



Comunicación

006

“e-PRODAT” – MEJORES PRÁCTICAS EN ADMINISTRACIÓN ELECTRÓNICA Y PROTECCIÓN DE DATOS

Francisco José López Carmona

Subdirector General de Registro de Ficheros y Consultoría

jose.lopezcarmona@madrid.org

Agencia de Protección de Datos de la Comunidad de Madrid

www.apdcm.es

Palabras clave

Administración electrónica, e-Administración, Protección de Datos, Datos Personales, Mejores Prácticas, Proyectos Europeos, e-PRODAT.

Resumen de su Comunicación

El desarrollo de los servicios de Administración Electrónica, conjuntamente con la configuración de redes de servicio público y los cambios que se están produciendo en la actitud de los ciudadanos en relación con los servicios públicos electrónicos, tienen un gran impacto en el derecho a la autodeterminación informativa.

Las mejores prácticas, o dicho de otro modo, las aproximaciones eficientes para mejorar las características de protección de datos personales de la e-Administración, aparecen como un mecanismo viable para alcanzar la excelencia en el respeto a este derecho fundamental, compaginándolo con el despliegue efectivo de servicios de administración electrónica. Proyectos como e-PRODAT buscan identificar y promover la implantación de tales prácticas.

“e-PRODAT” - MEJORES PRÁCTICAS EN ADMINISTRACIÓN ELECTRÓNICA Y PROTECCIÓN DE DATOS

1. Introducción

El espectacular incremento en la utilización de las Tecnologías de la Información y las Comunicaciones (TIC) por parte de los Gobiernos y las Administraciones de todos los niveles en el ámbito de la Unión Europea está mejorando espectacularmente la calidad y la eficiencia de los servicios públicos. Sin embargo, la utilización de estas nuevas herramientas de servicio conlleva algunos riesgos que han de ser controlados, y en particular los relacionados con la privacidad de los ciudadanos. Las TIC proporcionan una inmensa potencia para captar, tratar, almacenar y transmitir datos de carácter personal. Las normativas europea y española han fijado reglas objetivas para el tratamiento de los datos personales, con la finalidad de garantizar a todos y cada uno de los ciudadanos el derecho a decidir y controlar la utilización de sus propios datos de carácter personal, y se han creado diversas instituciones, tanto de ámbito estatal como autonómico (y entre estas últimas, la Agencia de Protección de Datos de la Comunidad de Madrid), cuyo objetivo es el control de la aplicación del derecho a la autodeterminación informativa.

2. Administración electrónica y protección de datos

Habitualmente, tanto los grupos de interés o agentes de política pública que se movilizan en defensa de la privacidad ¹ como las autoridades públicas de control del derecho a la protección de datos de carácter personal ², tienden a destacar los aspectos de posible amenaza derivados de la extensión del uso de estas tecnologías para la provisión de los servicios públicos.

No obstante, debemos destacar inicialmente algunos de los importantísimos aspectos positivos de dicho uso en el contexto público, tales como:

- Las características de las culturas organizativas de los empleados públicos en muchos países europeos, que incluyen valores como la imparcialidad, la orientación hacia el cumplimiento y el respeto a las leyes, etc...
- El hecho de que los Servicios de Administración Electrónica europeos se encuentran entre los más avanzados y extendidos del mundo, con varios proyectos de alto nivel y compromiso político ³, y muchas experiencias de utilización masiva por parte de los ciudadanos.
- Los ciudadanos europeos manifiestan una mayor confianza en el tratamiento de sus datos personales por parte de las administraciones públicas (incluso aquéllas que utilizan datos especialmente protegidos o delicados, tales como los servicios sanitarios públicos) que en el realizado por empresas u organizaciones privadas (en particular televenta, tarjetas de crédito, compañías de seguros), como muestra el Eurobarómetro de marzo de 2004 ⁴.

1 Por ejemplo, la Comisión de Libertades e Informática (CLI) - www.asociacioncli.org -, o el "Electronic Privacy Information Center" (www.epic.org) en Estados Unidos de América.

