CEPS Background Briefing
En préparation des Elections du Parlement Européen

Éclairer le débat sur la protection des données

Elspeth Guild, Sergio Carrera et Alejandro Eggenschwiler

Bon nombre de domaines d'action de l'UE feront l'objet de débats et de discussions critiques au cours de la campagne des élections au Parlement européen, du 4 au 7 juin 2009. Même si les grands thèmes et l'importance qui leur est accordée varient considérablement d'un Etat membre à un autre, les questions soulevées par l'évolution des politiques et de la législation de l'UE au cours des dix dernières années dans l'Espace de liberté, de sécurité et de justice (ELSJ) méritent une analyse informée et cohérente. Ces politiques portent sur des éléments essentiels du droit à la liberté et à la sécurité qui revient à chaque citoyen dans une Europe élargie.

La présente note de synthèse est consacrée à la protection des données. Après avoir exposé l'état actuel de la politique européenne de protection des données et les mesures qui devraient être adoptées dans un avenir proche, elle met en évidence les principaux problèmes que pose cette politique. La conclusion recense les défis majeurs à relever et contient des recommandations cruciales pour les cinq prochaines années.

La présente note de synthèse fait partie d'une série de quatre, traitant respectivement de l'immigration, de l'asile, des frontières et de la protection des données. Ces notes ont été réalisées dans le cadre du projet « Informing the Immigration Debate : Preparing for the European Parliament Elections 4-7 June » financé par le Barrow Cadbury Trust, une fondation caritative indépendante qui apporte un appui financier à des initiatives en faveur de la justice sociale (pour plus d'informations voir http://www.bctrust.org.uk). Elles visent à éclairer le débat sur des thèmes techniques qui suscitent souvent des polémiques, tandis que les partis politiques se préparent aux élections européennes et informent les électeurs.

Elspeth Guild est professeur de droit européen des migrations à l'université Radboud de Nimègue (Pays-Bas) et chercheuse au Centre for European Policy Studies (CEPS) de Bruxelles. Sergio Carrera est chercheur et chef de la section Justice et Affaires Intérieures au CEPS. Alejandro Eggenschwiler est assistant de recherche.

Les auteurs souhaiteraient remercier Anaïs Faure-Atger (CEPS) pour la traduction vers le Français.

CENTRE FOR EUROPEAN POLICY STUDIES
Thinking ahead for Europe

BARROW CADBURY

1. Etat des lieux et perspectives

Le droit à la protection des données dans l'UE est basé sur un ensemble de textes juridiques appartenant à la fois au droit international et au droit communautaire (pour une liste complète des mesures adoptées dans le domaine de la protection des données, voir l'annexe). La directive de 1995 sur la protection des données[1] est l'élément principal de la législation en la matière : elle établit les principes généraux que les Etats membres doivent observer pour garantir le droit des individus au respect de leur vie privée, tout en assurant qu'aucune restriction n'est imposée à la circulation des données. La directive s'applique à des opérations telles que la collecte, le stockage, la divulgation et la diffusion des données personnelles, tant par des moyens automatiques (bases de données électroniques) que non automatiques (systèmes traditionnels de classement) ; la directive octroie à la personne concernée par ces opérations une série de droits, notamment le droit d'être informé si des données qui la concernent sont traitées, le droit d'obtenir la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la directive, et le droit à un recours juridictionnel en cas de violation, pendant le traitement des données personnelles, des droits qui lui sont conférés. Pour faire face aux menaces pour la protection des données que représentent les progrès technologiques, la directive a été complétée par deux autres instruments traitant de la protection des données personnelles dans les secteurs des télécommunications[2] et des communications électroniques.[3] Leur but principal est de garantir la confidentialité des communications en interdisant les écoutes, les enregistrements, le stockage et les autres types d'interception ou de surveillance.

