CEPS Background Briefing

En preparación para las elecciones al Parlamento Europeo

Informando el debate sobre protección de datos

Elspeth Guild, Sergio Carrera y Alejandro Eggenschwiler

Muchas áreas de las políticas de la UE serán objeto de debate crítico y discusión en las campañas previas a las elecciones al Parlamento Europeo del 4-7 de junio de 2009. A pesar de la amplitud de los temas y la importancia relativa vinculada a ellos variarán sustancialmente de un estado miembro a otro, los temas que se han convertido en políticas y derecho de la UE en los últimos diez años en el Área de Libertad, Seguridad y Justicia merecen un análisis documentado y coherente. Estas políticas tienen una incidencia en el núcleo del derecho de cada individuo a la libertad y seguridad en una Europa ampliada.

Este Background Briefing trata específicamente sobre las políticas Europeas sobre protección de datos. Después de esquematizar el actual estado de la cuestión y los siguientes pasos legislativos a tomar en el futuro próximo, presenta el escenario con los déficits y temas principales que rodean esta política Europea. La sección conclusiva destaca los retos más importantes en este campo y propone recomendaciones para los próximos cinco años.

Este Policy Briefing es uno de un conjunto de cuatro breves que abordan, respectivamente, la inmigración, el asilo, las fronteras y la protección de datos. Los cuatro artículos son parte del proyecto: "Informing the Immigration Debate: Preparing for the European Parliament Elections 4-7 June", con el apoyo de Barrow Cadbury Trust, una fundación caritativa independiente que financia y promueve iniciativas de justicia social (para más información, véase http://www.bctrust.org.uk). El objetivo de todos estos Policy Briefings es informar el debate sobre estos temas controvertidos y a menudo técnicos para los partidos políticos en su preparación para las elecciones al PE y dirigirse al electorado.

Elspeth Guild es catedrática en el Centre for Migration Law de la Radboud University de Nimega (Países Bajos) e investigadora senior en la Sección de Justicia y Asuntos de Interior en CEPS. Sergio Carrera es investigador y responsable de la Sección de Justicia y Asuntos de Interior en CEPS. Alejandro Eggenschwiler es asistente de investigación en CEPS.

Salvo que se indique lo contrario, las opiniones expresadas son atribuibles sólo a los autores a título personal y no a cualquiera de las instituciones a las que están asociados. Los autores quieren agradecer a Raül Hernández i Sagrera (Investigador en el Observatori de Política Exterior Europea de la Universitat Autònoma de Barcelona) por llevar a cabo la traducción del texto al español.

1. Estado de la cuestión y siguientes pasos

El derecho a la protección de datos en la UE se basa en un conjunto de actos jurídicos que pertenecen tanto al derecho internacional como al derecho Europeo (para una lista completa de las medidas adoptadas en el ámbito de protección de datos, véase el Anexo). La "directiva sobre protección de datos" de 1995[1] es la pieza clave de la legislación Europea en este ámbito dado que establece los principios generales que los estados miembros deben seguir con el fin de garantizar el derecho a la privacidad del individuo, al mismo tiempo que asegura que no se impongan restricciones a la circulación de datos entre ellos. La directiva regula operaciones de recogida, almacenamiento, revelación y diseminación de datos personales, tanto por medios automáticos (bases de datos electrónicas) y medios no automáticos (sistemas de archivos tradicionales), en relación a los cuales se concede al 'sujeto de los datos' un conjunto de derechos, incluyendo el derecho a ser informado si los datos relacionados con dicha persona están siendo procesados; el derecho a obtener la rectificación, el borrado o bloqueo de datos que no han sido procesados legalmente; y el derecho a recurso judicial en el caso de que haya una vulneración de los derechos conferidos durante el procesamiento de los datos personales. Con el fin de hacer frente a las amenazas al derecho del individuo a la protección de datos derivadas del desarrollo tecnológico, la directiva ha sido complementada por dos instrumentos más que tratan la privacidad en los sectores de las telecomunicaciones[2] y las comunicaciones electrónicas.[3]l principal objetivo de éstas Directivas es garantizar la confidencialidad de las comunicaciones prohibiendo cualquier escucha, grabación, almacenamiento u otros tipos de intercepción o vigilancia no autorizados.