2 Por ejemplo, en España, la Agencia Española de Protección de Datos (www.agpd.es) y las Agencias de Protección de Datos de la Comunidad de Madrid (www.apdcm.es), Cataluña (www.apdcat.es) y el País Vasco (www.avpd.es).

3 Comisión Europea. "e-Europe 2005: an information society for all". [en línea]. Sitio web de la Comisión Europea., Marzo de 2005. http://europa.eu.int/information_society/eeurope/2005/index_en.htm [Acceso en línea realizado el 11 de abril de 2005].

4 Comisión Europea. "Special Eurobarometer 196 on Data Protection". [en línea]. Sitio web de la Comisión Europea, Diciembre de 2003. http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_highlights.pdf [Acceso en línea realizado el 27 de septiembre de 2004].

- Las tecnologías en las que se apoya la Administración electrónica admiten una personalización masiva, que puede ser dirigida no sólo al tratamiento de los datos personales sino también al cumplimiento individual – para cada titular de datos - de las exigencias legales en relación con la protección de los datos personales.

Entretanto, asistimos tanto en el ámbito europeo como en España a un incremento en la regulación relativa a la privacidad y la protección de datos personales, y en particular en relación con actividades de e-Administración. En la Unión Europea:

- Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales.

- 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.

- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al procesamiento de datos personales y la protección de la privacidad en el sector de las telecomunicaciones.

- Directiva 2002/58/CE, de 12 de julio de 2002 del Parlamento Europeo y Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Otras tendencias que pueden asimismo identificarse son:

- La toma de conciencia de los ciudadanos – y su preocupación creciente – en relación con la privacidad de sus datos personales, lo que en algunos países europeos puede ser visto aún como un cambio cultural en sus etapas iniciales.

- La complejidad e interdependencia de las organizaciones públicas, que pueden ser vistas cada vez más como redes de servicio público, incluyendo al mismo tiempo la participación de diferentes niveles gubernamentales o administrativos (municipio, región, estado, instituciones europeas) e incluso organizaciones no gubernamentales y agentes privados ⁵.

- La creciente sofisticación e interconexión de los sistemas de información, tanto en el interior de cada organismo público como entre distintos participantes en una misma red de servicio público. Este proceso viene apoyado por distintas tecnologías e infraestructuras TIC, siendo la fundamental Internet. Conviene citar expresamente los estándares técnicos orientados al intercambio de información, tales como XML y los denominados “Web Services” entre muchos otros.

⁵ Podemos citar como ejemplo la interconexión en línea entre Agencias Tributarias en distintos países de la Unión Europea para evitar la doble imposición de IVA, o el proceso de adopción internacional de menores que en España tiene como participantes a las Administraciones Estatal y Autonómica, Colegios Profesionales – Psicólogos, Trabajadores Sociales – y Asociaciones sin ánimo de lucro denominadas “ECAI” (Entidades Colaboradoras de Adopción Internacional).

Finalmente, es preciso destacar la reconfiguración de la posición de conocimiento del ciudadano – con

las limitaciones derivadas de la brecha digital, agente de la sociedad de la información – que incrementa su demanda de participación activa en los servicios públicos, incluyendo en particular el muchas veces complejo equilibrio entre transparencia (por ejemplo, en la incorporación a la función pública, obtención de subvenciones públicas, etc...) y protección de datos personales. De hecho, aumenta la demanda de conocer más acerca de otros y de que se conozca menos acerca de nosotros mismos.

Estas demandas se basan en:

- La extensión en la utilización de Internet, que ha crecido en la Unión Europea (25) un 143,5% desde 2.000 hasta 2.005, alcanzando en la actualidad la cifra de 226,9 millones de usuarios (49,3% de la población) ⁶.
- El ejemplo: la progresiva adopción de servicios a través de Internet tanto en el ámbito público como en el privado (¿Por qué no pagar impuestos o solicitar una beca, teniendo en cuenta que ya estoy transfiriendo dinero – banca por Internet -, adquiriendo libros u otros bienes, leyendo periódicos, etc...?).
- Aunque no exclusiva de los servicios públicos, la progresiva mejora de la posición del “cliente” frente al proveedor de bienes o servicios, inicialmente ocasionada por el exceso global en la oferta privada (para clientes con suficiente capacidad adquisitiva) y la extensión masiva de la educación ⁷.

