11ème rapport annuel

du Groupe de travail « Article 29 »

sur la protection des données

COMMISSION EUROPEENNE

1830-6454

11ème rapport annuel

sur l'état de la protection des personnes à l'égard du traitement des données à caractère personnel dans l'Union européenne et les pays tiers

portant sur l'année 2007

Adopté le 24 juin 2008

Le présent rapport a été produit par le Groupe de travail « Article 29 » sur la protection des données. Il ne reflète pas nécessairement les avis et les points de vue de la Commission européenne et n'est pas lié par ses conclusions.

Ce rapport est également disponible en allemand et en anglais. Il peut être téléchargé sur le site de la Direction générale « Justice, Liberté et Sécurité » section « Protection des données » à l'adresse suivante http ://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm

TABLE DES MATIÈRES

PRÉSENTATION DU PRÉSIDENT DU GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES

Le développement technologique et économique entraîne un traitement de plus en plus complet des données à l'aide de systèmes informatiques de plus en plus complexes. Simultanément, une coopération accrue entre les États membres de l'UE participe de manière significative au traitement transfrontalier des données à caractère personnel, comme dans le cadre de la directive « services » de l'UE.

De plus, les initiatives lancées par le Conseil ou la Commission avec pour objectif d'améliorer la lutte contre le terrorisme et la criminalité ont un impact sur le traitement des données à caractère personnel au sein du marché intérieur. C'est le cas, par exemple, de la directive 2006/24/CE, qui demande aux fournisseurs de télécommunications et de services Internet de conserver les données relatives au trafic pour un usage ultérieur, et aux transporteurs aériens de transférer les données des passagers qu'ils collectent et conservent dans le cadre de la prestation de leurs services.

Il va donc sans dire qu'en 2007, les autorités européennes chargées de la protection des données ont dû faire face à de multiples défis, ce qui ne les a pas empêchées de s'acquitter également de tâches importantes. Le Groupe de travail « Article 29 » a ainsi adopté 17 avis. De plus, il a élaboré et publié d'autres documents sur d'importantes questions en rapport avec la protection des données.

Un sujet majeur cette année a été le traitement très controversé des données des passagers collectées par les transporteurs aériens à des fins répressives. Le Groupe de travail « Article 29 » s'est montré particulièrement critique envers les négociations sur un accord UE-États-Unis sur les données PNR et a critiqué avec véhémence la présentation par la Commission, en novembre 2007, d'un modèle qui viserait à introduire un régime similaire dans l'UE.

Le Groupe de travail a également beaucoup contribué à l'interprétation du concept de « données à caractère personnel » au sens de la directive 95/46/CE. Il a abordé le sujet difficile et pourtant vital des règles d'entreprise contraignantes afin d'accélérer la procédure de coordination entre les autorités chargées de la protection des données et, à la suite de longs débats, il a convaincu la société SWIFT, qui était critiquée à cause de l'accès des autorités américaines aux données relatives à ses transferts de fonds internationaux, de changer sa méthode de traitement des données ainsi que ses transferts de données en mettant sur pied un nouveau centre opérationnel en Europe.

Citons quelques-uns des domaines clé :

Une des principales activités du Groupe de travail « Article 29 » durant l'année couverte par ce rapport fut la 1re Journée de la protection des données, qui s'est tenue le 28 janvier, date anniversaire de l'adoption de la convention européenne no 108 par le Conseil de l'Europe en 1981.

Proclamées conjointement par les autorités européennes chargées de la protection des données et le Conseil de l'Europe, de nombreuses activités ont été lancées en collaboration avec des parlementaires, des politiciens et des ONG à travers l'Europe avec, pour principale motivation, d'informer les citoyens européens, de sensibiliser les plus jeunes et d'examiner les problèmes pour parvenir à une protection efficace de la vie privée. Portes ouvertes, tables rondes, rencontres avec des représentants haut placés des gouvernements ainsi qu'une large couverture médiatique ont souligné l'importance de la protection des données dans le contexte des dernières propositions de l'UE et initiatives de l'industrie qui menacent le respect de la vie privée de nos citoyens.

Une évaluation approfondie des activités relatives à la Journée européenne de la protection des données, qui avait pour but l'échange d'expériences entre les autorités chargées de la protection des données et la diffusion des bonnes pratiques, aidera à améliorer les résultats en 2008 et dans les années à venir.

En rédigeant et en adoptant un avis sur les données à caractère personnel (**WP 136**), le Groupe de travail « Article 29 » a apporté une importante contribution à l'interprétation uniforme et à l'application harmonisée d'un concept clé de la directive 95/46/CE. Une divergence d'interprétation de la notion de données à caractère personnel pourrait compromettre la sécurité juridique et constituer un frein à la libre circulation des données. Cet avis, qui vise à donner des orientations à toute personne concernée par la collecte et le traitement des données à caractère personnel, doit être considéré comme une étape importante dans le travail réalisé par le Groupe de travail « Article 29 », et sera utile lors des nombreuses prochaines discussions relatives à la possibilité d'utiliser et de réidentifier des données anonymisées.

En juillet 2007, le troisième accord PNR UE-États-Unis a été signé à la suite d'un débat aussi intense que constructif avec la Commission et le Conseil sur les principes fondamentaux de l'accord ainsi que d'un atelier qui a connu une large participation, organisé conjointement avec la commission LIBE du Parlement européen en mars 2007.

Si dans son avis **WP 138** adopté le 17 août 2007, le Groupe de travail a favorablement accueilli le fait que le nouvel accord à long terme fournisse une base légale au transfert des données des passagers, et évite ainsi un vide juridique, il a cependant explicitement critiqué le niveau de protection des données prévu dans l'accord, jugé trop faible. Le nouvel accord laissant de nombreuses questions ouvertes, le Groupe de travail « Article 29 » s'est tourné vers la Commission et le Conseil dans l'espoir de clarifier au moins ces questions-là.

En ce qui concerne la proposition relative à l'utilisation des données PNR présentée par la Commission le 6 novembre 2007, le Groupe de travail « Article 29 » n'a pu qu'exprimer sa grande déception (**WP 145**). En effet, la proposition se calque trop sur l'accord relatif aux PNR précédemment signé entre l'UE et les États-Unis. La Commission ne pourrait, selon les agences chargées de la protection des données, justifier aucun besoin urgent pour un tel système supplémentaire, en particulier si l'on considère la directive 2004/82/CE (directive API), qui exige déjà des compagnies aériennes de collecter les données contenues dans les passeports des passagers pouvant, outre les contrôles douaniers et de l'immigration, être également utilisées à des fins répressives. Le Groupe de travail « Article 29 » maintient que, sans tenir compte des nombreux défauts et failles encore à revoir, une évaluation approfondie de la directive API devrait avant tout être menée afin de déterminer si les données des passagers constituent effectivement un outil utile dans la lutte contre le terrorisme et la criminalité organisée.

Il a, en conséquence, appelé le Conseil à dialoguer avec toutes les agences et sociétés impliquées dans la collecte et le traitement des données des voyageurs, en particulier les compagnies aériennes, les opérateurs de systèmes de réservation informatisés, le Parlement européen, ainsi que les organisations de protection des données et des consommateurs pour trouver des solutions d'amélioration du respect de la vie privée qui soient acceptables pour toutes les parties prenantes, et qui tiennent compte de leurs préoccupations légitimes.

Cette année a également été marquée par l'adoption de l'avis **WP 130** relatif au traitement des données à caractère personnel dans les dossiers médicaux électroniques tenus par les hôpitaux, les médecins et les autorités sanitaires. Étant donné l'importance de ce secteur et le fait que, dans ce contexte, des données à caractère particulièrement sensible sont collectées et traitées, le Groupe de travail « Article 29 » a estimé indispensable de sensibiliser et de conseiller toutes les personnes travaillant dans ce domaine. À la suite de la publication de son avis dans le cadre de ce que l'on appelle une « procédure de consultation », le Groupe de travail « Article 29 » a reçu de nombreux commentaires qui seront débattus et pourraient être pris en compte en 2008.

Le Groupe de travail a publié, dans un rapport final sur son site web, ses conclusions sur l'action commune de mise en application des autorités chargées de la protection des données des États membres dans le secteur de l'assurance maladie. Pour la première fois, toutes les autorités européennes chargées de la protection des données ont collaboré de manière systématique à l'examen d'un secteur industriel qui concerne presque tous les citoyens européens, et qui collecte et traite de gigantesques quantités de données à caractère personnel, dont une grande majorité sont à caractère sensible. Suite aux résultats de l'enquête, le Groupe de travail « Article 29 » continuera de contrôler la mise en application de la directive 95/46/CE dans d'autres secteurs dans les années à venir.

Les 15 et 16 octobre 2007, la 3e Safe Harbor Conference s'est tenue à Washington, organisée cette fois-ci par le ministère américain des affaires économiques et la commission américaine du commerce. La conférence a mis en avant l'importance que le Groupe de travail « Article 29 », la Commission et les autorités américaines participantes attribuent aux relations UE-États-Unis dans le domaine de la protection des données. Les participants ont jugé crucial qu'en vue d'un échange de plus en plus important de personnes et de biens entre les deux continents, un tel dialogue soit poursuivi et intensifié. Étant donné le nombre croissant de défis, il est important de tenir compte des nouveaux développements politiques et technologiques. Tous les participants ont confirmé que la Safe Harbor Conference était un lieu de débat approprié pour parvenir à une meilleure compréhension du système de protection des données des uns et des autres, et pour établir des bases légales et réelles communes pour garantir une protection efficace des données à caractère personnel.

De plus, le Groupe de travail « Article 29 » a également convenu d'une procédure pour accélérer les procédures d'approbation des règles contraignantes en matière de traitement des données à caractère personnel par les entreprises internationales (règles d'entreprise contraignantes). Malgré certains progrès dans ce domaine, il reste encore beaucoup à faire pour améliorer la coordination actuelle entre les autorités de contrôle. C'est pourquoi, le Groupe de travail « Article 29 » intensifiera le dialogue avec l'industrie dans le but de parvenir à une meilleure optimisation des procédures.

De plus, à la demande de la Commission, le Groupe de travail a adopté des avis sur le système d'information du marché intérieur (**WP 140**) et sur le système de coopération en matière de protection des consommateurs (**WP 139**). Les questions abordées dans ces avis seront d'importance dans les travaux futurs du groupe.

En général, l'année 2007 a été globalement marquée par une tendance à l'intrusion croissante des organisations gouvernementales et des entreprises dans la vie privée des citoyens. Rien n'indique que cette tendance diminuera, même dans les années à venir. C'est pourquoi, il est fondamental que la société soit consciente de ces menaces et réagisse de manière appropriée. Dans le futur, le Groupe de travail « Article 29 » s'efforcera également de contribuer à garantir les droits fondamentaux des citoyens à la protection de leurs données.

Ceci est le dernier rapport d'activité que je présente en tant que Président du Groupe de travail « Article 29 », puisque mon second mandat prendra fin en février 2008. C'est pourquoi, j'aimerais saisir cette occasion pour remercier tous mes collègues qui ont contribué aux résultats de cette collaboration. Je souhaiterais mentionner en particulier le professeur José Luis Piñar Mañas qui, de février 2004 à février 2007, a représenté le Groupe de travail « Article 29 » en tant que vice-président, ainsi qu'Alex Türk, le président de la CNIL, qui a assumé cette tâche en avril 2007. J'aimerais particulièrement remercier le secrétariat d'Alain Brun, le chef d'unité, qui a apporté son soutien à notre travail de façon remarquable, ainsi que tous les membres d'équipe des autorités nationales chargées de la protection des données qui, dans l'ombre, ont contribué au succès de notre entreprise.

Peter Schaar

Chapitre 1

Questions examinées par le Groupe de travail «Article 29» sur la protection des données à caractère personnel[1]

[1] Tous les documents adoptés par le Groupe de travail «Article 29» sur la protection des données figurent sur http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_fr.htm

1.1. TRANSFERT DE DONNÉES VERS LES PAYS TIERS

1.1.1. Dossiers Passagers (PNR)

Avis 2/2007 (WP 132) concernant l'information des passagers au sujet du transfert des données des dossiers passagers (Passenger Name Record – PNR) aux autorités américaines

Cet avis ainsi que ses annexes (questions fréquemment posées et modèles de notes) sont destinés aux agences de voyages, aux compagnies aériennes et à toutes les autres organisations fournissant des prestations de services de voyages aux passagers effectuant un vol à destination et au départ des États-Unis d'Amérique. Cet avis et ses annexes mettent à jour et remplacent l'avis précédent du 30 septembre 2004 (WP 97). L'accord intérimaire du 16 octobre 2006 constitue le cadre juridique existant pour le transfert des informations PNR aux autorités américaines. Le début des négociations en vue d'un nouvel accord[2] est prévu pour 2007. Cet avis a donc pour but de donner des conseils et orientations quant aux questions suivantes : qui doit fournir quelle information? Comment? Et quand? L'avis contient des conseils quant aux informations données par téléphone, en personne et sur internet.

Le Groupe de travail « Article 29 » a établi des modèles de notes d'information (annexés à cet avis) afin de simplifier la tâche des organisations devant fournir ces renseignements et également afin de s'assurer de la cohérence des informations fournies dans l'ensemble de l'Union européenne.

Avis 5/2007 (WP 138) concernant le nouvel accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure, conclu en juillet 2007

Le présent avis vise à analyser les conséquences du nouvel accord sur le transfert de données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure (DHS) sur les libertés et droits fondamentaux et, en particulier, sur le droit des passagers au respect de la vie privée. La conclusion d'un nouvel accord à long terme fournit une base juridique au transfert de données des dossiers passagers. Le Groupe de travail a toujours soutenu la lutte contre le terrorisme international et la criminalité organisée transnationale, car il la juge nécessaire et légitime. Néanmoins, toute restriction des libertés et droits fondamentaux des personnes, dont le droit au respect de la vie privée et le droit à la protection des données, doit reposer sur un fondement solide et assurer un juste équilibre entre les exigences inhérentes à la protection de la sécurité publique et d'autres intérêts généraux, tels que le droit au respect de la vie privée des personnes.

Avis commun (WP 145) sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives présentée par la Commission le 6 novembre 2007

Le présent avis a pour objectif d'analyser les répercussions sur les droits et libertés fondamentaux, en particulier le droit à la vie privée des passagers, de la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives, présentée par la Commission européenne le 6 novembre 2007. La proposition est largement inspirée de l'accord PNR UE-USA signé en juillet 2007 et nombre de ses dispositions sont similaires à celles dudit accord. Aussi les préoccupations en matière de protection de la vie privée exprimées par le Groupe de travail « Article 29 » au sujet de cet accord PNR restent-elles d'actualité pour quelques mesures exposées dans le présent avis. Celui-ci prend également en considération les conclusions de l'avis 9/2006 du Groupe de travail « Article 29 » du 27 septembre 2006 sur la directive 2004/82/CE du Conseil puisque celle-ci prévoit aussi le transfert des données des dossiers passagers aux autorités publiques par les transporteurs aériens. Cependant, dans le cas d'un régime PNR européen, la limitation des droits et libertés fondamentaux doit être solidement justifiée et trouver le juste milieu entre le besoin de protéger la sécurité publique et la restriction des droits des personnes physiques.

[2] Un nouvel accord a été signé entre l'Union européenne et les États-Unis d'Amérique à Bruxelles, le 23 juillet 2007 et à Washington, le 26 juillet 2007. Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007, JO L 204 du 4.8.2007, p.16. Accord entre l'Union européenne et les États-Unis d'Amérique, JO L 204 du 4.8.2007, p.18 http://europa.eu.int/eur-lex/lex/JOHtml.do?year=2007&serie=L&textfield2=204&Submit=Search&_submit=Search&ihmlang=fr

1.1.2. Règles d'entreprise contraignantes (BCR)

Recommandation 1/2007 (WP 133) sur les demandes standards d'approbation des règles d'entreprise contraignantes pour le transfert des données à caractère personnel.

La directive 95/46/CE sur la protection des données ne permet le transfert des données à caractère personnel à l'extérieur de l'EEE que lorsque le pays-tiers assure « un niveau de protection adéquat des données personnelles (art. 25) ou lorsque le responsable de traitement offre des garanties suffisantes au regard de la protection de la vie privée (art. 26). Bien que les règles d'entreprise contraignantes BCR ne soient pas un outil expressément inscrit ni mentionné dans la directive 95/46/CE sur la protection des données, les BCR sont l'une des manières par lesquelles de telles garanties suffisantes (art. 26) peuvent être démontrées « par un groupe de sociétés dans le cadre des transferts intra-groupe ».[3] L'utilisation des BCR comme base légale des transferts de données internationaux en provenance de l'EEE suppose l'approbation de chacune des autorités de protection de données (DPA) des pays à partir desquels les données doivent être transférées.

1.1.3. Jersey

Avis 8/2007 (WP 141) sur le niveau de protection des données à caractère personnel à Jersey

Les îles Anglo-Normandes se composent de cinq îles principales : Jersey, Guernesey, Aurigny, Herm et Sercq, qui sont situées dans la Manche, dans le golfe de Saint-Malo, au large des côtes nord-ouest de la France. Sur le plan constitutionnel, elles sont divisées en deux bailliages, celui de Guernesey et celui de Jersey. Le bailliage de Jersey est une dépendance de la Couronne britannique. Le Royaume Uni est responsable des affaires internationales et de la défense de l'île, tandis que celle-ci est autonome du point de vue de ses affaires intérieures, dont la protection des données. Jersey fait partie du territoire douanier communautaire. Le tarif douanier commun, les prélèvements et autres mesures à l'importation de produits agricoles sont applicables aux échanges entre Jersey et les pays tiers, et les marchandises circulent librement entre l'île et la Communauté. En revanche, certaines autres règles communautaires, dont celles liées à la protection des données, ne sont pas applicables. Lors de la transposition de la directive par le Royaume-Uni, les autorités de Jersey avaient signalé que cette législation ne s'appliquerait pas sur leur territoire. Depuis lors, elles ont introduit leur propre réglementation dans ce domaine. En vertu de l'Article 299 du traité instituant la Communauté européenne, la directive ne s'applique pas à Jersey, qui est donc un pays tiers au sens des articles 25 et 26 de la directive.

1.1.4. Îles Féroé

Avis 9/2007 (WP 142) sur le niveau de protection des données à caractère personnel aux îles Féroé

Situées dans le nord de l'Atlantique, les îles Féroé se composent de 18 îles et sont divisées en sept comtés, eux-mêmes divisés en 120 communautés. Elles constituent, avec le Danemark et le Groenland, le Royaume de Danemark, qui est une monarchie constitutionnelle. Par la loi d'autonomie de 1948, les îles Féroé sont devenues une communauté autonome au sein du Royaume de Danemark. Cette loi divise l'ensemble des domaines de politique en deux grandes catégories, les affaires communes, administrées par le Royaume, et les affaires spécifiques (féroïennes), gérées par les autorités législatives et administratives locales féroïennes. Aux îles Féroé, les aspects relatifs aux données à caractère personnel sont réglementés par des lois adoptées par le parlement féroïen et par des lois régissant les affaires communes. La loi sur la protection des données, adoptée en 2001 par le parlement local, est administrée par l'Agence féroïenne de protection des données.