La privacidad y la protección de datos también están contenidas en la Convención Europea para la Protección de los Derechos Humanos y las Libertades Fundamentales (art. 8) y la Convención 108,[4] ambas adoptadas bajo los auspicios del Consejo de Europa, así como en la Carta de Derechos Fundamentales de la Unión Europea (arts. 7 y 8).[5] Además, cabe subrayar que en el contexto de la UE hay un Supervisor Europeo de Protección de Datos (EDPS)[6] y un grupo de trabajo sobre la protección de individuos respecto al tratamiento de datos personales,[7] los cuales se han creado como organismos independientes con poderes supervisores y consultores. Concretamente, el EDPS asegura que las instituciones y organismos de la UE traten los datos personales de los individuos legalmente; aconseja los órganos con poder decisorio de la UE sobre nuevas propuestas legislativas y sobre cualquier tema que tenga un impacto en la protección de datos. También coopera con las autoridades nacionales de protección de datos para promover un nivel homogéneo de protección de datos en la UE (véase el Anexo 1 para una selección de opiniones del EDPS).[8] El grupo de trabajo brinda la plataforma para esta cooperación reuniendo a los representantes de las autoridades nacionales de protección de datos, el EDPS y la Comisión Europea.[9]

A pesar de todo, el marco legal expuesto hasta ahora se aplica sólo a las políticas del Área de Libertad, Seguridad y Justicia (ALSJ) que se agrupan en el Título IV del TCE (visados, asilo e inmigración) – el Primer Pilar. Las cuestiones de protección de datos pueden también tener eco en otras políticas del ALSJ del Título VI del TUE (cooperación policial y judicial en materia penal) – el Tercer Pilar – que fueron reguladas en la reciente Decisión marco 2008/977/JAI sobre la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.[10] Esta división es fruto de la doble estructura de pilares en el ALSJ, y tiene como riesgo disminuir el nivel y la coherencia en la protección de datos en la UE, especialmente en virtud del hecho de que la Decisión marco no se aplica al tratamiento de un amplio conjunto de datos personales, incluyendo: datos internos; datos intercambiados entre estados miembros y terceros países; y datos procesados por Europol, Eurojust, el Sistema de Información de Schengen (SIS) y el Sistema de Información de Aduana (CIS).

2. Déficits y Temas Principales sobre las Políticas Europeas sobre Protección de Datos

El ALSJ está siendo conducida por la creencia firme de que la tecnología es la solución a cada amenaza a la seguridad, sin considerar el hecho de que podría dar lugar a más inseguridad en términos de derechos fundamentales y libertades del individuo, especialmente las que hacen referencia al derecho de protección de los datos personales tal y como establece el artículo 8 de la Carta de Derechos Fundamentales. La UE ha creado hasta ahora un buen número de bases de datos y sistemas de intercambio de información, que incluyen, por ejemplo:[11]

- EURODAC, una base de datos que contiene las huellas dactilares de todos los solicitantes de asilo y todas las personas retenidas cruzando irregularmente la frontera exterior de la UE. A finales de 2007, EURODAC registró 1,086,246 huellas dactilares, y su coste ascendió a 8.1 millones de euros durante los cinco primeros años de su actividad. Después de una caída entre 2005 y 2006, en 2007 las estadísticas de EURODAC muestran un aumento (del 19% en 197,284 en 2007 comparado con los 165,958 en 2006) en el nombre de transacciones de datos de solicitantes de asilo. Además, el número de personas detenidas en relación con un cruce irregular de la frontera exterior de la UE vio una disminución del 8% en 2007 (38.173).[12]

1 Directiva 95/46/EC relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la protección de estos datos (OJ 1995 L 281/31)

2 Directiva 97/66/EC relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (OJ 1998 L/24/1).

3 Directiva 2002/58/EC relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (OJ 2002 L 201/37), enmendada por la Directiva 2006/24/EC (OJ 2006 L 105/54).

4 Convención para la protección de individuos en cuanto al tratamiento automático de datos personales.

5 OJ 2000 C 364/1

6 El art. 41 del Reglamento 45/2000/CE relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (OJ 2001 L 8/1).

7 Art. 29 de la Directiva 95/46/CE.

8 http://www.edps.europa.eu/EDPSWEB

9 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

10 Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (OJ 2008 L 350/60).

11 Para una visión general de los bases de datos y sistemas de información de la UE, véase F. Gyer (2008), "Tacking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Szecurity and Justice", CHALLENGE Research Paper N° 9, mayo de 2008, Centre for European Policy Studies.

12 Comisión Europea, Comunicación, Informe anual de las actividades de la Unidad Central de EURODAC en 2007, COM (2009), 13, 26.1.2009, Bruselas.