Convergamos en llamar “e-ciudadanos” a aquéllos cuyas características se ajustan al perfil que acabamos de describir, y tratemos de ejemplificar (de un modo muy simplificado) su relación con la privacidad en línea.

- Un porcentaje elevado de internautas afirma no realizar compras en la red por desconfianza sobre la seguridad de su información personal (especialmente tarjetas de crédito).
- Las sucesivas oleadas de virus informáticos que se transmiten a través de correo electrónico u otros mecanismos basados en Internet tienen un impacto directo en el usuario final, haciendo de la seguridad un problema personal.
- Asimismo, los internautas contemplan como fenómenos cada vez más frecuentes la recepción de correo no deseado o “spam” y de modo creciente el “phishing”, o suplantación de la personalidad de un tercero para, por medio de argucias, obtener información personal, generalmente datos de tarjetas de crédito u otros económicos.
- En relación con los puntos anteriores, se produce la difusión masiva de productos y servicios relacionados con la seguridad y confidencialidad de la información – aplicaciones antivirus, cortafuegos personales, sistemas de cifrado de información -.

6 Internet World Stats. “Internet Usage in the European Union”. [En línea], 2006. <http://www.internetworldstats.com/stats4.htm#eu>. [Acceso en línea realizado el 4 de enero de 2006].

7 Cf. El concepto acuñado por Giovanni Sartori de “inteligencia a nivel de calle” (Ground Level Intelligence)

- Se produce una cierta “experiencia positiva de la seguridad” por el internauta, como la utilización de certificados electrónicos de identidad y firma electrónica especialmente en relaciones con la Administración Públicas (más de 700.000 certificados electrónicos emitidos y más de 2.000.000 declaraciones de IRPF presentadas por Internet, etc...), las experiencias satisfactorias de compra o servicio a través de “canales seguros”, etc...

Para completar nuestra visión sobre las tendencias relevantes en e-Administración y Protección de Datos, haremos referencia a los modelos “puros” de intercambio de información de ciudadanos entre redes de servicio público, que podrían describirse del siguiente modo:

- Centrado en la red: a partir de la identificación de un ciudadano (por mecanismos que pueden ir desde un simple código individual hasta tarjetas inteligentes o no, conteniendo o no certificados electrónicos individuales asociados a la capacidad de firma electrónica, o incluso parámetros biométricos como la huella digital, el iris, etc...) y de estándares comunes de intercambio de información (formatos acordados entre las organizaciones asistenciales). Es decir, cuando un ciudadano accede a cualquier servicio público, simplemente acredita (mediante cualquier procedimiento) su identidad, y la organización a la que accede desencadena los procesos electrónicos de intercambio de información que sean necesarios (validación de título o derecho a la prestación, intercambio de información, etc...).

- Centrado en el usuario. Este modelo es el “tradicional” del traslado de certificados u otra documentación administrativa por el propio ciudadano, y puede abordarse también mediante la automatización, por ejemplo, de la carga/descarga de información administrativa y acreditación de identidad/derecho al servicio a partir de tarjetas inteligentes (con chip integrado).

En este punto, debe ya quedar acreditado que todos estos procesos tienen una repercusión substancial sobre la protección de datos personales (y en particular, sobre el derecho a la autodeterminación informativa), y que en el ámbito de los servicios públicos debe alcanzar un equilibrio razonable con otros derechos ciudadanos tales como la asistencia sanitaria, la educación, la justicia, la seguridad, etc... En particular:

- Más datos: necesidad (y por tanto, disponibilidad) ubicua de datos personales para la prestación del servicio público.

- Más intercambio: necesidad creciente (y viabilidad técnica) de transferencia de información personal entre diferentes organizaciones (estatales, regionales, locales o internacionales) tanto públicas como privadas.

- Más complejidad: esquemas de red con la participación de organizaciones diferentes hacen mucho más difícil entender – y por tanto, controlar en la medida de lo posible – el flujo de información personal.

- ¿Quién es quién? Necesidad creciente de identificar los actores intervinientes en una red de servicio público, incluyendo los titulares de los datos, y de confiar en los mecanismos identificativos de otras instituciones.