La loi danoise sur la protection des données ne concerne que le traitement de données effectué par les autorités du Royaume (la police, le ministère public, les autorités pénitentiaires du comté, le service pénitentiaire et de probation, le Haut commissaire des îles Féroé, les

[3] Voir document de travail WP 74, Section 3.1: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_fr.htm

autorités chargées du traitement des affaires relevant du droit des familles, les autorités cléricales). Étant donné qu'elle découle de la directive[4], elle est censée fournir un niveau de protection au moins adéquat en ce qui concerne le traitement de données à caractère personnel et, par conséquent, les domaines qu'elle couvre ne sont pas examinés dans le présent document.

1.2. COMMUNICATIONS ÉLECTRONIQUES INTERNET ET NOUVELLES TECHNOLOGIES

Avis 1/2007 (WP 129) sur le Livre vert sur les technologies de détection dans le travail des services répressifs, des douanes et d'autres services de sécurité

Le 1er septembre 2006, la Commission européenne a adopté le Livre vert sur les technologies de détection dans le travail des services répressifs, des douanes et d'autres services de sécurité (COM(2006) 474), ci-après le « Livre vert ». L'objectif poursuivi est de susciter un débat au niveau européen au sujet des technologies de détection et de réunir le plus possible de « réponses stimulantes et de propositions concrètes » en vue de « renforcer l'approche commune des technologies de détection » au « sens le plus large possible ». Le Groupe de travail « Article 29 » a été invité avec d'autres parties à prendre part au processus de consultation.

Les réponses aux questions posées dans le Livre vert ainsi que d'autres commentaires éventuels influenceront les mesures et actions concrètes futures. Et, selon les priorités identifiées lors du processus de consultation publique, des mesures spécifiques pourraient être prises dès que possible. Si des intervenants manifestent leur intérêt, une task-force pourrait être créée pour des actions sur des sujets spécifiques. Elle pourrait être composée de représentants des autorités nationales de différents États membres et d'experts du secteur privé.

[4] Loi n° 429 du 31 mai 2000 sur le traitement des données à caractère personnel. Cette loi transpose la directive 95/46/CE du 24 octobre 1995 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.

1.3. COMPTABILITÉ, AUDIT ET AFFAIRES FINANCIÈRES

Huitième directive sur les contrôles légaux des comptes Avis n° 10/2007 (WP 143) du Groupe de travail « Article 29 »

Le 15 février 2007, le Groupe de travail « Article 29 » a examiné un document de travail présenté par la DG Marché intérieur sur la transmission aux régulateurs publics de pays tiers de documents d'audit contenant des données à caractère personnel. Ce document de travail expose le cadre réglementaire européen établi par la directive 2006/43/CE concernant les contrôles légaux des comptes annuels et des comptes consolidés[5] (« la huitième directive »). La huitième directive fixe les conditions d'exercice de l'activité de contrôleur légal des comptes et prévoit une supervision publique indépendante des contrôleurs légaux des comptes, assurée par les États membres. Elle contient également des dispositions particulières concernant la coopération entre les organismes de supervision publique des États membres et les autorités compétentes des pays tiers. Cette coopération devrait comprendre l'échange, avec les autorités de pays tiers, des documents d'audit et d'autres documents détenus par les cabinets d'audit européens.

1.4. DONNÉES À CARACTÈRE PERSONNEL

Avis 4/2007 (WP 136) sur le concept de données à caractère personnel

Le Groupe de travail reconnaît la nécessité de mener une analyse approfondie du concept de données à caractère personnel. Les informations relatives aux pratiques actuelles dans les États membres de l'UE semblent indiquer un certain degré d'incertitude et de diversité dans les pratiques, d'un État membre à l'autre, sur des aspects importants de ce concept, ce qui risque d'affecter le bon fonctionnement du cadre existant en matière de protection des données dans différents

[5] JO L 157 du 9.6.2006, p. 57.

contextes. Les résultats de cette analyse d'un élément capital pour l'application et l'interprétation des règles de protection des données auront nécessairement un impact considérable sur un certain nombre de questions importantes, notamment pour certains domaines, tels que la gestion de l'identité dans le contexte de l'administration en ligne (« e government ») et des services de télésanté (« e health »), de même que dans le contexte de la technologie RFID (radio identification).

L'objectif du présent avis adopté par le Groupe de travail est de parvenir à une même interprétation du concept de données à caractère personnel, des cas dans lesquels la législation nationale en matière de protection des données devrait s'appliquer, et de ses modalités d'application. Élaborer une définition commune de la notion de données à caractère personnel revient à définir ce qui relève ou non du champ d'application des règles nationales de protection des données. Le corollaire de ce travail est de fournir des orientations sur les modalités d'application des règles de protection des données à certaines catégories de situations qui se présentent à l'échelle européenne, afin de contribuer à l'application uniforme de ces normes, une mission essentielle du Groupe de travail « Article 29 ».

1.5. BIOMÉTRIQUES & DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ

Document de travail (WP 131) sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)

Dans le présent document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), le Groupe de travail « Article 29 » donne des indications au sujet de l'interprétation du cadre juridique de protection des données applicable aux systèmes de DME et explique certains principes généraux. Il donne également des indications au sujet des exigences en matière de protection des données auxquelles doit satisfaire l'institution de systèmes de DME ainsi que les garanties applicables.

Le Groupe de travail « Article 29 » examine d'abord le cadre juridique général de protection des données pour les systèmes de DME. Il rappelle l'interdiction générale du traitement de données à caractère personnel relatives à la santé énoncée à l'article 8, paragraphe 1, de la directive 95/46/CE sur la protection des données et examine ensuite l'éventuelle application des dérogations prévues à l'article 8, paragraphes 2, 3 et 4, de cette même directive dans le cadre des systèmes de DME en insistant sur la nécessité d'une interprétation stricte de ces dérogations. Le Groupe de travail « Article 29 » réfléchit également à un cadre juridique adapté aux systèmes de DME et formule des recommandations sur onze sujets pour lesquels des garanties spéciales au sein des systèmes de DME semblent particulièrement nécessaires afin de garantir les droits à la protection des données des patients et des personnes.

Avis n° 3/2007 (WP 134) sur la proposition de règlement du Parlement européen et du Conseil modifiant les instructions consulaires communes adressées aux représentations diplomatiques et consulaires de carrière, en liaison avec l'introduction d'éléments d'identification biométriques et de dispositions relatives à l'organisation de la réception et du traitement des demandes de visa (COM(2006)269 final).

La proposition de modification des ICC qui fait l'objet du présent avis vise à créer la base juridique pour la collecte obligatoire d'éléments d'identification biométriques des demandeurs de visa et à établir des dispositions concernant l'organisation des consulats des États membres – compte tenu de la politique commune en matière de visas et de l'intégration renforcée entre les bureaux consulaires. L'adoption d'un règlement modifiant les instructions consulaires communes sur les visas en ce qui concerne l'introduction d'éléments d'identification biométriques est une « condition préalable » à la mise en œuvre du système d'information sur les visas, ou Visa Information System (VIS)[6], étant donné que ce règlement définit « le cadre juridique du relevé des identifiants biométriques requis ».

[6] Proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (COM(2004)835 final) présentée par la Commission le 28 décembre 2004.

Le système d'information sur les visas sera mis en place et réglementé dès l'entrée en vigueur du règlement du Parlement européen et du Conseil concernant le VIS et l'échange de données entre les États membres sur les visas de court séjour, qui est en cours d'examen. La création d'une base de données centralisée, contenant des données sur les demandeurs de visas, incluant des empreintes digitales et des photos numérisées (dites « images faciales ») ainsi que des données sur les individus voyageant en groupe et les individus offrant l'hospitalité dans les pays de destination des demandeurs, est considérée comme l'une des clés pour la mise en œuvre d'une politique commune en matière de visas ainsi que pour la réalisation des objectifs définis à l'article 61 du traité instituant la Communauté européenne (TCE), à savoir la libre circulation des personnes dans un espace de liberté, de sécurité et de justice.

1.6. MISE EN APPLICATION

Rapport 1/2007 (WP 137) sur la première action commune de mise en application : évaluation et étapes à venir

Dans son premier rapport sur la mise en œuvre de la directive relative à la protection des données (COM (2003) 265 final), la Commission européenne invitait le Groupe de travail « Article 29 » à « discute[r] périodiquement de la question générale du meilleur respect de la directive… [et à] envisager de lancer des enquêtes sectorielles au niveau communautaire et de tenter de définir des normes en la matière » afin de donner une vue d'ensemble de la mise en application et de fournir des conseils aux différents secteurs, dans le but d'améliorer le respect de la directive de la manière la moins contraignante possible.

En réponse, le Groupe de travail a demandé en juin 2004 à la task-force « mise en application » de débattre d'une stratégie européenne et de critères communautaires pour assurer le respect de la directive. En novembre 2004, dans sa déclaration concernant la mise en application (WP 101), le Groupe de travail « Article 29 » a annoncé qu'il s'engageait à « développer des stratégies de mise en application proactives [et] à accroître les actions de mise en application » et il a établi six critères à prendre en compte pour décider si un secteur doit faire l'objet d'une mise en application concertée.

Considérés conjointement, les critères définis dans le document WP 101 convergeaient vers le choix d'un secteur ayant une activité très harmonisée et dont par ailleurs l'impact sur la protection des données à caractère personnel soit également élevé. Le Groupe de travail « Article 29 » a donc décidé de faire de l'assurance médicale privée, et plus particulièrement de l'assurance-soins de santé, l'objet de sa première intervention synchronisée.

1.7. CONSOMMATEURS

Avis 6/2007 (WP 139) concernant les questions de protection des données posées par le système de coopération en matière de protection des consommateurs (SCPC)

Le présent avis du Groupe de travail « Article 29 » sur la protection des données (ci-après « le Groupe de travail ») porte sur les questions de protection des données posées par le système de coopération en matière de protection des consommateurs (ci-après « le SCPC »), qui est la base de données électronique gérée par la Commission européenne pour l'échange d'informations entre les autorités chargées de la protection des consommateurs dans les États membres et la Commission, conformément aux dispositions du règlement (CE) 2006/2004 relatif à la coopération en matière de protection des consommateurs (ci-après « le règlement CPC »).

Cet avis fait suite à une lettre du 30 mars 2007 du chef de l'unité B-5 « Application du droit et recours des consommateurs » de la direction générale Santé et protection des consommateurs de la Commission européenne (ci-après « la DG SANCO »), adressée au secrétariat du Groupe de travail en vue d'obtenir son avis.

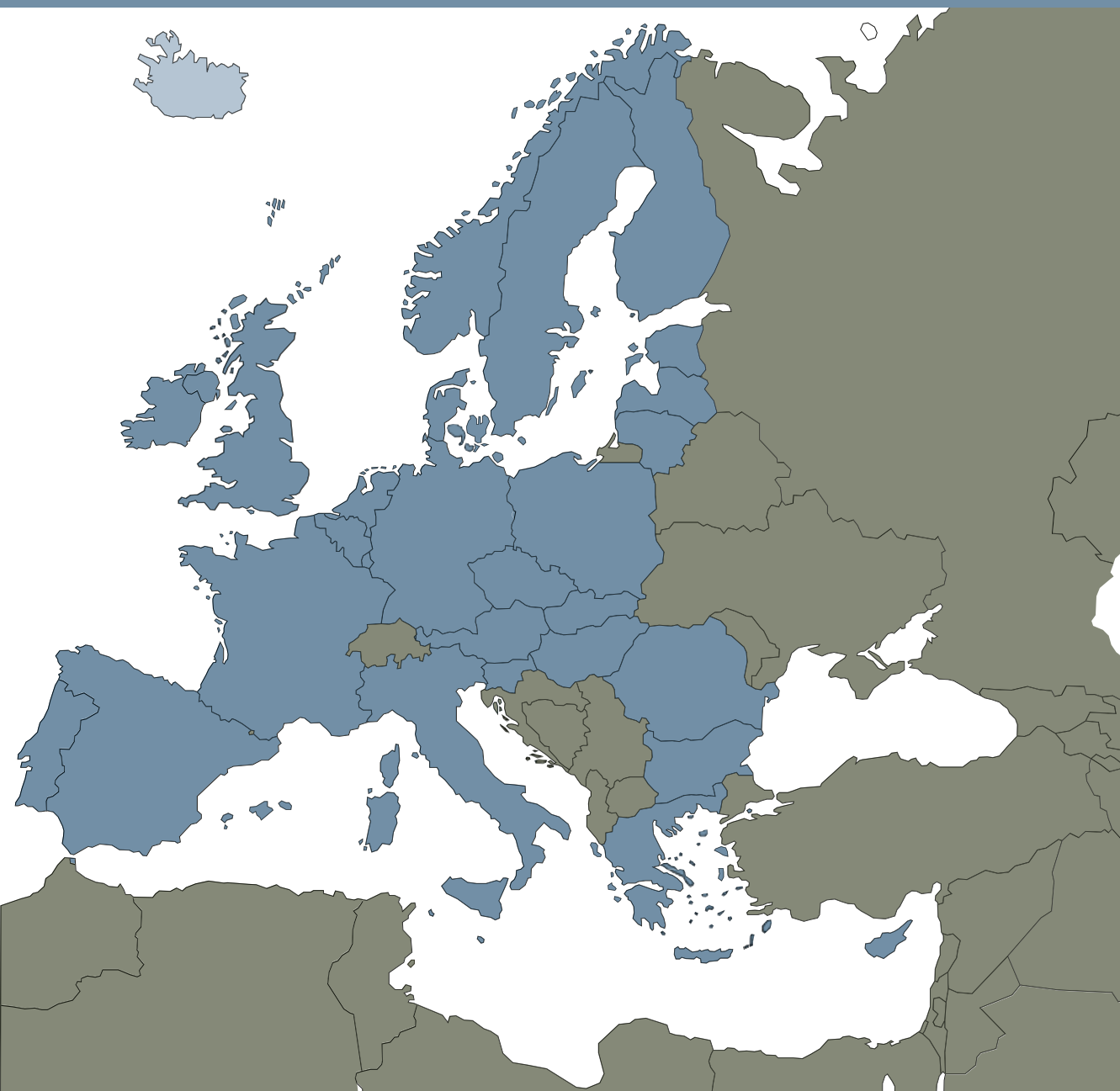
1.8. SYSTÈME D'INFORMATION DU MARCHÉ INTÉRIEUR (IMI)

Avis 7/2007 (WP 140) sur les questions de protection des données liées au système d'information du marché intérieur (IMI)

Le projet de création d'un système informatisé pour l'échange d'informations comportant des données à caractère personnel suscite de sérieuses préoccupations au regard des droits fondamentaux des personnes, et notamment de leur droit à la vie privée.

La complexité du système d'information du marché intérieur (IMI) et la diversité des questions qu'il soulève ont amené la DG « Marché intérieur » de la Commission européenne à solliciter l'avis du Groupe de travail « Article 29 » (« GT29 »). L'avis du GT29 porte essentiellement sur les questions abordées dans les documents « Issue paper on Data Protection in IMI » (Document de réflexion sur la protection des données dans le cadre du système IMI) (D-4784) et « IMI – General Overview » (IMI- Vue d'ensemble) (D-1804). Il a donc pour objet d'analyser les implications de l'IMI sur les données à caractère personnel, dont la protection est garantie par la directive 95/46/CE (« directive sur la protection des données ») et le règlement (CE) n° 45/2001 (« règlement sur la protection des données »).

Chapitre 2
Principaux développements dans les États membres



Autriche

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La **directive 2006/24/CE sur la conservation de données** n'a pas encore été transposée. Un projet publié au printemps 2007 a soulevé beaucoup de critiques et a même reçu un avis négatif de la commission pour la protection des données, qui était censée jouer un rôle de surveillance. Aucun nouveau projet n'a été publié depuis.

B. Jurisprudence

Un citoyen qui souhaitait que sa banque autrichienne lui fasse savoir lesquelles de ses données personnelles avaient été transmises aux autorités des États-Unis par SWIFT a déposé plainte car sa banque ne lui avait pas donné la réponse souhaitée. La commission pour la protection des données a rejeté sa plainte, jugeant que SWIFT avait agi en toute indépendance et que c'était à cette dernière qu'il incombait de fournir ces informations (Affaire K121.245/0009-DSK/2007).

Un patient en désaccord avec un médecin sur le type de traitement requis avait trouvé inopportune la remarque sur son état émotionnel que le médecin avait incluse dans son bref compte rendu de l'incident. Le patient a demandé le retrait de cette remarque sur la base du droit de rectification. L'hôpital (tout comme le responsable du traitement des données) a refusé, et la commission pour la protection des données a rejeté la plainte, jugeant que l'information était correcte dans la mesure où elle faisait partie du compte rendu de l'incident rédigé par le médecin et de l'impression personnelle de celui-ci (Affaire K121.246/0008-DSK/2007).

Un citoyen autrichien avait commis une infraction au code de la route en Suisse. Les autorités autrichiennes ont aidé leurs homologues suisses à identifier cette personne en transmettant des données à caractère personnel. Ce citoyen a déposé plainte devant la commission pour la protection des données et a été débouté. Il a fait appel de la décision devant le tribunal administratif autrichien (*Verwaltungsgerichtshof*, abrégé en VwGH). Il arguait, entre autres, que la commission pour la protection des données n'avait pas l'indépendance que requiert l'article 28 de la directive 95/46/CE. Le tribunal administratif a rejeté tous ses arguments et a confirmé que la commission pour la protection des données était organisée conformément au droit européen applicable (Décision de la VwGH Zl. 2006/06/0322).

Pour la jurisprudence sur la vidéosurveillance, voir le sous-titre « Questions diverses importantes ».

C. Questions diverses importantes

Vidéosurveillance
Les aspects relatifs à la vidéosurveillance restent en tête des préoccupations de la commission pour la protection des données. En 2007, celle-ci a délivré plusieurs permis. L'un concernait la vidéosurveillance dans le réseau de métro de la société des transports publics de Vienne (Wiener Linien GmbH & Co KG). Cette société souhaitait introduire la vidéosurveillance pour lutter contre le vandalisme et protéger ses travailleurs et les passagers. La commission a délivré un permis d'une durée limitée, qui viendra à échéance le 30 juin 2009. Passé ce délai, la société des transports publics de Vienne devra prouver les effets positifs de la vidéosurveillance pour obtenir le renouvellement de son permis.

Ce sujet a suscité beaucoup de discussions, tout comme l'emploi de la vidéosurveillance dans les grands immeubles à appartements.

La question de la vidéosurveillance a été plus souvent abordée dans les médias et les citoyens y ont été fort attentifs.