Les règles de protection de la vie privée et des données personnelles sont également contenues dans la Convention européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales (art. 8) et dans la Convention 108,[4] toutes deux adoptées sous les auspices du Conseil de l'Europe, et dans la Charte des droits fondamentaux de l'Union européenne (articles 7 et 8).[5] Il convient en outre de souligner l'existence, dans le contexte de l'UE, d'un Contrôleur européen de la protection des données (CEPD)[6] et d'un Groupe de protection des personnes à l'égard du traitement des données à caractère personnel,[7] qui ont été établis en tant qu'organes indépendants dotés de compétences de supervision et de conseil. En particulier, le CEPD veille à ce que les institutions et les organismes communautaires traitent les données personnelles des citoyens dans le respect de la légalité ; il conseille les instances décisionnelles de l'UE sur les nouvelles propositions de loi et sur toute question ayant un impact sur la protection des données. Il coopère également avec les autorités nationales chargées de la protection des données pour promouvoir un niveau homogène de protection des données dans l'UE (pour une sélection des Avis du CEPD, voir la liste présentée en Annexe).[8] Le Groupe de protection offre une plate-forme pour une telle coopération en réunissant des représentants des autoritésnationales chargées de la protection des données, du CEPD et de la Commission européenne.[9]

Toutefois, le cadre juridique que l'on vient de présenter ne s'applique qu'aux domaines d'action de l'ELSJ qui sont regroupés sous le Titre IV du TCE (visas, asile et immigration) – le « premier pilier ». Des problèmes touchant la protection des données peuvent également se présenter dans les domaines de l'ELSJ relevant du Titre VI du TUE (coopération policière et judiciaire dans les affaires criminelles) – le troisième pilier – qui sont régis par la décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale,[10] récemment adoptée. Cette division est le résultat de la structure de l'ELSJ, qui englobe différents piliers. En conséquence, le niveau de la protection dans l'UE risque d'être abaissé et sa cohérence minée, en particulier parce que la décision-cadre ne s'applique pas au traitement d'un large éventail de données personnelles, notamment les données internes, les données échangées entre les Etats membres et les pays tiers, et les données traitées par Europol, Eurojust, le Système d'Information Schengen (SIS) et le Système d'information douanier (SID).

2. Insuffisances et enjeux dans le domaine de la protection des données

L'ELSJ est inspiré par la ferme conviction que la technologie offre la solution à toutes les menaces contre la sécurité, sans examiner la possibilité que cette technologie entraîne une insécurité accrue en matière de droits fondamentaux et de libertés fondamentales, en particulier pour ce qui concerne le droit à la protection des données personnelles tel qu'il est établi à l'article 8 de la Charte des droits fondamentaux. L'UE a jusqu'à présent développé un certain nombre de bases de données et de systèmes d'échange d'informations, parmi lesquels on trouve:[11]

• EURODAC, une base de données contenant les empreintes digitales de tous les demandeurs d'asile et de toutes les personnes arrêtées alors qu'elles franchissaient de manière irrégulière les frontières extérieures de l'UE. A la fin de 2007, EURODAC contenait 1 086 246 séries d'empreintes, et avait coûté €8,1 millions à l'UE, après cinq années de fonctionnement. Après une baisse entre 2005 et 2006, les statistiques d'EURODAC pour 2007 montrent une augmentation de 19% du nombre des transactions relatives à des données sur les demandeurs d'asile (197.284 contre 165.958 en 2006). En outre, le nombre de personnes arrêtées en raison d'un franchissement irrégulier de la frontière extérieure de l'UE a reculé de 8% en 2007 (38.173).[12]

1 Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995 L 281/31).

2 Directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JO 1998 L 24/1).

3 Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002 L 201/37), modifiée par la directive 2006/24/CE (JO 2006 L 105/54).