3. Mejores prácticas

El contexto descrito en los apartados anteriores configura la necesidad de enfatizar las políticas de protección de datos por parte de las administraciones públicas. Se trata no simplemente de cumplir las obligaciones derivadas de la legislación de protección de datos personales (en particular, de la Ley Orgánica

15/1999, de Protección de Datos de Carácter Personal) sino de encontrar vías eficientes y contrastadas para que las administraciones públicas acomoden su actuación a los principios de protección de datos.

Algunas áreas de mejor práctica incluirían:

- Promover la toma de conciencia de los ciudadanos sobre su derecho fundamental a la protección de datos personales.

Las autoridades de protección de datos (tales como la Agencia Española de Protección de Datos o las Agencias autonómicas) no son en general bien conocidas en el ámbito de la Unión Europea. Dos tercios de los ciudadanos de la UE (15) desconocen la existencia de autoridades independientes de control en este ámbito, lo que contrasta con el 60% de ellos que declaran sentirse preocupados por posibles amenazas a su privacidad⁸.

Algunas posibles actuaciones de mejora en este ámbito incluyen la formación de los propios empleados públicos, la incorporación de información general sobre protección de datos personales en sitios web de las AAPP, así como a formularios administrativos en cualquier soporte, la edición de materiales informativos específicos (folletos, etc...), entre otras.

- Promover la información a los ciudadanos sobre el tratamiento de sus propios datos cuando éstos acceden en línea a un servicio público concreto.

En contraposición con actuaciones para promover una mayor concienciación, con carácter general, sobre el derecho fundamental a la protección de datos personales, estas actuaciones buscan la información individual a un ciudadano en particular sobre el tratamiento que, de sus datos personales, se hace cuando accede a un servicio público electrónico en particular:

Las buenas prácticas en este terreno se orientan a incluir información sobre el tratamiento concreto en formularios electrónicos, a hacer esta información sencilla de entender, a informar en línea sobre el acceso interactivo a información personal (por ejemplo, con mensajes en pantalla del tipo "En este momento estamos conectando con la Agencia Tributaria para obtener su información fiscal" o "Enviando su información al Ministerio de ..."), a solicitar permiso expreso e informado para el tratamiento o acceso a datos de terceros cuando proceda, a informar sobre decisiones basadas en el tratamiento de datos personales (por ejemplo "Su solicitud de beca ha sido denegada por no haber podido encontrar información sobre su titulación académica en el fichero del Ministerio de Educación"), a coordinar iniciativas para la declaración de ficheros de datos personales por Administraciones Públicas, etc...

⁸ Comisión Europea. "Special Eurobarometer 196 on Data Protection". [en línea]. Sitio web de la Comisión Europea, Diciembre de 2003. http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_highlights.pdf [Acceso en línea realizado el 27 de septiembre de 2004].

- Menos es más: economía de información personal

Otro grupo de mejores prácticas son las relativas a la utilización efectiva de la mínima cantidad de información personal necesaria para la prestación de servicios públicos. Por ejemplo, se trata de limitar la exposición pública de datos – personalizando el acceso mediante medios electrónicos con autenticación del titular -, revisar sistemáticamente impresos electrónicos para asegurar que no contienen más información que la imprescindible, preparar interfaces orientadas a tareas/perfil de usuario (y no multiusuario: el sistema informático de un hospital no debe mostrar al personal administrativo el diagnóstico, sino sólo la información relevante para sus funciones), desarrollar sistemas de identificación digital que prevengan el cruce incontrolado de datos, etc...

- Facilitar el ejercicio de los derechos de las personas sobre sus datos

En este ámbito se incluye la capacitación de los funcionarios para identificar y atender las solicitudes de los ciudadanos para ejercer sus derechos de acceso, rectificación y cancelación de datos, el establecimiento de procedimientos internos adecuados, la posibilidad de ejercer estos derechos vía Internet, etc...

- Inclusión digital

Aunque la mayoría de las preocupaciones relacionadas con el respeto al derecho fundamental a la protección de datos personales se refieren a la información que las Administraciones Públicas NO DEBEN requerir o tratar, es importante destacar la importancia de la inclusión y la actualización de la información personal para asegurar el pleno acceso de los ciudadanos a los servicios públicos.