Évaluation de la solvabilité
Ces dernières années, les fournisseurs de téléphonie mobile autrichiens et d'autres sociétés ont pris pour habitude de vérifier la solvabilité de chaque nouveau client. Face à cette pratique, beaucoup de citoyens dont la demande avait été rejetée à la suite d'un avis négatif ont déposé plainte. La commission pour la protection des données a traité plusieurs aspects de cette problématique. Elle a souvent jugé insatisfaisante la façon dont les agences d'évaluation de la solvabilité traitaient les personnes concernées qui exerçaient

leurs droits d'accès, de rectification et de suppression. L'exactitude des données méritait aussi attention.

Une agence d'évaluation de la solvabilité a affirmé ne pas être le responsable du traitement des données pour une part du processus d'évaluation parce que les sociétés qui commandaient ces évaluations se contentaient d'introduire les données brutes dans un système de cotation placé sous leur responsabilité. La commission pour la protection des données a jugé cet argument fondé et a déclaré que les sociétés elles-mêmes étaient les responsables du traitement des données pour cette partie du système. Il a été fait appel de cette décision de la commission devant la Cour constitutionnelle autrichienne (*Verfassungsgerichtshof*).

De plus, la commission pour la protection des données a pris des mesures pour arrêter des règles strictes pour les bases de données des agences d'évaluation de la solvabilité, surtout pour une grande base de données appelée « registre du crédit à la consommation » (*Konsumentenkreditevidenz*).

Belgique

A. Mise en œuvre des Directives 95/46/CE et 2002/58/CE et autres développements législatifs

A l'occasion du 15ème anniversaire de la *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la Loi Vie privée) qui transpose la directive 95/46/CE, la Commission de la protection de la vie privée (ci-après la Commission belge ou la Commission) a préparé une *Version annotée*[7] de cette législation. Ce commentaire propose pour chacun des articles de la loi, un certain nombre de références – normatives et jurisprudentielles – jugées utiles à la remise en contexte de ces dispositions, à leur bonne compréhension ainsi qu'à leur interprétation. Les textes règlementaires européens (tant de l'Union européenne que du Conseil de l'Europe), les avis du Groupe 29, la jurisprudence de la Cour européenne des droits de l'homme figurent parmi les sources notamment mentionnées dans ce guide de références. Cet anniversaire a par ailleurs été l'occasion pour la Commission belge de faire le point sur 15 années de travaux, sur les perspectives et les défis qui l'attendent ainsi que débattre de certaines questions d'actualités au cours d'une séance académique tenue au Parlement.

Loi relative aux communications électroniques

Dans le courant de l'année 2007, la Commission belge s'est penchée sur une proposition de modification de *la Loi du 13 juin 2005 relative aux communications électronique (Avis 18/2007 du 27 avril 2007)*, laquelle transpose en droit belge la directive 2002/58/CE (M.B., 20 juin 2005). Si cette proposition n'a, *in fine*, pas abouti, les amendements qu'elle suggérait sont intéressants à mentionner dès lorsqu'ils visaient à améliorer la protection de la vie privée dans le cadre de la fourniture de service de localisation par téléphone portable : d'une part en accordant aux utilisateurs de l'équipement les mêmes garanties de protection de leur vie privée qu'aux abonnés (information préalable obligatoire de l'utilisateur, information obligatoire d'activation du service directement sur le téléphone portable lors de chaque requête de localisation et droit d'annulation des services pour l'utilisateur final) et d'autre part en étendant ces protections aux enfants mineurs dès l'âge de 12 ans (obtention de leur consentement en sus de celui de leurs représentants légaux). La Loi du 13 juin 2005 n'a cependant donc pas été modifiée dans le sens décrit ci-dessus.

Loi réglant l'installation et l'utilisation de caméras de surveillance

Le rapport annuel précédent indiquait que la question de la vidéosurveillance avait été au cœur des préoccupations tant du législateur que de la Commission belges en 2006.

Au terme de longues discussions et d'une série d'auditions des acteurs concernés par la problématique – dont la Commission belge –, la *Loi réglant l'installation et l'utilisation de caméras de surveillance* a été votée le 1er mars 2007 (ci-après la Loi Caméras – M.B., 31 mai 2007). Cette législation sectorielle règlemente spécifiquement les traitements d'images à des fins de surveillance. Toutefois, sauf dérogations explicites, cette dernière demeure d'application. Les grandes lignes de cette nouvelle règlementation peuvent être résumées comme suit :

La Loi Caméras est applicable à tout système d'observation fixe ou mobile installé et utilisé à des fins de surveillance et de contrôle de certains lieux. L'installation et l'utilisation de caméras de surveillance réglées par des législations particulières (détectives privés, sécurité des matchs de football) de même que l'installation et l'utilisation de caméras destinées à garantir, sur le lieu de travail, la sécurité et la santé, la protection des biens de l'entreprise, le contrôle du processus de production et le contrôle du travail sont exclues de son champ d'application.

La Loi Caméras distingue trois types de lieux (lieux ouverts, lieux fermés accessibles au public et lieux fermés non accessibles au public), chacun d'entre eux obéissant à des règles distinctes tant au niveau de la procédure d'installation de la caméra de surveillance qu'au niveau de son utilisation.

[7] Ce document est disponible sous forme de CD-Rom auprès de la Commission. Il peut également être téléchargé sur son site Internet.

Seul le placement d'une caméra de surveillance dans un lieu ouvert est subordonné à l'obtention préalable d'un avis favorable des responsables politiques locaux et d'un avis favorable des services de la police locale attestant qu'une étude de sécurité et d'efficience a été menée et que l'installation envisagée est conforme aux principes de la règlementation en matière de protection des données. L'appréciation de la proportionnalité sera par ailleurs différente selon que la caméra est placée dans l'un ou l'autre lieu (images filmées, accès aux données, destinataires des données, conservation des données, nombre d'appareils). A titre d'exemple, les caméras doivent être placées sur la voie publique de manière à éviter que des lieux privés (tels entrées ou fenêtres de bâtiments privés) ne figurent dans leur champ. Toujours en ce qui concerne les lieux ouverts, le visionnage en temps réel n'est admis que sous le contrôle d'autorités administratives ou judiciaires dans le but de permettre aux services de police d'intervenir directement en cas d'infraction, de dommage ou d'atteinte à l'ordre public.

Afin de satisfaire à son obligation d'information, le responsable de traitement est tenu d'apposer un pictogramme signalant l'existence d'une surveillance par caméra. Toute utilisation cachée de caméras est interdite (Voy. *Avis 22/2007 du 13 juin 2007 relatif à l'avant-projet d'arrêté royal définissant la manière de signaler l'existence d'une surveillance par caméra, pris en exécution de la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance*).

Enfin, quel que soit le lieu dans lequel le responsable de traitement souhaite installer une caméra de surveillance, il doit notifier sa décision à la Commission belge au moyen d'un formulaire spécialement conçu à cet effet (déclaration thématique spécifique). Toute installation de caméras dans un lieu fermé doit par ailleurs être simultanément notifiée auprès des services de police locale.

Mise en place des comités sectoriels
Des comités sectoriels institués au sein de la Commission belge veillent à ce que les traitements de données à caractère personnel effectués dans divers secteurs spécifiques (sécurité sociale, autorités publiques etc.) ne portent pas atteinte à la vie privée. Certains d'entre eux disposent d'une compétence d'autorisation de certains traitements. La composition de ces comités inclut des membres de la Commission belge d'une part et des experts choisis pour leur connaissance pratique du secteur concerné d'autre part. L'année 2007 a vu plusieurs de ces comités entamer leurs travaux dans cette composition paritaire et les demandes d'autorisation à eux adressées se multiplier.

Communication de données de santé
Le rapport annuel 2006 indiquait également qu'un projet de loi portant création d'un comité sectoriel de la sécurité sociale *et de la santé devrait être adopté au début de l'année 2007. Aux termes de la Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* telle que modifiée le 1er mars 2007, le comité sectoriel jusqu'alors compétent en matière de sécurité sociale, a vu ses compétences étendues à certains traitements de données à caractère personnel relatives à la santé. La nouvelle section « santé » de ce comité est ainsi chargée d'autoriser la communication de données relatives à la santé pour autant que cette communication soit légalement requise. Elle est par ailleurs chargée de veiller au respect des dispositions fixées par ou en vertu de la loi visant à la protection de la vie privée à l'égard des traitements de ces mêmes données.

B. Jurisprudence

Aucune décision particulièrement importante rendue par les cours et tribunaux ne nous parait devoir ici être mentionnée.

C. Questions diverses importantes

Introduction générale
La tendance déjà constatée en 2005 et 2006 de centralisation et d'interconnexion de données s'est confirmée en 2007. Dans ses avis rendus au cours de cette année, la Commission belge a, comme lors des années précédentes, mis l'accent sur le nécessaire respect du principe de compatibilité entre les fichiers afin d'éviter les croisements systématiques de données ainsi que sur la nécessaire transparence de ces traitements à l'égard des citoyens et la préservation d'une certaine maîtrise informationnelle par tous. La multiplication des projets d'administration électronique (voy. la rubrique « secteur

public ») a, notamment, été l'occasion de réaffirmer ces principes.
Même si elles n'ont pas toutes abouti, certaines initiatives législatives méritent également d'être mentionnées dès lorsqu'elles visaient à offrir un cadre légal clair aux traitements de données particulièrement sensibles, telles celles appelées à figurer dans la base de données policière nationale, ou aux traitements de données auxquelles il est de plus en plus fréquemment fait appel telles les données fiscales. Ce fut également l'occasion pour la Commission belge de rappeler certains principes essentiels.

Comme en 2006, la Commission belge a poursuivi l'examen du respect de la législation en matière de protection des données par la société SWIFT. Ce même respect du par les entreprises dans le cadre de la mise en place de dispositifs d'alerte interne (whistleblowing) ou lors de transferts de données à caractère personnel à l'étranger (par exemple par la voie de l'adoption de règles d'entreprise contraignantes) a également retenu son attention.

Enfin, la Commission belge a développé certaines positions et recommandations au regard de nouvelles technologies telles que la télévision numérique et d'autres médias interactifs ainsi qu'à l'égard de la diffusion d'images en général et en milieu scolaire en particulier.

Ces différents aspects qui ont marqué l'activité de la Commission belge en 2007 sont détaillés ci-dessous.

Secteur de la police et de la sécurité
Banque nationale de données policières : aux termes d'un avis 12/2007 du 21 mars 2007, la Commission belge a accueilli favorablement l'initiative règlementaire tendant à déterminer les modalités selon lesquelles les services de police peuvent, dans le cadre des missions qui leur sont confiées, recueillir et traiter des données à caractère personnel et des informations. Elle a examiné ce projet à l'aune des exigences – de prévisibilité et de proportionnalité tout particulièrement – de la Convention européenne des droits de l'homme (CEDH) et de la jurisprudence de la Cour chargée de veiller à son application. La Commission a toutefois assorti son avis favorable de conditions, jugeant qu'en plusieurs points, il n'était répondu que de manière sommaire aux exigences de l'article 8 de la CEDH. Tout en se déclarant consciente de la difficulté pratique de structurer et de catégoriser l'ensemble des renseignements et informations bruts recueillis ou communiqués aux services de police, elle a notamment jugé nécessaire de circonscrire le plus précisément possible ces systèmes d'information afin que le citoyen soit en mesure de prévoir raisonnablement ce qui est susceptible d'y figurer et pour quels motifs.

Secteur public
Traitements de données par l'administration des finances : L'initiative tendant à réglementer certains traitements de données à caractère personnel réalisés tant au sein de l'administration des finances – par ses différents services – que dans le cadre des relations externes que cette administration entretient avec d'autres organisations publiques et privées a également retenu l'attention de la Commission belge. Les projets de texte soumis à son avis visaient, d'une part, à mettre la pratique actuelle de l'administration des finances en adéquation avec la Loi Vie privée et d'autre part, à encadrer légalement tant l'informatisation globale et intégrée de l'administration des finances que l'usage, dans le cadre de la lutte contre la fraude fiscale, d'outils automatisés d'aide à la prise de décision. Ainsi, étaient notamment prévus : 1) la création d'un registre de « dossier unique » pour chaque contribuable (personne physique et/ou morale) ; 2) la réalisation de traitements de données au moyen d'outil automatisé d'aide à la prise de décision (entrepôt de données – *datawarehouse*) pour l'identification des risques et groupes à risque d'objets et de sujets liés au non respect total ou partiel de la législation fiscale (datamining); ainsi que 3) des flux de données sortant et entrant au SPF Finances à destination ou en provenance d'autres autorités et professions.

Aux termes des avis qu'elle a rendus sur cette initiative, la Commission belge a notamment mis en exergue les éléments suivants *(Avis 01/2007 du 17 janvier 2007 et 16/2007 du 11 avril 2007 sur l'avant-projet de loi relatif à certains traitements de données à caractère personnel par le Service public fédéral finances) :*

- tout échange de données collectées pour des finalités différentes – fut ce au sein même de l'administration des finances – ne peut être présumé compatible mais doit, préalablement à sa réalisation, faire l'objet de

l'analyse de compatibilité prévue à l'article 4 de la Loi Vie privée. Cette disposition prévoit explicitement que des données ne peuvent être traitées ultérieurement de manière incompatible avec les finalités pour lesquelles elles ont été collectées à l'origine compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables des intéressés et des dispositions légales. Une procédure d'autorisation interne après examen d'un comité *ad hoc* ne peut s'y substituer.

- la Commission approuve la distinction opérée entre les tâches de gestion administrative et celles de contrôle, recouvrement et contentieux. Elle précise à cet égard que la description de ces finalités devrait se faire au départ d'un critère fonctionnel et non au départ d'un critère organique ;
- même si les données fiscales ne sont pas, en tant que telles, reprises sous la qualification de « données sensibles » *sensu stricto* aux termes de la législation belge, elles sont souvent – et à juste titre – considérées comme telles tant leur impact sur la vie privée de chacun est important ;
- la Commission est d'avis qu'une telle règlementation particulière doit – en principe – se conformer à la Loi Vie privée. Si pour des raisons spécifiques, des dérogations à la réglementation de base de la protection des données à caractère personnel devaient s'avérer nécessaires et justifiées, ces dérogations devraient figurer dans la Loi Vie privée elle-même ;
- si la Commission n'a pas d'objection à la création et à l'utilisation d'un identifiant sectoriel fiscal, elle s'interroge par contre sur l'utilisation de cet identifiant fiscal dans les relations externes de l'administration des finances et sur les risques qu'un tel numéro devienne *de facto* un second numéro d'identification universel. L'utilisation généralisée de cet identifiant fiscal ne pourra remplacer l'utilisation du numéro de registre national, encadrée en droit belge par un comité chargé de veiller, par son pouvoir d'autorisation, à son utilisation conforme à la Loi Vie privée ;
- la Commission n'est pas opposée à la mise en place d'un contrôle interne au sein d'une organisation ou d'un service public. Au contraire, elle accueille favorablement la création d'un comité interne chargé de veiller à la « conformité interne » de la protection des données, sans préjudice de sa compétence de contrôle externe et de celle de ses comités sectoriels ;
- en ce qui concerne la durée et les modalités de conservation des données, la Commission requiert une évaluation régulière de la nécessité de les conserver et des modalités de cette conservation. Elle préconise une évaluation obligatoire et régulière de la nécessité du maintien de ces données avant l'expiration du délai maximal, les données devant être directement supprimées dès qu'il est constaté qu'elles ne sont plus exactes, pertinentes ou nécessaires. La Commission a en outre suggéré qu'à la suite de chaque évaluation, une séparation soit clairement faite entre les données nécessaires aux activités courantes et celles qui, le cas échéant, seraient archivées ;
- enfin, la Commission accueille favorablement l'encadrement procédural spécifique de l'usage du *datawarehouse* et des techniques de datamining prévus par le projet de loi dès lors que cet encadrement offre des garanties permettant d'éviter que ces outils soient utilisés de manière opaque et disproportionnée : avant chaque décodage ou lors d'une insertion de données complémentaires dans le *datawarehouse*, un rapport, aux termes duquel une balance des intérêts et une analyse de nécessité doit être réalisée, sera soumis, pour avis, au comité de contrôle interne. Complémentairement à cet encadrement procédural, la Commission a recommandé qu'un service *adhoc* (tiers de confiance) en charge du décodage/codage des données soit mis en place. Ce projet de règlementation n'a toutefois pas abouti.

Décisions automatisées : Dans le cadre des avis rendus sur ce projet de règlementation comme dans d'autres, la Commission a également insisté sur le nécessaire respect de l'interdiction de prise de décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative sur le seul fondement d'un traitement automatisé de données. Qu'il s'agisse d'une décision visant à accorder un avantage automatique à la personne concernée – par exemple au terme de mesures de simplification administrative -, ou d'une décision qui s'inscrit dans une démarche de contrôle ou de lutte contre la fraude, la Commission se montre invariablement vigilante. Même autorisée par une loi, telle prise de décision doit être entourée de garanties appropriées visant à préserver une certaine maîtrise informationnelle par la personne concernée.

Dans le cadre de son appréciation du projet de règlementation spécifique des traitements de données par l'administration des finances commenté ci-dessus, la Commission conclut à cet égard que les traitements de données et les prises de décision – telle une décision d'entamer un contrôle fiscal à l'encontre d'une personne déterminée – ne pourront être exclusivement réalisés sur la base de l'information résultant du *datawarehouse*.

Aux termes d'un avis rendu relativement à un projet d'application automatique de prix maximaux pour la fourniture d'électricité et de gaz naturel aux clients à revenus modestes – basé sur un couplage de données des fournisseurs d'énergie et de données de sécurité sociale -, la Commission rappelle cette interdiction ainsi que le nécessaire respect du principe de proportionnalité et suggère la mise en place d'un système d'opting-out.

