. Mitjans de comunicació social.* Barcelona: Institut d'Estudis Autonòmics; CONDE CASTEJÓN, J.; PÉREZ VELASCO, M. M. (2002). «Regulación versus autorregulación en Internet y los nuevos servicios de comunicación». En: VV.AA. *Régimen Jurídico de Internet.* Madrid: La Ley; PÉREZ VELASCO, M. M. «El acceso a los datos de los extranjeros inscritos en el padrón (Comentario a la Ley orgánica 14/2003, de 20 de noviembre)». *Revista Derecho Migratorio y Extranjería*. N.º 5, marzo, Lex Nova, 2004; PÉREZ VELASCO, M. M. «La regulación jurídica de la interconexión de bases de datos personales en el contexto de la Administración Electrónica». *Revista electrónica datospersonales.org*. N.º 12, noviembre 2004. Agencia de Protección de Datos de la Comunidad de Madrid.

9. TRUCHE, Pierre; FAUGERE, Jean-Paul; FLICHY, Patrice (2002). «Rapport au Ministère de la fonction publique et de la réforme de l'État». *Administration électronique et protection des données personnelles: Livre Blanc*. http://www.ladocfrancaise.gouv.fr