Algunas buenas prácticas en este terreno incluyen el establecimiento de procedimientos periódicos de actualización de datos personales, la verificación de tales datos con los propios ciudadanos (por ejemplo enviándoles un mensaje por correo electrónico, o un escrito), etc...

Existen diversas iniciativas de identificación y difusión de mejores prácticas en protección de datos, incluyendo la elaboración a modo de recomendación por autoridades de control en materia de protección de datos o iniciativas conjuntas como "The Virtual Privacy Office" (<http://www.datenschutz.de/privo/>), que agrupa a distintas autoridades de protección de datos de Länder alemanes y otros países.

Debe citarse en particular el Premio Europeo a las Mejores Prácticas de las Administraciones Públicas en materia de Protección de Datos, otorgado por la Agencia de Protección de Datos de la Comunidad de Madrid (www.apdcm.es). Por ejemplo, en su edición de 2005, el proyecto premiado ha sido el titulado "Gestión de la identidad de forma compatible con la protección de datos en el Gobierno electrónico" presentado conjuntamente por el Gobierno y la Comisión de Protección de datos de Austria ⁹, obteniendo menciones especiales la Universidad Rey Juan Carlos y la Oficina de Vivienda de la Comunidad de Madrid.

⁹ Agencia de Protección de Datos de la Comunidad de Madrid. "El Gobierno y la Comisión de Protección de Datos de Austria, Premio Europeo a las mejores prácticas en protección de datos de la APDCM". [en línea], 2006. http://www.madrid.org/cs/Satellite?idPage=1109266885668&c=CM_Actualidad_FA&literal=Actualidad&pagename=APDCM%2FCM_Actualidad_FA%2FfichaActualidad_APDCM&language=es&cid=1132041518273 [Acceso interactivo el 12 de enero de 2006].

4. e-PRODAT

e-PRODAT ¹⁰ (www.eprodat.org) es un proyecto europeo dirigido a la promoción del intercambio de conocimiento y experiencias entre Agencias y otras instituciones públicas, en relación con la protección de los datos personales utilizados por Gobiernos y Administraciones Públicas para la prestación de servicios públicos, y en particular aquéllos relacionados con Administración Electrónica o basados en Internet, contribuyendo en especial a identificar y difundir mejores prácticas en este área.

Sus objetivos fundamentales son los siguientes:

- El intercambio estructurado de conocimiento y experiencias relativas a la protección de los datos personales en instituciones públicas pertenecientes a distintos países europeos, comenzando con un análisis a escala europea y estudios de caso de las regiones y ciudades participantes.
- Crear un “Observatorio Europeo de Protección de Datos y Administración Electrónica” para el análisis permanente del cumplimiento de las leyes y principios europeos de protección de datos, y la concienciación sobre protección de datos entre los ciudadanos europeos.
- Identificar mejores prácticas sobre protección de datos y Administración Electrónica vigentes en servicios públicos europeos, y generar recomendaciones para mejorar los estándares de protección de datos en las Administraciones Públicas.

Los socios participantes son la Agencia de Protección de Datos de la Comunidad de Madrid (España, líder del proyecto), el Inspectorado de Protección de Datos (Estonia), el Ayuntamiento de Bolonia (Italia), la Asociación de Autoridades Locales de la Prefectura de Kavalas (Grecia), el Ayuntamiento de Santa Cruz de Tenerife (España), la Región de Abruzzo (Italia), la Región de Grecia Occidental (Grecia), la Universidad de Patras (Grecia) y la Universidad Rey Juan Carlos (España).

La duración de e-PRODAT será de 24 meses (Febrero 2005 a Enero 2007). Su presupuesto total alcanza los 820.000 euros, de los que 515.000 serán fondos estructurales (FEDER) proporcionados por la Unión Europea a través del programa de cooperación INTERREG IIIC (www.interreg3c.net).

¹⁰ Agencia de Protección de Datos de la Comunidad de Madrid. “e-PRODAT (English)”. [en línea], 2005. www.eprodat.org [Acceso interactivo el 18 de mayo de 2005].