Couplage – organisation intermédiaire : Les demandes d'autorisation de transferts de flux de données adressées à la Commission belge et à ses comités sectoriels montrent également que dans un objectif de simplification administrative – mais également parfois dans une démarche de contrôle – différentes instances publiques souhaitent, de plus en plus souvent (comme dans l'exemple ci-dessus visant l'octroi automatique d'un tarif préférentiel), coupler les données d'un même citoyen. Les données relatives à la situation financière de la personne concernée sont, dans ce cadre, les données les plus fréquemment sollicitées par exemple pour l'attribution de tout droit ou avantage soumis à une condition de revenus. Ce recours accru au couplage a conduit la Commission belge à préconiser l'intervention d'une organisation intermédiaire (thrusted third party) présentant toutes les garanties d'indépendance requises pour permette une confiance légitime des personnes concernées *(Voy. l'avis 02/2007 du 17 janvier 2007 relatif au projet d'arrêté royal déterminant les règles suivants lesquelles certaines données hospitalières doivent être communiquées au ministre qui a la Santé publique dans ses attributions).*

Traitements ultérieurs à des fins statistiques et scientifiques : Le rôle d'une organisation intermédiaire dans le cadre de traitements ultérieurs de données à des fins historiques, statistiques et scientifiques a également été spécifié. À l'occasion de la demande d'accès par un chercheur aux données cadastrales disponibles au sein de l'administration des finances, la Commission a ainsi précisé quelles devaient être les garanties fournies par le monde académique lors de traitement de données à caractère personnel à des fins statistiques et scientifiques *(Avis 32/2007 du 7 novembre 2007 relatif à l'utilisation de données cadastrales à des fins de recherche statistique et scientifiques).* À cette occasion, elle a également rappelé sa jurisprudence – et celle des comités sectoriels établis en son sein -, relative à l'utilisation de l'identifiant national unique. Afin de mettre en balance les intérêts des chercheurs à collecter des données à caractère personnel à des fins de recherches scientifiques ou statistiques et ceux des citoyens à maîtriser l'usage qui est fait de leurs données, la Commission prône une méthode de travail aux termes de laquelle le responsable de traitement de la base de données dont est issu l'échantillon de personnes à interroger procède lui-même au premier contact avec les personnes concernées en vue de leur demander leur consentement à participer à l'enquête envisagée *[Avis 16/2006 du 14 juin 2006 relatif aux modalités de la communication de données du Registre national dans le cadre d'une recherche (scientifique)].*

Secteur privé

Swift : Les traitements de données à caractère personnel effectués par la société SWIFT, et en particulier leur transmission aux États-Unis et leur consultation par le Trésor américain (UST) dans le but avoué de la lutte contre le terrorisme, avaient, en 2006, fait l'objet de deux avis de la part de la Commission belge. La Commission y concluait à la violation de plusieurs dispositions– pénalement sanctionnées – de la Loi Vie privée par la société belge en sa qualité de responsable de traitement. Tout au long de l'année 2007, la Commission a suivi de près l'évolution de cette question et les mesures mises en œuvre par la société SWIFT pour rétablir une activité conforme à la réglementation belge. À cet effet, elle a initié une procédure de recommandation à l'égard de cette société. À l'heure de la rédaction de ce rapport, cette procédure est toujours en cours.

Règles d'entreprises contraignantes (Binding Corporate Rules – BCR) : la loi Vie privée confie au roi, après avis de la Commission belge, la compétence d'autoriser le transfert international de données vers un pays tiers non adéquat

sur la base de règles d'entreprises contraignantes offrant des garanties suffisantes en matière de protection des données. La société General Electric (GE) a choisi de recourir à cette forme d'encadrement pour ses flux transfrontières de données relatives à ses employés. Aux termes de ses règles, GE s'engage à avertir le Service public fédéral (Ministère de la) Justice et la Commission belge lorsqu'une obligation légale étrangère impose la communication de données, sauf lorsque cette autorité interdit spécifiquement cette information. Si la Commission accueille favorablement cette obligation d'information – par ailleurs préconisée par le Groupe 29 aux termes de son WP 128 relatif aux traitements de données opérés par SWIFT dont question ci-dessus -, elle est d'avis: 1) que l'exception dont elle est assortie devrait être limitée à l'interdiction émise par les seuls autorités chargées d'assurer le respect de la loi; 2) que cette interdiction devrait avoir une base légale; et 3) qu'elle devrait être limitée dans le temps. La Commission conditionne par ailleurs son avis positif à la suppression de l'exception au droit d'opposition fondée sur le consentement individuel de l'employé et à l'insertion de possibilité d'un audit par les autorités de protection des données. *(Avis n°13/2007 du 21 mars 2007 relatif au projet d'arrêté royal autorisant les transferts vers un pays non-membre de la communauté européenne et n'assurant pas un niveau de protection adéquat de données à caractère personnel d'employés de la société General Electric).*

Whistleblowing : le rapport 2006 indiquait, qu'à la suite de nombreuses questions et demandes d'information relatives à l'introduction de lignes étiques professionnelles au sein d'entreprises (whistleblowing), la Commission belge avait adopté une recommandation relative à la compatibilité des systèmes d'alerte professionnelle avec la loi vie privée. À l'appui de cette recommandation, la Commission belge a, en 2007, accueilli favorablement un système d'alerte professionnelle institué auprès de l'Ombudsman flamand autorisé à effectuer des enquêtes à propos de dénonciations d'irrégularités émanant de membres du personnel des services publics flamands.

Nouvelles technologies

Télévision numérique : aux termes d'un avis concernant la diffusion par voie numérique de services de télévision « traditionnels » à l'exclusion d'autres possibilités offertes par la télévision numérique (par exemple en matière d'interactivité), la Commission formule les constats suivants :

- le traitement automatisé, par les télédistributeurs, de données de télévision numérique doit être qualifié de « traitement de données à caractère personnel » ;
- quant à la légitimité du traitement, la Commission estime qu'à l'appui de la collecte de données personnelles, le télédistributeur de télévision numérique pourrait invoquer soit le consentement de la personne concernée, soit la nécessité de procéder à tel traitement, par exemple à des fins de facturation, en vue de l'exécution du contrat de distribution auquel l'intéressé aurait souscrit. La Commission exclut par contre toute prévalence de l'intérêt légitime du télédistributeur sur la protection de la vie privée du consommateur concerné (article 5 f) de la Loi Vie privée – article 7f) de la directive 95/46/CE) ;
- l'avis insiste tout particulièrement sur l'importance du principe de finalité et sur l'effectivité des droits de la personne concernée ;
- enfin, la Commission belge se déclare favorable à l'adoption d'un code de conduite spécifiquement destiné à ce secteur.

(Avis 06/2007 du 7 février 2007 relatif à la télévision numérique et à la protection de la vie privée).

Modes interactifs de consommation médiatique : dans un avis 29/2007 du 19 septembre 2007 consacré aux nouveaux modes de consommation médiatique en général, la Commission belge met en lumière les nouveaux risques pour la vie privée qu'induisent ces nouveaux modes de consommation médiatique, tout spécialement lorsqu'ils sont interactifs, en particulier la télévision interactive : profilage des utilisateurs, manipulation des utilisateurs, perte du droit à une consommation anonyme des médias et perte du droit à l'information, à la diversité culturelle et au pluralisme des médias. Quant au profilage, l'avis insiste sur le fait que la fourniture du service et le profilage constituent deux finalités distinctes. Un traitement (ultérieur) de données à des fins de profilage n'est donc permis que lorsque la personne y a indubitablement consenti. Il importera de vérifier si la liberté de ce consentement est respectée : un refus du profilage ne peut avoir pour conséquence l'exclusion du service

et plus généralement, l'impossibilité d'accéder à ces nouveaux modes de consommation médiatique.

Recommandation concernant la diffusion d'images
En général : face au constat de la multiplication de la diffusion d'images par et sur des supports toujours plus nombreux et variés, la Commission belge a pris l'initiative d'émettre une recommandation sur ce thème. Le lecteur intéressé y est renvoyé *(Recommandation d'initiative 02/2007 du 28 novembre 2007 relative à la diffusion d'images).*

En milieu scolaire : sur la base des principes dégagés, la Commission belge a rendu un avis sur la diffusion de photographies de mineurs en milieu scolaire. De telles diffusions se multiplient en effet, que ce soit par le postage de photos de classe sur le site Internet de l'école ou par la publication de photos individuelles. La Commission indique que les principes de la loi Vie privée trouvent à s'appliquer sans restriction à ces traitements de données à caractère personnel. Elle exclut en effet l'applicabilité des exceptions prévues pour les traitements de données à des fins de journalisme.

En principe, pour tel traitement de données à caractère personnel, le consentement des « personnes concernées » sera requis. S'agissant d'un mineur sans faculté de discernement, ce consentement sera sollicité auprès de ses représentants légaux. S'agissant d'un mineur capable de discernement, la Commission recommande d'associer le mineur en exigeant son consentement propre et celui de ses représentants légaux.

La Commission distingue également selon qu'il s'agit de photos ciblées ou non ciblées. Un consentement tacite pourrait être présumé lors de la prise d'une photo non ciblée destinée à rapporter un événement donné (photo de groupe lors d'une fête scolaire, publication dans un journal de l'école). Les personnes concernées n'en doivent pas moins être informées de la prise des photos mais aussi de leur finalité et du type de publication envisagée. L'utilisation de telles photos à des fins publicitaires pour l'école est exclue. De telles photos ne peuvent porter atteinte à l'honneur et à la bonne réputation. Aucune donnée à caractère personnel superflue ne doit par ailleurs accompagner la photographie. Cette précaution doit d'autant plus être observée lorsque des données sensibles sont révélées.

Pour les *photos ciblées* (portrait individuel par exemple), le consentement informé – notamment quant à l'exercice de ses droits d'information d'accès, de rectification et d'opposition – de la personne concernée est requis et ce, pour chaque type d'images prises et de mode de diffusion. En application du principe de proportionnalité, la Commission belge recommande encore que si l'objectif de la publication sur Internet est d'informer parents et élèves, la publication se fasse sur une partie du site dont l'accès leur est réservé, par exemple moyennant l'introduction d'un mot de passe.

Nouveau site Internet de la Commission belge de la protection de la vie privée
À l'occasion de la première Journée européenne de la protection des données, la Commission belge a lancé son nouveau site Internet, dont le contenu a été très largement enrichi par rapport à sa version antérieure. Ce site est conçu de manière à répondre tant aux attentes des citoyens désireux de s'informer qu'aux nécessités d'un public averti en matière de protection des données à caractère personnel. L'ensemble des avis, recommandations et autorisations auxquels la présente contribution renvoie y est disponible à l'adresse http://www.privacycommission.be

Bulgarie

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La pleine transposition, dans la législation bulgare, de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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 a été acquise par les amendements apportés en 2006 à la loi sur la protection des données à caractère personnel (LPDP, *Law on Personal Data Protection*).

La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques a été mise en œuvre par la loi sur les communications électroniques promulguée dans le Journal officiel numéro 41 de 2007.

En 2007, l'ordonnance n°1 de 2007 relative au niveau minimum de mesures techniques et organisationnelles et au type autorisé de protection des données à caractère personnel, publiée conformément à l'article 23, alinéa 5, de la LPDP, a été adoptée et promulguée dans le Journal officiel numéro 25 de 2007. Cette ordonnance détermine le niveau minimum de mesures techniques et organisationnelles pour le traitement des données à caractère personnel et le type autorisé de protection.

Conformément à l'art. 9, alinéa 2, de la LPDP, de nouveaux règlements concernant l'activité de la Commission pour la protection des données à caractère personnel (CPDP, *Commission for Personal Data Protection*) ont été promulgués dans le Journal officiel numéro 25 de 2007. Ces règlements relatifs aux fonctions et aux activités de la CPDP et aux questions y afférentes visent à assurer la mise en œuvre stricte de la LPDP et à établir des règles claires tant pour les responsables du traitement des données à caractère personnel que pour les personnes concernées par ces données.

B. Jurisprudence

En 2007, les cas typiques de violation de la directive 95/46/CE ainsi que de la LPDP concernaient le traitement illégal de données à caractère personnel de personnes physiques sans le consentement de celles-ci et sans que les responsables du traitement des données n'aient notifié au préalable les catégories de données à caractère personnel traitées, les buts poursuivis, les destinataires de ces données et le droit des personnes à accéder à leurs données à caractère personnel.

La CPDP a traité des plaintes portant sur le traitement de données à caractère personnel dépassant les buts légaux spécifiques, clairement définis, ainsi que sur un retraitement non conforme à ces buts. Ces cas révèlent une conservation illégale de données en vue d'une utilisation à d'autres fins, notamment pour le marketing direct. L'expérience de la CPDP permet de conclure que les individus sont particulièrement sensibles à la divulgation de certaines catégories de leurs données à caractère personnel, surtout celles liées à leur santé, mais ce ne sont pas là des cas spécifiques à 2007.

L'année 2007 a été marquée par une diminution considérable du nombre de plaintes pour traitement de données à caractère personnel à des fins de marketing direct ou de vidéosurveillance à l'insu des personnes concernées et sans leur consentement.

En ce qui concerne la diffusion de données à caractère personnel sur l'Internet, le travail de la CPDP montre que, dans la plupart des cas, les données à caractère personnel ont été recueillies par le biais d'inscriptions sur des sites Internet et que les personnes ont donné ces données de leur plein gré.

En 2007, la CPDP a émis des avis sur des questions liées au traitement légal de données à caractère personnel par des responsables du traitement de ces données. Des demandes d'avis ont été formulées tant par des responsables du traitement de données à caractère personnel que par des particuliers au sujet de leurs droits découlant de la LPDP. Des avis ont été rendus sur le traitement légal des numéros d'identification personnelle (codes PIN), sur le traitement des données personnelles à des fins statistiques, sur les conditions

préalables au traitement légal des données à caractère personnel des clients d'entreprises fournissant des services publics ainsi que sur la photocopie de cartes d'identité de clients par les banques.

À la suite des amendements apportés à la LPDP en 2006 et à l'adoption du nouvel art. 36a de la LPDP, la CPDP a pris des décisions concernant le transfert de données à caractère personnel tant aux pays de l'Union européenne qu'à des pays tiers. Elle a tranché dans des cas où des responsables du traitement de données à caractère personnel transfèrent des données à caractère personnel à d'autres responsables du traitement de données situés sur le territoire de pays tiers, en dehors de l'Union européenne et de l'Espace économique européen, et ce, après avoir évalué la suffisance du niveau de protection des données à caractère personnel offert dans le pays tiers concerné. Elle a réalisé cette évaluation sur la base de critères tels que la nature des données fournies, la durée du traitement des données, l'objectif de la fourniture de données à caractère personnel, la notification aux particuliers concernés par ce transfert de données des buts de cette fourniture de données et des destinataires des données dans le pays tiers, le droit d'accès de la personne et la possibilité de rectifier ou supprimer des données lorsque le traitement n'est pas conforme à la LPDP, la protection des données offerte dans le pays tiers concerné et les mesures garantissant la possibilité d'indemnisation lorsque des individus encourent des dommages à la suite d'un traitement illégal de données. En 2007, les demandes adressées par des responsables du traitement de données à caractère personnel à la CPDP conformément à l'art. 36a de la LPDP ont porté sur la fourniture de données à caractère personnel d'employés sous contrat de travail aux responsables du traitement de données de sociétés unipersonnelles sises dans des pays tiers, en application de l'art. 1, point 14, des dispositions complémentaires de la LPDP. Des demandes ont également été introduites par des responsables du traitement de données chargés notamment de sélectionner des membres du personnel et d'embaucher des marins appelés à naviguer sous un pavillon étranger.

C. Questions diverses importantes

Janvier 2007 a vu débuter la mise en œuvre d'un projet de jumelage BG/2005/IB/OT/02 dans le cadre du programme PHARE BG2005/017-586.03.01: Poursuite du renforcement de la capacité administrative de la Commission bulgare pour la protection des données à caractère personnel et stipulation des conditions de mise en œuvre de la loi sur la protection des données à caractère personnel.

Ce projet de jumelage a été divisé en cinq parties : 1) analyse du cadre législatif ; 2) développement des institutions ; 3) système informatique de la CPDP ; 4) traitement des plaintes et inspections ; 5) stratégies et méthodes de sensibilisation du public aux activités de la CPDP.

Ce projet compte 42 activités, dont son objectif principal, à savoir le développement institutionnel et l'investissement y afférent dans la CPDP bulgare afin d'améliorer l'efficacité et la qualité de ses activités visant la protection des données à caractère personnel dans le pays, via l'adoption et la mise en œuvre des meilleures pratiques européennes destinées à prévenir les violations des règles de protection des données à caractère personnel et à assurer la meilleure protection possible de ces données.

Ces activités couvrent différents domaines de la protection des données à caractère personnel : les télécommunications, le ministère de l'Intérieur, la justice, la santé, les assurances, le marketing direct, les banques, la vidéosurveillance, l'administration en ligne, etc.

La mise en œuvre des activités prévues dans ce projet de jumelage a été réalisée en février 2008.

Le programme PHARE BG2005/017-586.03.01 prévoit l'exécution d'un contrat de livraison. Ce contrat devrait être signé d'ici la fin de février.

Chaque mois, des rapports de suivi sur le projet sont rédigés afin d'assurer des garanties et un contrôle efficace.

En 2007, un système informatique en ligne pour l'enregistrement des responsables du traitement de données

à caractère personnel a été créé afin d'offrir les opportunités suivantes :

1. Compléter le formulaire de demande sur une page spécifique du site Internet de la CPDP – www.cpdp.bg
2. Confirmer les données complétées avec et sans utilisation d'une signature électronique.
3. Inscription des responsables du traitement de données à caractère personnel (PDC, *personal data controllers*) approuvés dans le registre de la CPDP intitulé « Registre des PDC et des registres tenus par eux », avec un code d'identification unique.
4. Ce registre est public, et on y accède via le site Internet de la CPDP – www.cpdp.bg
5. Les PDC inscrits reçoivent sur leur adresse électronique une confirmation officielle de leur inscription dans le système ainsi que le nom d'utilisateur et le mot de passe leur permettant d'accéder à leur propre profil et d'effectuer des mises à jour en fonction des changements survenus dans la situation déclarée.
6. Accessibilité des données de ce registre public tant pour les PDC inscrits que pour toutes les parties intéressées, qui peuvent être informées à tout moment des nouvelles activités et du nouveau statut des organisations.

À présent, le système en est à sa dernière phase d'essais et fonctionne sur le réseau local de la CPDP. Il devrait être accessible à tous les PDC via le site Internet de la CPDP dans les premiers mois de 2008 – www.cpdp.bg

République de Chypre

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

Directives 95/46/CE et 2002/58/CE :
Aucun fait nouveau à signaler.

Le 31 décembre 2007, une loi intitulée « La conservation des données de télécommunications pour utilisation à des fins d'enquête sur des infractions pénales graves » a été publiée dans le Journal officiel de la République.

Cette loi transpose les dispositions de la directive 2006/24/CE du 15 mars 2006 relative à la conservation de données générées.

La durée de conservation des données a été fixée à six mois.

Les infractions pénales graves y sont définies comme des infractions qualifiées d'actes délictueux graves dans le Code pénal ou dans toute autre loi ou passibles d'une peine maximale de cinq ans d'emprisonnement ou plus.

L'accès aux données de télécommunications conservées en application de la loi est autorisé uniquement sur présentation d'une ordonnance délivrée par un président d'un tribunal de première instance ou par le doyen des juges d'un tribunal de première instance après qu'une demande d'accès a été introduite par un enquêteur de la police avec l'approbation du Procureur général.

La loi interdit expressément la conservation ou la divulgation du contenu de la communication.

Les données de télécommunications qui ont été transmises à l'autorité compétente en vertu d'une ordonnance d'un tribunal doivent être détruites dans une période de dix jours à compter de la date à laquelle le Procureur général de la République considère qu'elles ne sont pas liées à une infraction pénale grave.

Dans les autres cas, les données devront être détruites conformément à une politique prescrite par le Chef de la police et approuvée par l'autorité de surveillance.
Le Commissaire à la protection des données à caractère personnel a été désigné comme l'autorité de surveillance aux fins de superviser la mise en application de la loi.