- El Sistema de Información de Schengen (SIS), una base de datos utilizada por las autoridades de los estados miembros de Schengen para intercambiar datos sobre algunas categorías de personas y bienes, que se ha utilizado fundamentalmente como base de datos de nacionales de terceros países para retirar su entrada en la UE, y que se ha desarrollado en el SIS + para incluir los estados miembros de 2004. Los últimos serán transformados (con nuevas capacidades e información) en la segunda generación del SIS (SIS II).[13]
- El Sistema de Información de Visados (VIS), el cual contendrá la información de todas las personas que soliciten visados de curta duración en la UE.
- Adicionalmente, la creación de tres nuevas bases de datos de gran alcance en la UE ha sido propuesta por la Comisión Europea, como parte de su paquete de fronteras de 2008, que son las siguientes: categorías de nacionales de terceros países en las fronteras exteriores de la UE; un Sistema Automático de Control de Fronteras para la verificación de la identidad del viajero (para ciudadanos de dentro y fuera de la UE) basado en tecnología biométrica; y un Sistema de Autorización de Viajes Electrónicos que obligue a los viajeros de fuera de la UE a facilitar los datos personales para el control previo a la salida en Internet (véase el Briefing paper sobre fronteras).

El contenido y el modo en los que estas herramientas se utilizan es motivo de preocupación.

En primer lugar, el resultado de la búsqueda en base de datos de las autoridades puede ser problemático en función de cómo se lleva a cabo. Por ejemplo, no toda la población está en todas las bases de datos y, en consecuencia, sólo se tiende a sospechar sobre los que tienen un perfil que concuerda con el que las autoridades están buscando y que concuerda con el que ya tienen en la base de datos. Diferentes tipos de búsquedas dan lugar a diferentes problemas. Se suelen llevar a cabo una o más búsquedas por individuo. Las búsquedas basadas en perfiles, cuando no se sabe lo que se está buscando, suscita mucha más preocupación. El uso de datos reunidos comercialmente con el fin de cumplir la ley también puede traer problemas. Con tal de evitar el riesgo de agravio innecesario al individuo, los datos personales recopilados con fines de cumplimiento de la ley necesitan ser precisos. Los problemas surgen cuando los datos originales se integran con informaciones más recientes, generalmente cuando el individuo capta la atención de las autoridades, lo que lleva a una imagen completamente arbitraria de la persona. Además, los datos personales reunidos por razones de seguridad necesitan ser adecuados y proporcionales al propósito por el que se han recopilado, dado que una compilación de datos indiscriminada no sólo no garantiza una mejor seguridad, sino que también vulnera el derecho del individuo a la privacidad.

En segundo lugar, asegurar que el acceso a datos sensibles está limitado estrictamente a aquellos que tienen derecho a ello es una cuestión de suma importancia. El acceso a las bases de datos de la UE depende del instrumento que se ha creado en la base de datos. Por ejemplo, el acceso a EURODAC está limitado a los funcionarios que comprueban si un solicitante de asilo ya ha lo ha solicitado en otro país (o llegó irregularmente), pero ha habido cambios para ampliarlo a otras autoridades, incluidas las policiales. La cualidad de las agencias de seguridad encargas de recopilar, tratar e intercambiar datos, así como las implicaciones de dar a las autoridades de terceros países acceso a las bases de datos de la UE, necesita por ello ser evaluada con muchísimo cuidado para garantizar que los datos personales del individuo son tratados legalmente y de forma adecuada.

Por último, los individuos deben protegerse adecuadamente contra las consecuencias de las inexactitudes o un intercambio laxo de datos, y deben estar informados adecuadamente sobre los derechos que gozan en este sentido. Un informe del Eurobarómetro en 2008[14] mostró que, mientras que la mayoría de los ciudadanos de la UE (64%) están preocupados por cuestiones de protección de datos, sólo un cuarto de ellos (27%) es consciente de los derechos de los que gozan en caso de un mal uso de sus datos personales, y que ni tan sólo un tercio (29%) sabe que los datos sensibles como la información sobre orígenes racionales o étnicos recibe una protección legal especial. Los derechos del sujeto de los datos, junto a información efectiva sobre ellos, necesitan por ello que sean abordados como otra tema clave in el debate de protección de datos con el fin de eliminar las incoherencias que actualmente merman el marco legal de la UE en materia de protección de datos, especialmente en cuanto a su aplicación al ALSJ. El grado de protección concedida a nivel de la UE, efectivamente, está lejos de ser homogéneo, dado que los derechos del sujeto de los datos dependen mucho de la base de datos en consideración, y el espacio entre los estándares conseguidos en los ámbitos de las políticas que pertenecen respectivamente al Primer y al Tercer Pilar es todavía significativo.

3. Retos futuros y recomendaciones

Los siguientes retos de gran alcance pueden identificarse en relación con la protección de datos en el ALSJ de la UE:

En primer lugar, las normas de privacidad deben extenderse a los programas que tratan bases de datos y sistemas de información de la UE. Estos programas deben prever borrar automáticamente los datos al final del periodo permitido; impedir cualquier acceso no autorizado al sistema o cualquier duplicación de imágenes en las pantallas de los ordenadores; y prohibir demasiadas búsquedas de bases de datos que tengan lugar excepto cuando se trate de un orden judicial.