4 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

5 JO 2000 C 364/1.

6 Art. 41 du règlement 45/2001/CE relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO 2001 L 8/1).

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

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

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

10 Décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO 2008 L 350/60).

11 Pour un aperçu complet des bases de données et des systèmes d'échange des informations de l'UE, on se référera à F. Geyer (2008), "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice", CHALLENGE Research Paper No. 9, May 2008, Centre for European Policy Studies.

12 Commission européenne, Communication, Rapport annuel sur les activités de l'Unité centrale d'EURODAC en 2007, COM (2009) 13, 26.1.2009, Bruxelles.

• Le Système d'Information Schengen (SIS), une base de données utilisée par les autorités des Etats membres de Schengen pour échanger des données sur certaines catégories de personnes et de biens. Elle avait au départ été créée comme une base de données de ressortissants de pays tiers dont l'entrée dans l'UE devait être rejetée ; elle est devenue le SIS + pour inclure les Etats devenus membres en 2004. Cette dernière version doit à son tour être transformée (avec de nouvelles capacités et de nouvelles informations) pour aboutir à la deuxième génération du SIS : le SIS II.[13]

• Le Système d'Information sur les Visas (VIS), qui contiendra des informations sur toutes les personnes qui demandent un visa pour un court séjour dans l'UE.

• En outre, la Commission européenne a proposé de créer trois nouvelles bases de données à l'échelle de l'UE dans le cadre de son paquet Frontières de 2008, à savoir : un système d'entrée-sortie qui enregistre les mouvements de catégories spécifiques de résidents de pays tiers aux frontières extérieures de l'UE ; un système automatisé de contrôle aux frontières pour la vérification de l'identité des voyageurs (citoyens de l'UE et ressortissants des pays tiers) sur la base de la technologie de la biométrique ; et un système électronique d'autorisation de voyage qui oblige les voyageurs non communautaires à fournir des données personnelles pour un contrôle en ligne effectué avant le départ (voir le Briefing Paper sur les Frontières).

Le contenu et la manière dont ces outils sont utilisés suscitent toutefois un certain nombre de préoccupations.

Tout d'abord, l'extraction de données est l'une des questions les plus sensibles du débat sur la protection des données. Les résultats des recherches menées dans les bases de données par les autorités répressives peuvent être problématiques suivant la manière avec laquelle elles sont menées. Par exemple, étant donné que toute la population ne figure pas dans chacune des bases de données, les soupçons tendent donc à se porter uniquement sur les personnes dont les données figurent dans le système et qui répondent au profil que les autorités recherchent. Les différents types de recherche soulèvent des problèmes différents. La recherche ou les recherches multiples d'individu menées par les services répressifs sont en général les plus fréquentes. Les recherches basées sur des profils dans les cas où les fonctionnaires des services répressifs ne connaissent pas l'identité de la personne recherchée posent bien plus de problèmes. L'utilisation à des fins répressives de données collectées commercialement peut également poser des problèmes. Pour éviter le risque de préjudices inutiles aux personnes, les données personnelles collectées à des fins répressives doivent être précises. Des problèmes se posent lorsque des données originales sont intégrées à des informations plus récentes, généralement lorsque la personne concernée attire l'attention des autorités, ce qui résulte en un portrait complètement arbitraire de l'intéressé. En outre, les données personnelles collectées à des fins sécuritaires doivent être adéquates et proportionnelles aux fins pour lesquelles elles ont été collectées : en effet, une collecte indiscriminée de données non seulement ne constitue pas une garantie d'une meilleure sécurité, mais viole les droits à la vie privée de chaque individu.

Autre source majeure de préoccupation : la nécessité de garantir que l'accès aux données sensibles est strictement limité aux personnes qui doivent réellement disposer de ces données. L'accès aux bases de données de l'UE dépend de l'instrument qui a établi la base de données. Par exemple, l'accès à EURODAC est limité aux fonctionnaires qui vérifient si un demandeur d'asile n'a pas déjà introduit une demande d'asile dans un autre pays (ou est arrivé de manière irrégulière), mais il existe des pressions pour élargir cet accès à tous les services répressifs. La qualité des organismes qui collectent, traitent et échangent les données doit donc faire l'objet d'une évaluation prudente, tout comme l'examen des implications de l'octroi à des services de pays tiers de l'accès aux bases de données de l'UE, pour assurer que les données personnelles de chaque citoyen sont traitées de manière adéquate et dans le respect de la légalité.