L'autorité de surveillance est habilitée à mener des audits, à examiner des plaintes et à soumettre des affaires au Procureur général de la République lorsqu'une violation de la loi peut constituer une infraction pénale.

Conformément à une déclaration faite par la République de Chypre, les dispositions de la loi relative à la conservation des données de communications liées à l'accès à l'Internet, à la téléphonie par l'Internet et au courrier électronique par l'Internet entreront en vigueur le 15 mars 2009.

B. Jurisprudence

En mars 2007, un article d'un quotidien dénonçant la situation à l'ancien hôpital général de Nicosie (après son déménagement dans un nouveau bâtiment) a incité le Commissaire à mener une enquête.

Celle-ci a révélé que des documents contenant des données personnelles de patients avaient été laissés dans certaines parties de l'ancien hôpital et que, malgré la présence d'agents de sécurité à l'entrée de l'hôpital, l'accès au site était libre ; n'importe qui pouvait accéder aux bâtiments et à tout document s'y trouvant, y compris des personnes qui effectuaient des réparations dans l'hôpital.

Des explications ont été données par des représentants du ministère de la Santé, responsable du déménagement de l'hôpital, concernant les mesures de sécurité et les données laissées sur l'ancien site.

Ensuite, des mesures ont été prises pour prévenir tout accès non autorisé au site et les documents qui s'y trouvaient ont été transportés en lieu sûr et/ou détruits.

Compte tenu de toutes les circonstances de cette affaire et du fait qu'il avait été donné suite aux

injonctions du Commissaire, une amende de 1500 livres chypriotes a été infligée au directeur général du ministère.

Une affaire de pourriel impliquant l'envoi sur des téléphones portables de communications non sollicitées concernant des résultats de courses de chevaux a fait l'objet d'une enquête, après le dépôt de plusieurs plaintes auprès du Commissaire. Les messages étaient envoyés (par plusieurs numéros) au moyen de cartes de téléphone prépayées. L'expéditeur de ces messages n'a jamais répondu à nos lettres ni à nos questions, de sorte qu'après avoir suivi la procédure prescrite, le Commissaire a rendu une décision imposant une amende de 2000 livres chypriotes.

C. Questions diverses importantes

Un audit a été mené au service du cadastre afin de vérifier comment diverses opérations de traitement y étaient réalisées.

Basé sur un questionnaire, cet audit a révélé que :

- les informations données aux personnes concernées au sujet du traitement de leurs données n'étaient pas suffisantes ou pas satisfaisantes ;
- ce service recueillait des renseignements auprès de tiers et n'en informait pas les personnes concernées ;
- les données relatives aux propriétaires de biens immobiliers étaient données aux autorités municipales et autres autorités locales aux fins du calcul de l'impôt foncier sans que les propriétaires n'en soient informés ;
- certains documents utilisés par le service recueillaient des renseignements excessifs et non utiles ;
- le personnel du service participant au traitement de données à caractère personnel n'avait pas reçu d'informations ou de formation sur la loi relative à la protection des données ni de lignes directrices écrites ou autres concernant ses devoirs et obligations.

Ces constatations de l'audit ont été communiquées au service, et nous suivons la prise de mesures destinées à satisfaire aux instructions données par le Commissaire.

Les employés d'une autorité locale s'étaient plaints au Commissaire d'être obligés de laisser prendre leurs empreintes digitales aux fins de vérifier leurs heures d'arrivée au travail et de départ.

Pendant l'examen de cette plainte, l'autorité locale concernée a déclaré avoir décidé de recourir à cette méthode en raison des abus constatés dans l'utilisation du système précédent basé sur le poinçonnage d'une carte (les employés détruisaient leur carte ou poinçonnaient les cartes d'autres employés). Elle trouvait que la méthode des empreintes digitales était plus efficace et ne permettait aucune tricherie. L'autorité a aussi montré au Commissaire le système utilisé pour la prise des empreintes digitales. Tenant compte de tous les arguments et informations qui lui ont été exposés, le Commissaire a estimé que, dans ces circonstances, la prise des empreintes digitales pour vérifier la présence des employés n'était pas légale et a demandé à l'autorité de mettre fin à cette pratique et de détruire toutes les empreintes digitales déjà collectées.

Comme d'autres plaintes et questions avaient été soumises au Commissaire au sujet de la collecte et de l'utilisation des empreintes digitales d'employés pour vérifier leur présence au travail, le Commissaire a publié des orientations à ce sujet (orientations publiées sur notre site Internet) et a souligné que la collecte d'empreintes à cette fin est, à première vue, contraire à la loi et ne devrait être utilisée que dans des cas vraiment exceptionnels ou particuliers.

République tchèque

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La législation de base en matière de protection de données à caractère personnel se compose de la loi N° 101/2000 Coll. sur la protection des données à caractère personnel et des amendements à plusieurs lois connexes, qui sont entrés en vigueur le 1er juin 2000. L'Office pour la protection des données à caractère personnel (OPDP) a été créé sur la base des dispositions de cette loi. Indépendant de par ses statuts, il est doté de pouvoirs importants : il peut notamment prendre des mesures et imposer directement des amendes en cas de violation de la loi. Cette loi transpose essentiellement la directive 95/46/CE en droit tchèque. La loi N° 101/2000 Coll. a été amendée par la loi N° 439/2004 Coll., avec prise d'effet au 26 juillet 2004, et a ainsi été alignée sur la directive précitée.

La directive 2002/58/CE a été partiellement transposée en 2004 par la loi N° 480/2004 Coll. sur certains services de la société de l'information, qui comporte des dispositions spécifiques sur les communications non sollicitées et donne à l'OPDP une nouvelle compétence forte dans le cadre de la lutte contre le « pourriel commercial ». Le reste de cette directive a ensuite été mis en œuvre en 2005 par la loi N° 127/2005 Coll. sur les communications électroniques, qui transpose simultanément plusieurs autres directives faisant partie du « paquet télécommunications ».

En 2007, deux nouveaux textes législatifs de base ont été adoptés en matière de protection des données :

- un léger amendement a été apporté à la loi N° 101 sur la protection des données en raison de l'entrée de la République tchèque dans l'espace Schengen (loi N° 101 amendée par la loi N° 170/2007 Coll.) ;
- une procédure d'amendement a été ouverte pour la loi N° 127 sur les communications électroniques en raison de la nécessité de transposer en droit national la directive 2006/24/CE sur la conservation de données ; cette procédure n'est pas encore terminée.

B. Jurisprudence

Conformément aux règles législatives du gouvernement de la République tchèque, l'OPDP est le point de contact obligatoire auquel les projets de lois et autres règlements applicables sont soumis pour avis dans le cadre des procédures interministérielles avant d'être soumis au Parlement. En 2007, l'OPDP a rendu des avis sur plusieurs règlements.

La transposition de la directive sur la conservation de données exigera, hormis l'amendement de la loi sur les communications électroniques (voir ci-dessus), la modification de certaines autres lois, principalement la loi N° 283/1991 Coll. sur la police. Celle-ci fait d'ailleurs déjà l'objet d'une procédure d'amendement pour d'autres motifs. L'OPDP a émis de vives critiques sur ce projet, et la procédure n'est pas encore terminée.

La longue préparation de l'entrée de la République tchèque dans l'espace Schengen a culminé en 2007. Le 1er septembre 2007, le Système d'information Schengen a été mis en service aux fins d'essais. À la fin du mois de septembre 2007, la mission d'évaluation d'experts s'est clôturée sur des conclusions favorables. Dans le cadre des activités préparatoires, plusieurs lois ont dû être amendées, principalement :

- la loi N° 283/1991 Coll. (telle qu'amendée) sur la police de la République tchèque ;
- la loi N° 141/1961 Coll. (telle qu'amendée) sur les procédures pénales (code de procédure pénale) ;
- la loi N° 326/1999 Coll. (telle qu'amendée) sur le séjour d'étrangers sur le territoire de la République tchèque ;
- la loi N° 325/1999 Coll. (telle qu'amendée) sur le droit d'asile ;
- la loi N° 361/2000 Coll. (telle qu'amendée) sur le trafic sur le réseau routier ;
- la loi N° 56/2001 Coll. (telle qu'amendée) sur les conditions de circulation des véhicules sur le réseau routier.

La position de l'OPDP en tant qu'organe indépendant de surveillance pour le Système d'information Schengen a été définitivement confirmée. Enfin, la décision 2007/801/CE du Conseil du 6 décembre 2007 a confirmé la pleine application des dispositions de

l'acquis de Schengen dans neuf pays, dont la République tchèque.

C. Questions diverses importantes

En matière d'***activités de contrôle***, l'OPDP a réalisé un total de 112 inspections en 2007. La plupart des inspections effectuées par des inspecteurs indépendants et leur équipe de contrôle ont été organisées ponctuellement sur la base de requêtes ou de plaintes d'individus. Seuls 15 % environ des inspections reposent sur le Plan d'activités de contrôle mais ce type de contrôle est en général de nature beaucoup plus complexe, couvrant un plus large éventail de caractéristiques et d'aspects du traitement de données.

Le Plan d'activités de contrôle pour 2007 était centré sur 5 grands thèmes:

1) les systèmes informatiques de l'administration publique, avec un accent spécial sur le traitement de données liées à des renseignements sur le patrimoine immobilier de personnes physiques (par ex. le cadastre) ;
2) le traitement de données à caractère personnel dans le cadre de systèmes de surveillance (vidéosurveillance), avec un accent particulier sur les systèmes employés dans les secteurs de l'éducation, de la santé et des municipalités ;
3) l'état de préparation de la République tchèque à l'entrée dans l'espace Schengen, principalement à titre de suivi des conclusions de la mission d'évaluation d'experts de 2006 ;
4) les systèmes de transport – une attention particulière a été accordée au suivi des mouvements de voitures dans le secteur du transport routier, par ex. en relation avec la perception d'un péage ;
5) le traitement de données à caractère personnel dans l'administration judiciaire et les organes du ministère public.

Les activités de contrôle précitées n'incluent pas celles qui concernent les ***communications commerciales non sollicitées*** (« pourriel commercial »). En 2007, l'OPDP a reçu 1569 plaintes et autres requêtes liées à ce domaine spécifique. Les actions de contrôle y afférentes ont visé 515 entités, dont 466 ont été sommées de prendre des mesures et 71 se sont vu imposer des sanctions. Comme l'année précédente, les problèmes les plus fréquents peuvent être résumés comme suit :

- Bon nombre des entités contrôlées ont invoqué un consentement donné par téléphone et quasi aucune ne respectait systématiquement le principe d'option de participation alors que la loi l'exige.
- Presque personne n'a déclaré la communication comme une communication commerciale. Les messages ont toutes sortes de désignations (bulletin d'information, info, nouvelles, etc). Or, la loi sur certains services de la société de l'information stipule qu'une communication commerciale doit être désignée « clairement et pleinement » comme telle.
- Certains fournisseurs de services Internet contribuent à opacifier l'interprétation de la législation en n'envoyant pas les communications commerciales eux-mêmes mais en ajoutant des notes publicitaires à la fin des messages qu'ils transmettent, sous la forme de brefs messages publicitaires placés à la fin d'un courriel.
- Chez certains fournisseurs de services électroniques, pour octroyer son consentement, il suffit de cocher une case dans le formulaire d'inscription dans la section de la demande de services qui s'y rapporte. Ces fournisseurs omettent de tenir compte du fait qu'un tel formulaire peut être complété par n'importe qui (et donc pour quiconque) s'il n'est pas protégé par un nom et un mot de passe d'accès.
- Pour que les communications commerciales respectent pleinement les dispositions de la loi, elles doivent être dûment accompagnées d'une adresse valable, à laquelle le destinataire peut signaler de façon directe et efficace qu'il ne souhaite pas que l'expéditeur continue à envoyer des informations commerciales. Toutefois, si l'expéditeur a organisé sa base de données de clients sur la base des adresses électroniques, un problème se pose si l'adresse expéditrice du client diffère de l'adresse enregistrée.

Outre ses activités générales de surveillance, l'OPDP a consacré beaucoup d'énergie aux activités de communication. Un *programme didactique* spécifique, comprenant un cours de quatre heures destiné aux enseignants du secondaire et centré sur la protection de la vie privée et des données à caractère personnel dans le contexte des droits fondamentaux de l'homme, a été mis au point par l'OPDP et le ministère de l'Éducation, de la Jeunesse et des Sports. De plus, un *film amusant*

comptant treize épisodes sur des questions de protection des données a été produit en coopération avec la Télévision tchèque et diffusé aux heures de grande écoute pendant quatre mois.

Enfin et surtout, un *concours ciblant les jeunes* et intitulé « C'est ma vie privée ! Interdit d'y regarder, d'y fouiller » a été lancé lors de la Journée de la protection des données et a été évalué en avril 2007. Des jeunes de deux catégories d'âges ont été encouragés à exprimer par écrit ou sous forme graphique ce qu'ils entendent par la protection de la vie privée et la protection des données à caractère personnel. Les prix ont été décernés aux gagnants lors du Festival international du film pour enfants et adolescents dans la ville de Zlin, le 1er juin 2007, jour du septième anniversaire de la création de l'OPDP.

Le 11 décembre 2007, l'Agence pour la protection des données de la Communauté autonome de Madrid a octroyé à l'OPDP le Prix européen pour les meilleures pratiques en matière de protection des données dans les services publics européens.

Danemark

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La loi danoise sur le traitement des données à caractère personnel, loi N° 429 du 31 mai 2000, est entrée en vigueur le 1er juillet 2000. La traduction anglaise de cette loi peut être consultée à l'adresse suivante : http ://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/

Cette loi transpose la 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.

La directive 2002/58/CE a été transposée en droit national danois par les textes suivants :

- la Constitution danoise
- la loi sur les pratiques de marketing, section 6 (cf. loi N° 1389 du 21 décembre 2005)
- la loi N° 429 du 31 mai 2000 sur le traitement des données à caractère personnel
- la loi sur les conditions de concurrence et les intérêts des consommateurs sur le marché des télécommunications (cf. décret N° 780 du 28 juin 2007)
- le décret N° 1031 du 13 octobre 2006 sur la fourniture de réseaux et services de communications électroniques
- le chapitre 71 de la loi sur l'administration de la justice (cf. décret N° 1261 du 23 octobre 2007)
- la section 263 du Code pénal (cf. décret N° 1260 du 23 octobre 2007)

La section 57 de la loi sur le traitement des données à caractère personnel exige que l'avis de l'Agence danoise pour la protection des données à caractère personnel (DPA, *Data Protection Agency*) soit demandé lors de la rédaction de décrets, de circulaires ou de règlements généraux similaires revêtant une importance pour la protection de la vie privée en relation avec le traitement de données. Cette disposition concerne aussi les propositions de lois. La DPA a rendu son avis sur plusieurs lois et règlements ayant une incidence sur la vie privée et la protection des données.

En 2007, le ministère de la Justice a déposé un projet de loi relatif à la sécurité lors de certains événements sportifs (registre des hooligans).

En vertu de ce projet de loi, la police pourrait restreindre la liberté de mouvement d'une personne qui aurait été accusée d'un délit commis en relation avec un événement sportif s'il y avait des raisons de croire que, sans cette restriction de mouvement, cette personne commettrait d'autres délits dans la zone géographique couverte par la mesure de restriction de mouvement.

Une personne faisant l'objet d'une mesure de restriction de sa liberté de mouvement serait interdite d'accès à certains événements sportifs et ne pourrait circuler dans un rayon de 500 mètres de ces événements sportifs pendant une période allant de 6 heures avant l'événement jusqu'à 6 heures après. Ce projet limiterait la mesure de restriction de la liberté de mouvement à un maximum de 2 ans.

D'après ce projet de loi, la police devrait transférer les données à caractère personnel relatives aux personnes faisant l'objet d'une mesure de restriction de mouvement aux clubs sportifs afin de permettre à ceux-ci d'appliquer la mesure de restriction. Parmi les données à caractère personnel transférées aux clubs sportifs figureraient les noms et photos.

La DPA a estimé que ce projet de loi soulevait des doutes quant à la protection de la vie privée des personnes concernées. Elle doutait que le traitement de données sensibles qui est proposé réponde aux buts décrits dans le projet de loi.

Elle a souligné que ce projet permettrait un traitement de données sensibles concernant les personnes concernées même si celles-ci n'étaient accusées que d'un délit.

De plus, elle a estimé que le projet pourrait mener à la diffusion de données sensibles dans un cercle plus large, ce qui accroîtrait le risque de traitement de données non conforme à la loi sur le traitement des données à caractère personnel.

Bien que la dernière version en date de ce projet de loi tienne compte d'un bon nombre des inquiétudes formulées par la DPA, le projet n'a pas encore été adopté.

B. Jurisprudence

Il a été demandé à la DPA de rendre un avis concernant la demande d'ATP[8] (*Arbejdsmarkedets Tillægspension*) de transférer des données à caractère personnel à des pays tiers (cf. section 27 (4) de la loi sur le traitement des données à caractère personnel).

Il a été signalé à la DPA qu'à la fin de 2006, ATP comptait près de 4,5 millions de membres et environ 150 000 employeurs cotisants des secteurs privé et public.

Les données à caractère personnel traitées par ATP comprennent des renseignements couvrant le nom, l'adresse, d'autres informations de contact, le numéro national, l'employeur, l'emploi et la formation.

ATP souhaitait transférer les données concernant les membres et les employeurs cotisants à des sociétés de traitement de données en Inde et en Afrique du Sud, principalement pour garantir la continuité des opérations.

La DPA a informé ATP de la section 41 (4) de la loi sur le traitement des données à caractère personnel, qui stipule : « En ce qui concerne les données traitées pour l'administration publique qui revêtent un intérêt particulier pour des puissances étrangères, des mesures seront prises pour garantir qu'elles puissent être éliminées ou détruites en cas de guerre ou de circonstances similaires ».

Après avoir correspondu avec ATP, la DPA a conclu qu'en vertu de la section 41 (4), il était interdit à ATP de transférer des données à caractère personnel en Inde et en Afrique du Sud.

La DPA a souligné la nature et le volume (couvrant presque toute la population du Danemark) des données à caractère personnel traitées par ATP.

Elle a aussi souligné que, lors de l'adoption de la loi sur le traitement des données à caractère personnel, le législateur avait cité tant les données à caractère personnel du registre national que les données à caractère personnel sur la formation des citoyens comme renseignements couverts par la section 41 (4).

C. Questions diverses importantes

En 2005, le ministère de la justice a décidé de créer un groupe d'experts chargé d'évaluer la législation en vigueur sur la vidéosurveillance et de constituer une base de renseignements qui permette de tracer la limite entre le besoin de sécurité et de prévention de la criminalité et le droit des citoyens à la vie privée.

Cette décision découlait, entre autres, d'un récent avis de la DPA, qui mettait en exergue plusieurs facteurs suspects relatifs à la mise en œuvre conjointe de la loi sur la vidéosurveillance et de la loi sur le traitement des données à caractère personnel.

Sur la base des conclusions de ce groupe d'experts, auquel la DPA a donné un avis, une nouvelle loi a été adoptée par le Parlement danois le 1er juin 2007.