En segundo lugar, las bases de datos no deberían crearse sin un estudio de evaluación de impacto previo llevado a cabo por organizaciones objetivas e independientes. Cualquier estrategia de la UE sobre intercambio de datos necesita empezar con la evaluación e inventario de las políticas actuales, herramientas y estructuras institucionales involucradas en el intercambio de datos en el ámbito de la seguridad a nivel de la UE. Cualquier base de datos nueva sólo debería crearse, y utilizarse posteriormente, con fines legales y específicos – evitando definiciones vagas y abiertas y compilaciones de datos sin un objetivo claro.

En tercer lugar, los sistemas de compilación de datos no deberían sacar a la luz datos sensibles sobre el origen étnico, la religión u otros aspectos prohibidos en el derecho no discriminatorio de la UE. Criterios secretos indicando distinciones étnicas o religiosas, como el lugar de nacimiento de los padres del individuo, o su anterior nacionalidad, deberían prohibirse.

13 Informe de progreso de la Comisión sobre el Desarrollo de la Segunda Generación del Sistema de Información Schengen – julio de 2008 – deciembre de 2008, COM (2009) 133, 24.3.2009, Bruselas.

14 La Organización Gallup (2008), "Data Protection in the European Union. Citizen's perceptions", Eurobarómetro, página 5.

ANEXO

Medidas adoptadas

1. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ 1995 L 281/31).
2. Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24/1).
3. Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8/1).
4. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201/37).
5. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105/54).
6. Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350/60).

Opiniones adoptadas por el Supervisor Europeo de Protección de Datos en 2009
Supervisión

1. Opinion of 29 April 2009 on a notification for prior checking on Voice Logging at the Joint Research Centre Institute for Energy (JRC-IE) in Petten (Case 2008-014).
2. Avis du 1er avril 2009 sur la notification d'un contrôle préable à propos du dossier "Exercice annuel de retraite anticipée sans réduction des droits à pension" (Dossier 2008-719).
3. Avis du 30 mars 2009 sur la notification d'un contrôle préalable concernant le dossier "stagiaires structurels" (Dossier 2008-760).
4. Avis du 25 mars 2009 sur la notification d'un contrôle préalable à propos du dossier "traitement des demandes de levée de l'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission" (Dossier 2008-645).
5. Avis du 23 mars 2009 sur la notification de contrôle préalable à propos de la gestion des informations transmises par l'OLAF dans le cadre du Memorandum of Understanding (Dossier 2009-011).
6. Avis du 10 mars 2009 sur la notification d'un contrôle préalable à propos du dossier Procédure de fin de stage (Dossier 2008-720).
7. Opinion of 26 February 2009 on a notification for prior checking regarding ETF - Flexitime procedure (Case 2008-697).
8. Avis du 23 février 2009 sur la notification d'un contrôle préalable à propos du dossier "Groupe de réintégration et de réorientation professionnelle" (Dossier 2008-746).
9. Opinion of 20 February 2009 on a notification for prior checking regarding the engagement and use of temporary agents (Case 2008-315).
10. Opinion of 18 February 2009 on a notification for prior checking on the procedure for early retirement without reduction of pension rights (Case 2008-748).
11. Opinion of 9 February 2009 on a notification for prior checking regarding "ART: Audit Reconciliation Tool" (Case 2008-239).
12. Avis du 26 janvier 2009 sur la notification de contrôlé préalable à propos du dossier "Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme" (Dossier 2008-440).
13. Opinion of 21 January 2009 on a notification for prior checking on the assessment of staff's capacity to work in a third language before first promotion (Case 2008-690).
14. Opinion of 21 January 2009 on a notification for prior checking concerning the report on probation period (Case 2008-604)
15. Opinion of 16 January 2009 on a notification for prior checking on the management of Central and Local Training SYSLOG Formation (Case 2008-481).
16. Avis du 16 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "Procédure relative aux commissions d'invalidité" (Dossier 2008-626).
17. Avis du 15 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "gestion et facturation de la crèche du Secrétariat Général du Conseil" (Dossier 2007-441).
18. Avis du 9 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "Exercice annuel de retraite anticipée sans réductions des droits à pension" (Dossier 2008-552).

Opiniones adoptadas por el Grupo de trabajo sobre la protección de individuos respecto al tratamiento de datos personales en 2008

1. Opinion 3/2008 of the Article 29 Working Party on the World Anti-Doping Code draft International Standard for the Protection of Privacy.
2. Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, Adopted on 15 February 2007 and revised and updated on 24 June 20083.
3. Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive).
4. Opinion 1/2008 on data protection issues related to search engines.