Enfin, les citoyens doivent bénéficier d'une protection adéquate face aux risques posés par des inexactitudes dans les données ou une absence de rigueur dans les échanges de données. Ils devraient être dûment informés des droits qui sont les leurs à cet égard. Une enquête Eurobaromètre menée en 2008[14] a montré que si la majorité des citoyens de l'UE (64%) sont préoccupés par les questions relatives à la protection des données, seul un quart d'entre eux (27%) sont informés des droits dont ils bénéficient en cas d'utilisation abusive de leurs données personnelles, et moins d'un tiers (29%) savent que les données sensibles comme les informations sur les origines raciales ou ethniques bénéficient d'une protection juridique particulière. Les droits de la personne concernée, et une information effective à leur sujet, doivent donc être considérés comme un autre problème essentiel dans le débat sur la protection des données, de manière à éliminer les incohérences qui sapent actuellement le cadre légal de l'UE sur la protection des données, en particulier s'agissant de son application à l'ELSJ. Le niveau de garantie octroyé au sein de l'UE est loin d'être homogène, parce que les droits de la personne concernée varient largement suivant la base de données où elle figure, et parce que l'écart entre les normes atteintes dans les domaines d'action relevant respectivement du premier et du troisième pilier reste significatif.

3. Défis futurs et recommandations

Les principaux défis que l'on peut identifier concernant la protection des données dans l'ELSJ de l'UE sont les suivants :

Premièrement, les règles relatives au respect de la vie privée devraient être intégrées dans les programmes qui gèrent les bases de données et les systèmes d'information de l'UE. Ces programmes devraient prévoir la suppression automatique des données à l'expiration de la période autorisée, empêcher tout accès non autorisé au système et toute duplication d'images sur des écrans d'ordinateur, et interdire les recherches trop nombreuses dans les bases de données, excepté suite à une décision de justice.

Deuxièmement, les bases de données ne devraient être établies sans que des études d'impact soient menées au préalable par des organismes objectifs et indépendants. Toute stratégie de l'UE prévoyant obligatoirement des échanges de données doit être précédée par un inventaire et une évaluation des politiques en cours, des outils utilisés et des structures institutionnelles impliquées dans les échanges de données dans le domaine de la sécurité au niveau de l'UE. De nouvelles bases de données ne peuvent être établies et utilisées qu'à des fins spécifiques et licites, en évitant les définitions vagues et ouvertes et la collecte de données sans but précis.

Troisièmement, les systèmes de collecte de données ne doivent pas révéler de données sensibles, relatives à l'origine ethnique, aux convictions religieuses ou à d'autres aspects interdits par les dispositions du droit communautaire sur la non-discrimination. Les critères qui permettent d'établir indirectement des distinctions ethniques ou religieuses, comme le lieu de naissance des parents ou de la personne concernée, ou l'ancienne nationalité, doivent être interdits.

13 Rapport de la Commission relatif au développement du système d'information Schengen de deuxième génération (SIS II) - Rapport sur l'état d'avancement des travaux - Juillet 2008 - décembre 2008 COM (2009) 133, 24.3.2009, Bruxelles.

14 The Gallup Organisation (2008), "Data Protection in the European Union. Citizens'perceptions", Eurobaromètre, page 5.

ANNEXE

Mesures adoptées

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).

Avis adoptés par le Contrôleur européen de la protection des données en 2009
Supervision

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).

Avis adoptés en 2008 par le Groupe de protection des personnes à l'égard du traitement des données à caractère personnel

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.