Voici les principales dispositions de cette loi :

- Elle autorise les institutions financières, casinos, hôtels, restaurants, centres commerciaux et magasins de détail à instaurer une vidéosurveillance de leurs propres entrées et de leurs façades. Les zones situées directement près de leurs entrées et façades, qui sont ou peuvent être naturellement utilisées pour accéder à leurs propres entrées ou pour fuir, ne peuvent faire l'objet d'une surveillance que si celle-ci est clairement nécessaire à des fins de prévention de la criminalité.
- Elle amende la loi sur la protection des données afin d'étendre son application à tout traitement de données à caractère personnel lié à la vidéosurveillance et d'y inclure des règles spécifiques concernant la conservation de données (30 jours sauf nécessité pour les besoins d'un cas spécifique) et la divulgation de données (autorisée uniquement moyennant le consentement explicite de la personne concernée, si la divulgation est régie par la loi ou si les données sont divulguées à la police à des fins d'enquête).

[8] Institution indépendante, créée en application de la loi N° 46 du 7 mars 1964, aux fins de payer des pensions complémentaires aux salariés, etc.

- Il n'est pas nécessaire de notifier à la DPA le traitement de données lié à la vidéosurveillance.
- Il incombe à la DPA d'inspecter le traitement de données de vidéosurveillance réalisé par des responsables privés.

Dans un avis rendu avant que le Parlement danois n'adopte cette nouvelle loi, la DPA avait approuvé l'idée de limiter l'autorisation d'instaurer une vidéosurveillance dans des zones définies à certains groupes d'entreprises et aux seuls cas où cette surveillance est manifestement nécessaire pour prévenir la criminalité.

La DPA a souligné que la législation proposée mènerait à un traitement accru de données à caractère personnel, qui concerneraient aussi de simples passants traversant les zones sous surveillance.

Eu égard à l'extension de l'accès à l'usage de la vidéosurveillance, la DPA a insisté sur la nécessité de garanties adéquates, telles que des règles régissant la conservation et la divulgation de données.

En ce qui concerne les enregistrements sonores liés à la vidéosurveillance, la DPA a demandé que cet aspect soit examiné dans le cadre de l'adoption de la nouvelle loi parce que la législation actuelle, contrairement à la loi sur la protection des données, ne couvre pas le traitement de données à caractère personnel liées à des enregistrements sonores.

La DPA s'est déclarée favorable à l'idée d'être prévenue de l'instauration d'une vidéosurveillance, en partie pour des motifs liés aux ressources mais aussi parce qu'il lui incomberait d'inspecter tous les responsables, publics ou privés, qui traitent des données à caractère personnel dans le cadre d'une vidéosurveillance.

Estonie

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

Les principaux faits nouveaux à signaler pour la période couverte par ce rapport sont l'achèvement des projets de loi sur la protection des données à caractère personnel (ci-après PDPA, *Personal Data Protection Act*) et sur l'information publique (ci-après PIA, *Public Information Act*), l'adoption d'amendements à ces lois et leur entrée en vigueur partielle. La mise en œuvre complète de ces deux textes législatifs importants aura lieu dans le courant de l'année prochaine.

Des modifications de la classification des données à caractère personnel et l'inclusion des données biométriques dans la catégorie des données sensibles constituent les points les plus significatifs de la PDPA. Adoptée le 15 février 2007 et devant entrer pleinement en vigueur en 2008, cette loi se distingue aussi par le renforcement de la protection du traitement des données à caractère personnel. Elle modifie en effet les réglementations régissant le traitement des données à caractère personnel fournies aux fins d'un usage public légal et celui des données à caractère personnel destinées à la recherche ou aux statistiques gouvernementales, et elle crée une institution officiellement responsable de la protection des données à caractère personnel.

Depuis le 1er janvier 2008, la catégorie des données personnelles privées n'existe plus. Les données personnelles sont subdivisées en « données personnelles sensibles » et « données personnelles ». La suppression de la catégorie des données personnelles privées invalide aussi l'obligation de notifier le traitement de ces données.

Depuis le 1er janvier 2008, les données biométriques, principalement les empreintes digitales, les empreintes de paumes et les photos d'iris, sont traitées comme données personnelles sensibles, et l'expression « données relatives aux informations génétiques » a été remplacée par « données génétiques ».

Un des changements prévus par la loi est le droit pour une personne de demander qu'il soit mis fin à la divulgation et à tout autre usage de données personnelles qui ont été légalement classées à usage public. Dès lors, une personne garde le contrôle de tout nouvel usage de ses données après leur divulgation, ce que ne permettait pas la version précédente.

Depuis le 1er janvier 2008, la PDPA régit la collecte de données à caractère personnel pour l'évaluation de la solvabilité. Jusqu'alors, la loi ne limitait pas spécifiquement la période durant laquelle de telles données pouvaient être collectées. À présent, en cas de défaut de paiement, les données relatives à l'insolvabilité d'une personne ne peuvent être traitées et communiquées à des tiers que dans les trois ans suivant la date à laquelle la personne a failli à ses obligations. En conséquence, les données du registre du crédit ne peuvent remonter à plus de trois ans. Les données plus anciennes devront être éliminées. Cet amendement vise principalement à garantir que chaque responsable du traitement de données s'assure de la base du traitement des données et veille à ce que les contrats, accords et autres documents ne soient pas contraires aux exigences légales. Les dispositions relatives au consentement des personnes concernées ont changé elles aussi.

À l'avenir, une personne peut empêcher le traitement de données lorsque la base légale de la divulgation et du traitement ne peut être vérifiée.

Les seuls cas dans lesquels une personne ne peut interdire une poursuite du traitement des données sont ceux où la première divulgation a eu lieu à des fins journalistiques (la loi prévoit de nouvelles dispositions à cet égard) ou sur la base d'une loi (par exemple, des bases de données accessibles uniquement aux autorités gouvernementales).

B. Jurisprudence

Affaire 1 : Divulgation de données à caractère personnel sur le site Internet de la municipalité de Tallinn
Un citoyen avait demandé à la DPA de lui expliquer sur quelle base légale le nom de son enfant avait été cité dans le registre des actes juridiques de la municipalité de Tallinn, accessible au grand public. Selon lui, des

données à caractère personnel avaient été divulguées alors que l'accès de tiers à ces renseignements aurait dû être restreint.

La DPA a contacté la municipalité de Tallinn à ce propos. Elle lui a exposé par écrit son avis sur la divulgation de données à caractère personnel dans les actes juridiques de la municipalité de Tallinn et, sur la base de la plainte d'un citoyen, a demandé que le nom de l'enfant de cette personne soit retiré du registre des actes juridiques publié sur le site Internet de la municipalité de Tallinn. À la date précisée, la municipalité de Tallinn n'avait pas retiré le nom de l'enfant du registre.

Conformément à la loi sur l'organisation des administrations locales, les actes législatifs des villes ou des municipalités rurales peuvent être divulgués et rendus accessibles au grand public dans le respect de la procédure définie par la loi et par les statuts des villes ou des municipalités rurales. Toutefois, conformément à cette même loi, les données dont la divulgation est interdite par la loi ne peuvent être divulguées.

Le paragraphe 1 de la PDPA stipule que cette loi vise à protéger les droits et libertés fondamentaux des personnes physiques dans le cadre du traitement de données à caractère personnel dans l'intérêt général. Dans le cadre du traitement de données à caractère personnel, les responsables et les personnes autorisées doivent suivre les principes de pertinence et de minimalité (§6 (3) de la PDPA) et d'inviolabilité de la vie privée.

Selon l'Inspection de la protection des données, si le nom d'une personne ne répond pas en lui-même à la définition d'une donnée personnelle privée, il peut en devenir une lorsqu'il est assorti de renseignements supplémentaires. Du point de vue de la protection des droits fondamentaux, il est extrêmement important de ne pas traiter les données à caractère personnel au-delà de ce qui est nécessaire pour des buts spécifiques, déterminés au préalable.

Conformément à la PIA, si l'octroi d'un accès à des informations peut entraîner la divulgation d'informations à diffusion restreinte, il faut s'assurer que seule soit accessible la partie des informations ou du document ne faisant pas l'objet de restrictions (§38 (2) de la PIA).

Nous avons expliqué à la municipalité que, s'inspirant de l'article 1, alinéa 1, et du considérant 10 du préambule de la directive européenne 95/46/CE sur la protection des données, la PDPA souligne, en précisant le but, la nécessité de protéger les droits et libertés fondamentaux des personnes, en particulier le droit à l'inviolabilité de la vie privée. Sans pour autant rendre absolu le droit à la protection des données à caractère personnel ni l'inviolabilité de la vie privée, ce texte souligne que, dans le cadre du traitement de données à caractère personnel, dans les cas limites, nous devrions toujours faire passer l'interprétation qui protège l'inviolabilité de la vie privée avant d'éventuels intérêts publics.

Un conflit entre la protection de la vie privée et la nécessité de divulguer des données surgit clairement lorsque des données sont divulguées sur l'Internet. L'effet combiné de la PIA et de la PDPA est d'interdire la divulgation de données personnelles privées et de données personnelles sensibles (sauf dans les cas prescrits par la loi). Des données non sensibles peuvent être divulguées uniquement après une évaluation minutieuse des intérêts divergents en jeu : si la divulgation risque d'enfreindre le principe de l'inviolabilité de la vie privée de la personne concernée, des données non sensibles ne peuvent être rendues accessibles au grand public. À cet égard, il est important de noter que ces limites sont valables uniquement pour une divulgation au grand public.

Sur la base de ces argumentations, l'Inspection de la protection des données a estimé que la municipalité de Tallinn avait violé les principes de minimalité et de pertinence, dans la mesure où la divulgation sur l'Internet n'était pas proportionnelle au but spécifié et enfreignait l'inviolabilité de la vie privée.

L'Inspection de la protection des données a délivré une injonction à la municipalité de Tallinn, sommant celle-ci de retirer le nom de l'enfant de ce citoyen du registre des actes juridiques publié sur le site Internet de la municipalité de Tallinn pour le 15 janvier 2007.

Affaire 2 : Registre du crédit
Un contrat de location-vente « Ego » a été passé entre le nommé H.R. et Hansapank. En vertu de ce contrat, H.R. pouvait bénéficier d'une ligne de crédit et s'engageait à rembourser ce crédit à Hansapank par mensualités, conformément aux termes du contrat. Toutefois, H.R. a failli à ses obligations contractuelles de remboursement.

Ensuite, Hansapank et H.R. ont passé un contrat de rééchelonnement de cette dette découlant du contrat de location-vente « Ego ». À plusieurs reprises, H.R. n'a pas remboursé le montant pour lequel il s'était engagé en vertu du contrat précité.

Sur la base de la section 88 (2) (4) de la loi sur les institutions de crédit, du contrat de location-vente « Ego » et du contrat de rééchelonnement, Hansapank a divulgué les dettes de H.R. sur le site Internet d'AS Krediitiinfo.

H.R. a payé sa dette envers Hansapank en 2006 et a demandé le retrait de ses données du registre du crédit.

Ensuite, H.R. a déposé plainte devant l'Inspection de la protection des données. Celle-ci a délivré une injonction à Hansapank : d'après la plainte déposée, H.R. n'avait pas autorisé la publication de ses données personnelles sur le site Internet d'AS Krediitiinfo. En effet, Hansapank n'avait pas précisé les objectifs du traitement des données dans le contrat ni, à la connaissance de l'Inspection de la protection des données, dans tout autre document lié à la personne concernée. Or, la divulgation des données par Hansapank sans le consentement de la personne concernée est considérée comme un traitement de données et, en cas de litige, la personne concernée est censée n'avoir pas donné son consentement au traitement des données à caractère personnel qui la concernent (section 12 (5) de la PDPA).

Cette injonction a contraint la banque à cesser de divulguer illégalement les données personnelles de H.R. Hansapank s'est pliée à cette injonction mais a communiqué ses objections à l'Inspection de la protection des données. Celle-ci ayant rejeté lesdites objections, Hansapank a introduit un recours devant le tribunal.

Le tribunal administratif de Tallinn a estimé dans sa décision du 17.4.2007 que, dans sa conclusion finale, l'injonction était justifiée quant au fond et légitime.

Le 14 mai 2007, Hansapank a interjeté appel devant la Cour d'appel de Tallinn.

C. Questions diverses importantes

Pour la première fois durant cette période, l'Inspection de la protection des données a défini, de sa propre initiative, les priorités des opérations de surveillance pour l'année. Sept sujets ont été retenus et traités en profondeur à cette occasion. Pour chacun d'eux, l'inspection a publié un avis ou un document d'orientation sur son site Internet, via les médias ou un canal accessible aux groupes d'intérêts. Cette initiative émane de l'organisation. Les sujets choisis sont ceux que les responsables de l'Inspection ont jugé les plus problématiques ou les plus difficiles à interpréter dans les domaines de la protection des données à caractère personnel et de l'information publique.

Pour chacun de ces sujets, une analyse et, si nécessaire, une surveillance ont été effectuées ; en fonction des résultats, l'Inspection a élaboré des orientations, qu'elle a publiées sur son site Internet.

Voici les priorités choisies pour cette période : la transmission de données à caractère personnel à des pays tiers ; les dangers ou opportunités des recherches sur l'Internet ; l'admissibilité de l'enregistrement des appels téléphoniques; la divulgation de données à caractère personnel dans les instruments juridiques des administrations locales ; le traitement de données à caractère personnel dans le cadre du projet « carte d'identité-ticket » ; l'enfant et ses droits dans le cadre du traitement de données à caractère personnel ; le regroupement de données à caractère personnel dans l'émission de cartes privatives.

Voici un bref aperçu de deux avis intéressants:

Le traitement des données à caractère personnel dans le cadre du projet « carte d'identité-ticket »
En vertu de la loi sur les documents d'identité, le document d'identité principal et le seul qui soit obligatoire en Estonie est la carte d'identité. Le document « Traitement

des données à caractère personnel dans le cadre du projet « carte d'identité-ticket », publié par l'Inspection de la protection des données, étudie l'usage de la carte d'identité comme preuve d'achat de service, à partir de l'exemple du système « carte d'identité-ticket » de Tallinn et en se concentrant principalement sur le traitement des données de tels systèmes.

Ce document d'orientation est principalement destiné aux organismes publics et privés qui souhaitent mettre sur pied des systèmes d'information utilisant la carte d'identité comme preuve du droit de recevoir un service ou un produit. L'Inspection de la protection des données a formulé sept suggestions sur la base des principes de protection des données à caractère personnel.

Elle a estimé que le système consistant à utiliser la carte d'identité pour acheter le droit d'utiliser les transports publics, en vigueur à Tallinn, est conforme aux principes de la PDPA. L'Inspection de la protection des données accueille favorablement des initiatives qui permettent d'élargir le champ d'application des cartes d'identité et qui, dans le même temps, tiennent compte du droit des citoyens de recevoir une protection pertinente de leurs données à caractère personnel sous tous points de vue.

Les enfants et leurs droits en matière de traitement des données à caractère personnel

L'Inspection de la protection des données a analysé le traitement des données personnelles des enfants dans plusieurs domaines de la vie de tous les jours. Les informations publiées reposent sur les principaux instruments juridiques internationaux relatifs aux droits de l'enfant, sur les normes nationales dans les domaines pertinents, sur les résultats de la surveillance effectuée et sur les modèles de comportement dans différents environnements concrets. La loi sur la protection de l'enfant définit l'enfant comme une personne de moins de 18 ans. Ce document présente une argumentation juridique sur le traitement des données à caractère personnel des enfants et sur le droit de l'enfant à l'inviolabilité de sa vie privée.

Un paragraphe distinct analyse les questions liées à l'utilisation des webcams dans les écoles. La technologie permet aux parents de surveiller leurs enfants 24 heures sur 24 et le besoin d'une vidéosurveillance repose sur des considérations de sécurité. Par ailleurs, l'enregistrement de tout type de données sur bande vidéo affecte les droits fondamentaux des personnes.

L'Inspection a recommandé dans ce document que la surveillance des actions des enfants, d'une part, soit proportionnelle au droit d'un enfant à la vie privée et, d'autre part, soit basée sur l'intérêt général en termes de sécurité et de prévention des actes criminels, etc.

En outre, le document publié analyse les domaines qui concernent la divulgation des notations et des données des enfants sur l'Internet et une plus grande attention a été accordée au sujet de l'exposition des enfants aux médias.

Bref, nous avons émis l'avis que la protection de la vie privée des enfants devrait reposer sur deux aspects : la responsabilité et la prise de conscience.

Finlande

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE

La directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données a été transposée en droit finlandais par la loi sur les données à caractère personnel (523/1999), entrée en vigueur le 1er juin 1999. Cette loi a été révisée le 1er décembre 2000 ; des dispositions y ont alors été ajoutées concernant le processus décisionnel de la Commission et la force exécutoire des décisions relatives au transfert de données à caractère personnel à des pays non membres de l'UE en application de la directive sur la protection des données.

La protection de la vie privée est un droit fondamental en Finlande depuis le 1er août 1995. En vertu de la Constitution finlandaise, la protection des données à caractère personnel est réglementée par une loi spécifique.

La loi sur la protection des données dans les communications électroniques (516/2004), entrée en vigueur le 1er septembre 2004, a transposé la directive sur la vie privée et les communications électroniques (2002/58/CE). Elle entend assurer la confidentialité et la protection de la vie privée dans les communications électroniques et promouvoir la sécurité des informations dans les communications électroniques et le développement équilibré d'une vaste gamme de services de communications électroniques.

La responsabilité de l'application de la loi a été divisée, de sorte que la mission du bureau du médiateur pour la protection des données couvre les réglementations relatives au traitement des données de localisation, les réglementations relatives au marketing direct, les réglementations sur les services de catalogage et les réglementations sur le droit spécifique des utilisateurs à obtenir des informations.

À cet égard, il convient de noter qu'en vertu du code pénal, le ministère public est tenu de consulter le médiateur pour la protection des données avant d'engager des poursuites judiciaires dans une affaire concernant une violation du secret des communications électroniques.

B. Jurisprudence

La Cour de justice des Communautés européennes se penche sur la publication de données sur les revenus du travail

Une entreprise finlandaise publiait chaque année les revenus du travail de plus d'un million de Finlandais et transmettait ces données à une autre société aux fins d'un service SMS. Ces informations étaient ensuite transmises au public contre paiement d'un service commercial SMS.

Le médiateur pour la protection des données a demandé au Conseil compétent pour la protection des données d'interdire la publication de ces informations sur les revenus du travail. Le Conseil pour la protection des données est habilité à interdire le traitement illégal de données à caractère personnel. Or, le Conseil pour la protection des données et le tribunal administratif saisi de l'affaire après le Conseil n'ont pas suivi l'avis du médiateur pour la protection des données et ont accepté l'interprétation selon laquelle il s'agissait d'un traitement de données personnelles à des fins journalistiques, auquel la loi sur la protection des données à caractère personnel ne s'applique en principe pas. L'affaire est pendante devant le tribunal administratif suprême. Le 8 février 2007, le tribunal administratif suprême a soumis une demande de décision préjudicielle à la Cour de justice des Communautés européennes, qui a prévu une audience sur cette affaire le 12 février 2008. Le tribunal administratif suprême basera sa décision sur l'arrêt rendu à titre préjudiciel.

Le tribunal administratif suprême ordonne à une banque d'appliquer le droit d'accès complet aux données

En février 2007, le tribunal administratif suprême a confirmé l'interprétation de la loi finlandaise donnée par le médiateur pour la protection des données, selon laquelle le droit d'accès s'étend aux données relatives aux transactions de prêt d'un client et aux taux d'intérêt qui y ont été appliqués.

La banque avait fait valoir que des extraits de compte et des données relatives aux taux d'intérêt ne faisaient pas partie des dossiers des clients car les microfilms contenant ces données étaient stockés séparément des dossiers des clients. Toutefois, d'après le médiateur pour la protection des données, ce point de vue est erroné parce que c'est l'utilisation du dossier des données personnelles qui en détermine l'étendue. En vertu de la loi sur la protection des données à caractère personnel, les données traitées en vue d'une même tâche appartiennent au même fichier de données à caractère personnel (fichier de données logiques), même si diverses parties de ce fichier de données (sous-fichiers) sont stockées séparément. Comme l'objectif de l'utilisation des données d'intérêt était, comme pour les autres données relatives à X, d'assurer la gestion des relations avec le client, toutes les données appartenaient au même fichier de données. Le critère d'un stockage techniquement couplé ou distinct a été considéré sans importance.

Authentification du client dans des sociétés de crédit rapide

La demande de crédits rapides sollicités par téléphone portable ou via l'Internet a fort augmenté en Finlande. On dénombrerait actuellement entre 50 et 60 sociétés de crédit rapide. En raison d'une authentification insuffisante des demandeurs de crédit rapide, plusieurs prêts ont été souscrits au nom d'une autre personne à l'insu de tous.

Beaucoup de sociétés de crédit rapide authentifient le demandeur sur la base uniquement du numéro de sécurité sociale que celui-ci communique et des données d'abonnement de la société de télécommunications. Si ces données correspondent, la société suppose que le demandeur est bien la personne qu'il affirme être. Des procédures insuffisantes d'authentification ont mené à des cas d'usurpation d'identité. L'authentification se complique par le fait que le législateur n'a pas imposé aux créanciers une obligation spécifique d'identifier le demandeur d'un crédit rapide.

En mars 2007, le médiateur pour la protection des données a demandé au Conseil compétent pour la protection des données d'ordonner à une société de crédit rapide de modifier son processus d'authentification des demandeurs de crédit. Il a demandé que les créanciers identifient leurs clients afin d'assurer l'exactitude de toutes les données à caractère personnel traitées. L'avis du Conseil pour la protection des données revêtira une importance encore plus générale car, d'après une enquête réalisée à la demande du médiateur pour la protection des données, presque toutes les entreprises actives dans ce secteur utilisent un système similaire basé sur une faible identification. Cette décision pourrait avoir des répercussions dans d'autres domaines aussi.

C. Questions diverses importantes

Loi relative aux renseignements sur le crédit

La nouvelle loi relative aux renseignements sur le crédit est entrée en vigueur le 1er novembre 2007. Elle rassemble des dispositions sur les renseignements sur le crédit concernant les consommateurs, les entreprises et le personnel des entreprises concernées. Elle comporte des dispositions sur les données à stocker dans les dossiers de référence sur le crédit et sur la durée du stockage de ces données. Cette nouvelle loi définit avec plus de précision les buts dans lesquels les renseignements sur le crédit relatifs aux consommateurs peuvent être divulgués et utilisés.

En vertu de cette nouvelle loi, le médiateur pour la protection des données supervise aussi le traitement des renseignements sur le crédit concernant les entreprises. Les fournisseurs de renseignements sur le crédit doivent être fiables et doivent appliquer des bonnes pratiques en matière de renseignement sur le crédit. Actuellement, les renseignements sur les défauts de paiement confirmés par les autorités et notifiés par les débiteurs ainsi que l'évaluation de la solvabilité des personnes physiques et des entreprises peuvent être stockés dans les dossiers de référence sur le crédit.

Les informations sur un défaut de paiement, quel qu'il soit, sont stockées dans les dossiers de référence sur le crédit pour une durée prédéterminée. La nouvelle loi précise davantage ces durées de stockage et, dans certains cas, les écourte. Alors que le remboursement d'une dette peut raccourcir le délai de stockage, celui-ci peut être allongé si la personne ou l'entreprise se rend à nouveau coupable d'un défaut de paiement.

La nouvelle loi permettra aussi à des entreprises de vérifier les renseignements sur le crédit les concernant et de corriger les erreurs. Précédemment, ces droits n'étaient accordés qu'aux personnes physiques. Les fournisseurs de renseignements sur le crédit doivent aussi donner des renseignements sur le crédit aux consommateurs contre une redevance raisonnable. Le but est que les consommateurs puissent mieux s'assurer de la solvabilité de la partie avec laquelle ils passent un contrat.

Loi sur le traitement électronique des données de sécurité sociale et de santé des patients

La loi sur le traitement électronique des données de sécurité sociale et de santé des patients est entrée en vigueur le 1er juillet 2007. L'Institut finlandais d'assurance sociale s'emploie à créer en Finlande une base de données électronique nationale des patients, qui sera graduellement mise en service entre 2008 et 2011. Elle est destinée à être utilisée par l'ensemble du secteur des soins de santé.

La base de données comprend des services de stockage, d'archivage et de transfert des documents et prescriptions des patients. Cette réforme vise à améliorer la coopération entre les diverses parties actives dans le domaine de la sécurité sociale et des soins de santé et à améliorer le transfert électronique de données d'une unité à l'autre si le patient y consent.

L'objectif principal est de promouvoir la sécurité du traitement des données de sécurité sociale et de santé des patients et de proposer aux patients des services de santé à la fois sûrs et efficaces. De plus, la nouvelle loi permet aux patients d'accéder à leurs propres données et aux données d'ouverture de session concernant leur utilisation, par exemple, leur affichage en ligne.

Tous les fournisseurs publics de soins de santé doivent commencer à utiliser les services de cette base de données. Les fournisseurs privés de soins sont tenus de rallier le système si la conservation à long terme de leurs données concernant les patients se fait électroniquement.

Loi sur les prescriptions électroniques

La nouvelle loi sur les prescriptions électroniques, entrée en vigueur le 1er avril 2007, détermine les conditions d'installation et de mise en œuvre d'un système de prescriptions électroniques. En vertu de cette loi, les prescriptions peuvent être établies électroniquement et transférées via des réseaux de données au centre national des prescriptions, qui donne au pharmacien les informations nécessaires pour fournir la prescription.

Les médecins doivent expliquer à leurs patients l'utilisation des prescriptions électroniques et leur donner des instructions écrites au sujet du médicament et de son utilisation. Le patient a le droit de refuser la prescription électronique, auquel cas il recevra une prescription papier. Comme toutes les prescriptions électroniques sont stockées au centre des prescriptions, les patients peuvent, à tout moment, vérifier la validité de leurs prescriptions et la quantité de médicaments non fournis, sans devoir conserver les prescriptions d'origine. Le centre des prescriptions et les archives des prescriptions seront tenus à jour par l'Institut finlandais d'assurance sociale. Les prescriptions seront conservées au centre pendant 30 mois, après quoi elles devront être transférées aux archives.

Si toutes les prescriptions d'un patient ont été établies électroniquement, un médecin, un dentiste ou un pharmacien peut vérifier l'ensemble des médicaments donnés au patient et les interactions potentielles entre ces médicaments sur la base des données fournies par le centre des prescriptions (avec le consentement du patient). Les patients ont également le droit de recevoir des informations sur les personnes qui ont traité ou consulté les données qui les concernent au centre des prescriptions ou dans les archives des prescriptions.

Recommandations du Groupe de travail sur les biobanques

Dans son rapport publié le 12 octobre 2007, un Groupe de travail désigné par le ministère des Affaires sociales et de la Santé estime que, vu l'extension des collectes actuelles et futures d'échantillons de tissus humains à des fins médicales, il faut instaurer un contrôle des activités, renforcer les communications, uniformiser les procédures et définir des critères de qualité.

Ce Groupe de travail a proposé la création de biobanques en Finlande (système décentralisé). La principale tâche d'une biobanque serait de recueillir, gérer et stocker les échantillons biologiques humains et les informations qui en sont tirées ou qui y ont trait aux fins de recherches futures. Une biobanque peut soit collecter les échantillons elle-même ou chercher ailleurs des échantillons à incorporer dans ses collections.

D'après la proposition du Groupe de travail, le transfert d'un échantillon dans la biobanque serait soumis à l'autorisation du donneur de l'échantillon. Le consentement serait basé sur la connaissance de l'objectif général de la biobanque. Les donneurs d'échantillons ont le droit de savoir quel usage en sera fait. La possibilité d'influencer leur utilisation est garantie par l'obligation générale d'information, par la transparence des activités et par le contrôle exercé par les autorités sur les opérations de la biobanque. Les échantillons de recherche et de diagnostic existants, pris à des fins de diagnostic et de traitement de maladies, peuvent être transférés à une biobanque soit avec le consentement du donneur des échantillons ou, si le renouvellement du consentement est trop difficile, avec l'autorisation de l'Autorité nationale en charge des affaires médico-légales.

Les données sur les biobanques sont recueillies dans un registre des biobanques qui, tout comme les registres des collections d'échantillons spécifiques aux biobanques, constitue un système de données répondant aux besoins d'accès aux informations des chercheurs et du grand public.

France

A. Mise en œuvre de la directive 95/46/CE et autres développements législatifs

1. Décret du 25 mars 2007

La France a transposé la directive européenne du 24 octobre 1995 par la loi du 6 août 2004 modifiant la loi du 6 janvier 1978. Le premier décret d'application de cette nouvelle loi a été adopté le 20 octobre 2005 et contenait notamment des dispositions relatives à la désignation de correspondants Informatique et Libertés au sein des entreprises et des administrations. Une modification de ce décret, adoptée le 25 mars 2007, est notamment venue apporter des précisions procédurales.

- Information des personnes en cas de transfert de leurs données hors de l'Union européenne.

Le décret du 25 mars 2007 prévoit que les personnes dont les données sont transférées hors de l'Union européenne doivent non seulement être informées de ce transfert, mais plus précisément du pays d'établissement du destinataire, de la finalité du transfert, des catégories de données personnelles faisant l'objet du transfert et du niveau de protection offert par le pays tiers situé en dehors de l'Union européenne. En outre, le décret prévoit que lorsque le transfert est envisagé postérieurement à la collecte des données personnelles, celui-ci ne peut intervenir que dans un délai de quinze jours suivant la réception par l'intéressé des informations précitées.

- Procédure de droit d'accès

Le décret d'application du 25 mars 2007 précise les modalités d'exercice du droit d'accès. La demande de droit d'accès peut être présentée par courrier ou sur place en justifiant par tous moyens son identité auprès du responsable de traitement. Lorsque la demande est effectuée sur place et ne peut être satisfaite immédiatement, un avis de réception daté et signé doit être délivré à la personne à l'origine de la demande. Le décret impose au responsable de traitement de répondre à la demande de l'intéressé dans les deux mois suivant sa réception. À l'issue du délai de deux mois, le défaut de réponse du responsable de traitement est considéré comme un refus.

2. Avis sur le projet de décret pris pour l'application de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique venant transposer en droit français la directive 2000/31/CE

L'article 6 de la loi pour la confiance dans l'économie numérique (LCEN) prévoit l'obligation de conservation des données permettant l'identification des personnes ayant contribué à la création de contenu en ligne.

Cet article impose aux fournisseurs d'hébergement et aux fournisseurs d'accès à internet de conserver les données de nature à permettre l'identification des personnes ayant contribué à la création de contenus en ligne (blogs, pages personnelles, annonces sur un site de vente aux enchères …) et ce, aux fins de communication éventuelle aux autorités judiciaires ainsi qu'aux services en charge de la lutte contre le terrorisme.

La CNIL a récemment examiné un projet de décret définissant les catégories de données concernées ainsi que leur durée de conservation. La publication de ce décret, accompagnée de l'avis de la CNIL, devrait prochainement intervenir.

B. Jurisprudence

1. Diversité

Après avoir publié, en juillet 2005, ses premières recommandations sur le sujet, la CNIL a approfondi sa réflexion en procédant à plus de soixante auditions : chercheurs, statisticiens, organisations syndicales, représentants des grandes religions, mouvements associatifs, personnalités qualifiées, chefs d'entreprise… Ces auditions ont montré une grande variété de points de vue, parfois des divergences, et la difficulté en ce domaine, d'aboutir à un consensus.

Néanmoins, un constat se dégage pour la CNIL : la France doit améliorer son appareil statistique et des réponses peuvent d'ores et déjà être apportées pour faire progresser la connaissance de notre société et, par là même, mieux lutter contre les discriminations.

À cet effet, la CNIL a rendu public au mois de mai 2007 ses dix recommandations qui ont été saluées pour leur pragmatisme, leur équilibre et leur juste audace. Les points forts de ces recommandations sont les suivants :

- Il est indispensable de permettre aux chercheurs d'accéder plus facilement aux fichiers de personnel, aux fichiers administratifs et aux bases statistiques publiques, bien entendu, dans le respect de la protection des données.
- Pour mesurer la réalité de la discrimination vécue, il faut aussi développer les enquêtes par questionnaires auprès des personnes concernées. Dès lors qu'elles sont facultatives, fondées sur l'auto déclaration, et que les réponses sont confidentielles, des questions doivent pouvoir être posées sur la nationalité et le lieu de naissance des personnes, mais aussi de leurs parents. Il est aussi important que les personnes qui se sentent discriminées indiquent les critères – apparence physique, langue, nom…- sur lesquels se fondent, selon elles, cette discrimination.
- En outre, l'analyse des prénoms et des patronymes, sous certaines conditions, – c'est-à-dire quand elle n'aboutit pas à un classement dans des catégories « ethno-raciales » – peut être utile pour détecter d'éventuelles pratiques discriminatoires.
- A cet égard, la CNIL reste très réservée sur la création d'un référentiel « ethno-racial ». Les personnes auditionnées sont dans leur grande majorité hostiles à une telle nomenclature. Risques de renforcement des stéréotypes, de stigmatisation, classification incertaine, non scientifique, réductrice, approximative… autant de raisons qui expliquent les réticences actuelles et qui justifient une attitude très mesurée sur ce sujet. La CNIL a en particulier estimé que la décision de principe de créer une telle nomenclature, si elle devait être utilisée, de façon obligatoire, en particulier pour les statistiques publiques et pour le recensement, appartiendrait au Législateur sous le contrôle du Conseil constitutionnel.
- Enfin, il est nécessaire de modifier la loi informatique et libertés afin d'assurer une meilleure protection des personnes et de leurs données sensibles, en garantissant le caractère scientifique des recherches et en renforçant le contrôle de la CNIL sur ces fichiers de recherche pour lesquels le seul consentement des personnes ne saurait suffire.

Pour faire suite aux recommandations de la CNIL, Michèle Tabarot et Sébastien Huyghe, tous deux députés et membres de la CNIL, ont présenté un amendement au projet de loi relatif à la maîtrise de l'immigration, à l'intégration et à l'asile, visant à soumettre à autorisation de la CNIL les traitements de données faisant directement ou indirectement apparaître les origines raciales ou ethniques des personnes pour les besoins d'études ayant pour finalités *« la mesure de la diversité des origines des personnes, de la discrimination et de l'intégration »*. Afin de s'assurer de la qualité scientifique de ces études, il était prévu que la CNIL puisse saisir un comité désigné par décret. Afin de ne pas créer une nouvelle structure, il était envisagé de faire appel au conseil scientifique du Comité de concertation pour les données en sciences humaines et sociales, créé auprès des ministres de l'économie, de l'emploi, de l'éducation nationale et de la recherche.

Cette disposition a fait l'objet d'un recours devant le Conseil constitutionnel.

Par une décision du 15 novembre 2007, le Conseil l'a déclaré contraire à la Constitution, estimant que cette disposition était sans lien avec une loi portant sur l'entrée et le séjour des étrangers en France. Sur le fond, le Conseil a jugé que « … *si les traitements nécessaires à la conduite d'études sur la mesure de la diversité des origines des personnes, de la discrimination et de l'intégration peuvent porter sur des données objectives, ils ne sauraient, sans méconnaître le principe énoncé par l'article 1er de la Constitution, reposer sur l'origine ethnique ou la race […] »*.

Cette décision laisse ouverte la question de savoir quels types d'études peuvent aujourd'hui être conduites dans le domaine de la mesure de la diversité, de la discrimination et de l'intégration. Les récents commentaires du Conseil constitutionnel relatifs à l'arrêt qu'il a rendu le 15 novembre 2007 viennent apporter des précisions et laissent à penser que s'il exclut le recours à un référentiel ethno-racial, il permet cependant les études sur le ressenti d'appartenance ethnique.

2. L'internaute à la trace

En octobre 2005, la CNIL a refusé la mise en œuvre de quatre dispositifs de surveillance des réseaux « peer to peer » présentés par des sociétés de perception et

de répartition des droits du secteur musical (SACEM, SDRM, SPPF et SCPP). Ces quatre sociétés ont attaqué les décisions de la CNIL devant le Conseil d'État qui les a partiellement annulées le 23 mai 2007. Il a en effet considéré que la CNIL avait commis une « erreur d'appréciation » en considérant que les traitements ayant pour finalité de rechercher et constater la mise à disposition illégale d'œuvres musicales sur les réseaux étaient disproportionnés. En revanche, le Conseil d'État a retenu l'analyse de la CNIL concernant le procédé d'envoi de messages pédagogiques ciblés aux internautes. Il a ainsi estimé que ces envois étaient illégaux car ils ne relèvent pas des cas de figure où les fournisseurs d'accès à Internet sont autorisés à conserver les données de connexions des internautes.

À la suite de cette décision, la CNIL s'est rapprochée des sociétés de perception et de répartition des droits concernées afin de connaître leurs intentions. Trois d'entre elles (SACEM, SDRM, SCPP) ont renouvelé leurs demandes en les expurgeant du volet pédagogique invalidé. C'est ainsi qu'en novembre 2007, tenue de tirer les conséquences de la décision du Conseil d'État, la CNIL a autorisé ces trois sociétés à mettre en œuvre les traitements de recherche et de constatation d'infractions sur Internet. La dernière société concernée (la SPPF) a renouvelé sa demande au cours du mois de décembre 2007. La mise en œuvre de ce dispositif, identique aux trois autres, devrait être autorisée début 2008.

Parallèlement, dans deux arrêts d'avril et mai 2007, la Cour d'appel de Paris a considéré que les adresses IP collectées à l'occasion de la recherche et de la constatation des actes de contrefaçon sur internet ne permettent pas d'identifier, même indirectement, des personnes physique et que, dès lors elles ne constituent pas des données à caractère personnel. La CNIL, inquiète des conséquences d'une telle analyse sur la protection de la vie privée sur internet, s'est rapprochée de la chancellerie et du procureur près la cour de cassation afin que soit formé un pourvoi dans l'intérêt de la loi contre ces deux arrêts. La CNIL a indiqué que les autorités de protection des données des États membres de l'Union européenne ont rappelé, dans un avis du 20 juin 2007, que l'adresse IP constitue bien une donnée à caractère personnel.

La CNIL a par ailleurs procédé à plusieurs missions de contrôle dans les locaux de sociétés prestataires de service procédant à la surveillance des réseaux « peer to peer ». L'examen des éléments collectés lors des missions de vérifications devraient s'achever au premier trimestre 2008.

À ce stade, il doit également être souligné qu'en juillet 2007 le ministre de la culture et de la communication a créé une mission spécialement chargée de trouver des solutions pour *« lutter contre le téléchargement illicite et développer des offres légales d'œuvre »*. Cette mission menée, M. Denis OLIVENNES, a présenté, en novembre 2007, plusieurs recommandations. Leur prise en compte par le Gouvernement devrait engendrer des aménagements législatifs et techniques et sur lesquels la CNIL devra se prononcer.

C. Fonctionnement et activités de la CNIL

1. Adoption de délibérations

En 2007, la CNIL a siégé 40 fois au cours de 25 séances plénières, 12 formations restreintes et 3 bureaux. Ces réunions ont conduit à l'adoption de 393 délibérations (+30 % par rapport à 2006, + 600 % par rapport à 2003).

Ces délibérations portent sur des avis et autorisations que la CNIL émet au titre de ses missions de conseil ou d'expertise a), de simplification des formalités préalables b), de formalités déclaratives (autorisation ou refus d'autorisation, avis) c), de sanction d).

a) Conseil et expertise

En 2007, la CNIL a rendu 6 avis sur des projets de loi ou de décrets, parmi lesquels un avis sur le projet de décret pris pour l'application de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, et relatif à la conservation des données de nature à permettre l'identification de toute personne physique ou morale ayant contribué à la création d'un contenu mis en ligne.

b) Simplification des formalités préalables

Poursuivant les travaux entrepris en ce sens, la CNIL a adopté des mesures de simplifications des formalités préalables à

effectuer auprès de ses services. Ainsi, elle a adopté quatre autorisations uniques (dont une autorisation relative à la mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion d'infractions à la police des services publics de transports terrestres et une modification d'autorisation relative aux traitements de données à caractère personnel mis en œuvre dans des organismes financiers au titre de la lutte contre le blanchiment de capitaux et le financement du terrorisme) et a émis deux avis sur un acte réglementaire unique.

Ces simplifications s'accompagnent systématiquement d'un encadrement très précis. Elles ne sont pas applicables si les responsables de traitements ne respectent pas l'intégralité des conditions posées par la CNIL à cet effet.

c) Formalités déclaratives
La CNIL a adopté en 2007 :
- 214 autorisations
- 26 refus d'autorisation ;
- 22 avis sur des traitements sensibles ou à risque

d) Sanctions
La CNIL dispose, depuis la loi du 6 août 2004 qui a modifié la loi de protection des données de 1978, de pouvoirs de sanction qui lui permettent de prononcer des amendes d'un montant de 150 000 euros (300 000 euros en cas de réitération), dans la limite de 5 % du chiffre d'affaires.

Au total, sur l'année 2007, la CNIL a prononcé :
- 9 sanctions pécuniaires correspondant à des amendes allant de 5 000 à 50 000 € ;
- 5 avertissements ;
- 101 mises en demeure

2. Les saisines
En 2007, la CNIL a par ailleurs reçu 7 115 saisines (4 455 plaintes et 2 660 demandes de droit d'accès indirect aux fichiers de police et de gendarmerie). Les secteurs les plus concernés sont : *banque-crédit, prospection commerciale, travail, télécommunications*.

Ce chiffre est en augmentation de 20% par rapport à l'année 2006. La CNIL reçoit aujourd'hui deux fois plus de plaintes qu'il y a dix ans !

3. Les temps forts de l'année 2007
Etablir un cadre pour la biométrie
L'année 2007 a été l'occasion pour la CNIL d'examiner son premier système de reconnaissance vocale. Il s'agit d'un dispositif ayant pour objet de sécuriser et de faciliter la gestion et la réinitialisation des mots de passe utilisés pour accéder au système d'information de la société Michelin. Ce procédé permet de générer et de réinitialiser automatiquement les mots de passe. À cette occasion, la CNIL s'est notamment assurée de la bonne information des employés et que toutes les mesures étaient prises pour garantir la sécurité des données et prévenir les risques d'usurpation d'identité.

De même, la CNIL a examiné pour la première fois cinq dispositifs reposant sur la reconnaissance du réseau veineux du doigt de la main et ayant pour objet la contrôle de l'accès aux locaux ou à des systèmes d'information. Après avoir effectué une expertise technique approfondie de cette technologie, la CNIL a considéré que le réseau veineux, en l'état actuel de la technique, est une biométrie sans trace dont l'enregistrement dans une base de données ne comporte pas de risques particuliers au regard de la protection des données.

C'est en 1997 que la CNIL s'est prononcée pour la première fois sur un dispositif reposant sur la reconnaissance des empreintes digitales. Dix ans après, elle a estimé nécessaire de préciser sa position. Elle a ainsi souhaité préciser les principaux critères sur lesquels elle se fonde pour autoriser ou refuser le recours à des dispositifs reposant sur la reconnaissance des empreintes digitales avec un stockage sur un terminal de lecture-comparaison ou sur un serveur.

Cette grille d'analyse repose sur le constat que :
- l'empreinte digitale est une biométrie à « trace » Chaque personne laisse des traces de ses empreintes digitales, plus ou moins facilement exploitables, dans beaucoup de circonstances de la vie courante, par exemple sur un verre ou une poignée de porte etc ;
- ces « traces » peuvent être capturées à l'insu des personnes et être utilisées notamment pour usurper leur identité (utiliser l'exemplaire de l'empreinte relevé pour frauder un dispositif de reconnaissance d'empreintes digitales).

La prise en compte de ces particularités et des risques associés a amené la CNIL à distinguer les dispositifs en fonction du mode de stockage des empreintes :

- stockage sur un support individuel (tel que carte à puce ou clé USB) : le risque est limité, car la personne a la maîtrise de sa donnée biométrique qui ne peut pas être utilisée pour l'identifier à son insu.
- stockage sur le terminal de lecture-comparaison ou sur un serveur : le risque est élevé, car la personne perd la maîtrise de sa donnée qui est détenue par un tiers. En cas d'intrusion dans le système, on peut accéder à l'ensemble des empreintes.

Ainsi, la Commission n'autorise la mise en œuvre de dispositifs reposant sur la reconnaissance des empreintes digitales avec un enregistrement dans une base de données que s'il sont justifiés par un fort impératif de sécurité et satisfont donc à quatre exigences :

- la finalité du dispositif doit être limitée au contrôle de l'accès d'un nombre limité de personnes à une zone bien déterminée, représentant ou contenant un enjeu majeur dépassant l'intérêt strict de l'organisme tel que la protection de l'intégrité physique des personnes, de celle des biens et des installations ou encore de celles de certaines informations.
- la proportionnalité : Il importe de savoir si le système proposé est bien adapté ou est le mieux adapté à la finalité préalablement définie eu égard aux risques qu'il comporte en matière de protection des données à caractère personnel ;
- la sécurité : le dispositif doit permettre à la fois une authentification et/ou une identification fiable des personnes et comporter toutes les garanties de sécurité pour éviter la divulgation des données ;
- l'information des personnes concernées : elle doit être réalisée dans le respect de la « informatique et libertés » et, le cas échéant, du Code du travail.

Affaire SWIFT : vers une sortie de crise

La presse américaine a révélé en juin 2006 l'existence d'un programme de surveillance des transactions bancaires internationales, mis en place par la CIA peu après les attentats du 11 septembre 2001. Ces révélations ont indiqué que la CIA et le département du Trésor américain bénéficient d'un accès, depuis des années, à des millions de données transitant par SWIFT, qui est le principal réseau international de messagerie utilisé dans le domaine bancaire (cf rapport annuel 2006).

Cet accès, mis en place au titre de la lutte contre le financement du terrorisme, permet de surveiller non seulement les transferts financiers vers les États-Unis mais également tous les autres types de transactions réalisées par SWIFT, y compris à l'intérieur de l'Union européenne. Sont ainsi communiqués le montant de la transaction, la devise, la date valeur, le nom du bénéficiaire, le client qui a demandé la transaction financière et l'institution financière de ce client. L'objectif officiel de ce programme consiste à identifier des personnes supposées liées à des activités de financement du terrorisme. Mais les craintes d'utilisation à d'autres fins, moins sécuritaires et plus économiques, ne peuvent être éludées.

Le Groupe de coordination des CNIL européennes (Groupe de l'Article 29, ou G29) dans son avis de novembre 2006, a jugé que la société SWIFT n'avait pas respecté les règles européennes de protection des données, notamment en prêtant son concours à la mise en œuvre du programme de surveillance des données bancaires et financières par les autorités américaines. Le Groupe a jugé également que les institutions financières avaient une part de responsabilité dans cette affaire.

Un an après, on peut parler de « sortie de crise ». Le G29 a émis un communiqué de presse le 11 octobre 2007 pour saluer les progrès substantiels accomplis par SWIFT pour se mettre en conformité avec les principes de protection des données.

L'achèvement des négociations Europe – États-Unis.

La Commission européenne et le Conseil ont, au printemps 2007, négocié avec le gouvernement américain un certain nombre de garanties, afin de définir les règles d'usage des données stockées aux États-Unis dans la base SWIFT par les autorités américaines. Ces garanties concernent la limitation des usages à la lutte contre le terrorisme, le respect du principe de nécessité, des durées de conservation de 5 ans, la nomination d'une « personnalité européenne éminente » ayant compétence pour vérifier le bon fonctionnement du programme de

surveillance (M. Jean-Louis Bruguière). Cet accord politique a fait l'objet d'un échange de lettres qui ont été publiées par la Commission européenne.

Une architecture technique complètement restructurée.
L'architecture actuelle de SWIFT repose sur le principe d'une copie systématique de tous les messages dans deux centres opérationnels, l'un aux Pays-Bas, l'autre aux États-Unis. Ainsi, quelles que soient l'origine et la destination de ces messages, ceux-ci sont actuellement stockés durant 148 jours dans le centre opérationnel américain.

Cependant, à la fin de l'année 2009, cette architecture sera intégralement modifiée avec l'implantation d'un nouveau centre opérationnel en Suisse. Les messages émis par les clients de banques européennes seront systématiquement copiés dans les deux centres européens (Suisse et Pays-Bas), et ne transiteront plus par le serveur américain. La surveillance américaine ne s'exercera donc pas, en particulier, sur les messages concernant des transferts intra-Union européenne. Les messages en provenance ou à destination des États-Unis seront quant à eux systématiquement stockés dans le centre opérationnel américain.

Discovery
La CNIL constate un accroissement récent des exigences de communication de données personnelles détenues, entre autres, par les filiales françaises de sociétés américaines faisant l'objet de procédures de « discovery » devant les juridictions civiles américaines, ou « pre-trial discovery ». Il est devenu fréquent que les sociétés soumises à ces exigences, ou leurs filiales étrangères, se voient obligées de communiquer les copies des disques durs ou des messageries électroniques de certains salariés, voire de l'ensemble de leur personnel.

Par ailleurs, dans un cadre juridique différent, certaines autorités étrangères, telles que la Securities and Exchange Commission (SEC) ou la *Federal Trade Commission* (FTC), peuvent également exiger de sociétés étrangères la production de documents ou pièces, en vertu de pouvoirs d'enquêtes qui leur sont propres. Ces injonctions peuvent concerner des sociétés françaises, selon qu'elles sont filiales de sociétés américaines cotées sur le marché américain, ou qu'elles agissent directement sur le marché américain..

De nombreuses questions se posent au regard de la loi Informatique et Libertés notamment.

Ces demandes de communication peuvent contrevenir aux dispositions relatives à la protection des données, tout particulièrement en ce qui concerne l'information et le consentement des personnes, la proportionnalité du traitement effectué et les conditions du transfert de données hors de l'Union européenne.

De telles situations soulèvent en outre des difficultés relevant d'autres domaines que celui de la loi « Informatique et Libertés », notamment en matière d'entraide judiciaire internationale, de protection des intérêts économiques nationaux, voire de souveraineté nationale.

Inquiets des conséquences que ces obligations engendrent, et de la communication de telles quantités de données au regard des règles françaises et européennes applicables, un certain nombre d'entreprises françaises ou étrangères établies en France et des avocats spécialisés ont tenu à alerter la CNIL sur le développement de ce phénomène.

De manière préoccupante, ces entreprises expriment également des doutes quant à la protection de leurs secrets industriels et commerciaux, certaines d'entre elles évoquant de réelles craintes en matière d'intelligence économique.

Face à l'augmentation du nombre de sociétés concernées qui contactent aujourd'hui la CNIL, celle-ci a tenu à attirer l'attention du gouvernement sur ce point. Une réflexion inter-ministérielle devrait prochainement être engagée.

Fichiers centraux de crédit et de logement
La mise en place de fichiers permettant à l'ensemble d'un secteur d'activité, qu'il s'agisse des établissements de crédit ou des bailleurs professionnels, d'avoir des informations sur les risques de solvabilité présentés par les souscripteurs de crédit ou les demandeurs de logement suscite une grande vigilance de la part de la CNIL compte tenu du risque évident d'exclusion sociale des personnes concernées.

En particulier, la question de la légitimité et de la proportionnalité de l'introduction en France d'une

centrale de crédit se pose tant en termes éthiques et d'atteinte à la vie privée qu'en termes d'efficacité et de coûts. La CNIL s'est toujours refusée à reconnaître la légitimité de la mise en place d'une telle centrale en l'absence d'un encadrement légal spécifique. Elle estime que seul le Législateur a compétence pour se prononcer sur l'utilité sociale d'un « fichier positif » dans le secteur du crédit et pour préciser le cas échéant, les finalités et le contenu de cette base de données. Dans le droit fil de cette position, elle a refusé d'autoriser la mise en œuvre par la société Experian d'une centrale de crédit .

Par ailleurs, elle a refusé d'autoriser la société Infobail à mettre en œuvre deux traitements relatifs à l'information des professionnels de l'immobilier sur la gestion des impayés ou le recensement des locataires d'immeuble d'habitation respectant leurs obligations de paiement, au motif que ces fichiers portaient atteinte au droit au logement institué par le législateur, auquel il revient de se prononcer sur la constitution de fichier tant « négatif » que « positif », dans le secteur du logement.

Les contrôles de l'expérimentation du Dossier Médical Personnalisé (DMP)

La CNIL a procédé à près de 18 contrôles sur place auprès des principaux acteurs de l'expérimentation du DMP : hébergeurs, centres hospitaliers, réseaux de santé, médecins libéraux et centres d'appel. À l'issue de ces contrôles, elle a établi le constat suivant.

La CNIL a constaté que certains hébergeurs transféraient les identifiants de patients aux établissements de soins par voie électronique sans protection particulière. Certains centres d'appel, en cas de perte des identifiants permettant la consultation ou l'alimentation des DMP, envoyaient un mot de passe par courrier électronique non crypté au patient, ou lui communiquaient ce mot de passe par téléphone. Ces pratiques sont de nature à compromettre la confidentialité de ces informations.

La CNIL a également relevé que les patients n'étaient pas tous parfaitement informés que l'accès aux données médicales contenues dans leur DMP nécessitait une connexion internet. De plus, il leur a été parfois indiqué que l'accès à ces données était possible par l'intermédiaire du centre d'appel de l'hébergeur, alors que ce dernier a pour seule fonction d'assister techniquement les patients ou de leur permettre de modifier les données administratives les concernant, leur mot de passe ou la composition de leur cercle de confiance.

Une insuffisance des mesures d'identification-d'authentification mises en œuvre dans les centres d'appel a été relevée puisque l'authentification des patients ne s'opérait pas systématiquement par une interrogation à partir des questions défis (par exemple « le nom de votre belle mère? la marque de votre première voiture? ») qui ont été renseignées par les patients lors de leur inscription.

De plus, des hébergeurs proposent, pour les établissements de soins n'ayant pas équipé leurs professionnels de santé de CPS (carte de professionnel de santé), un accès aux DMP depuis leur site internet sur la base d'un simple identifiant et d'un mot de passe. Cette solution ne saurait être acceptée et est manifestement contraire aux décisions de la CNIL du 21 mars et du 30 mai 2006.

Il a toutefois été vérifié que les personnels administratifs et techniques, tant de l'hébergeur que des centres d'appel, n'ont pas accès aux données de santé contenues dans les DMP.

Allemagne

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La directive 2004/82/CE du 29 avril 2004 (directive API) a été transposée en droit national par le troisième acte de la loi modifiant la loi sur la police fédérale du 22.12.2007. Elle entrera en vigueur le 1er avril 2008.

Selon cette directive, les transporteurs aériens doivent transférer un certain nombre minimal de données. En réalité, lorsqu'elle a transposé la directive en droit national, l'Allemagne a élargi l'étendue de cet ensemble de données. Quoi qu'il en soit, au cours de la procédure législative, le BfDI a réussi à convaincre les législateurs de ne pas réaliser leurs plans initiaux, et de n'ajouter que le « sexe » et le « numéro de visa » à l'ensemble des données devant être transférées par les transporteurs aériens aux autorités de la police fédérale allemande. Les transporteurs aériens comme la police fédérale doivent supprimer ces données dans les 24 heures qui suivent leur collecte et/ou transfert.

L'accord PNR conclu avec les États-Unis en juin 2007, y compris l'échange de lettres y afférent entre le ministère américain de la sécurité intérieure et l'UE, a été transposé en droit national par la loi du 20 décembre 2007 sans aucun amendement. Il est entré en vigueur le 30 décembre 2007.

Le 31 décembre 2007, la loi sur le nouveau règlement pour la surveillance des télécommunications et d'autres mesures d'investigation discrète et sur la mise en œuvre de la directive 2006/24/CE (Journal officiel fédéral – BGBl. – I, n° 70 du 31.12.2007, p. 3198 et seq.) est entrée en vigueur. Cette loi prévoit la rétention des données relatives aux télécommunications, aux e-mails et au trafic sur Internet durant six mois, alors que la rétention obligatoire des données du trafic sur Internet ne sera applicable qu'à partir du 1er janvier 2009. Ainsi, tout le trafic des télécommunications de tous les citoyens de la République fédérale d'Allemagne sera enregistré, bien qu'il soit fort probable que seul un nombre extrêmement réduit de cet énorme volume de données sera utilisé par les autorités policières. Si l'on s'en réfère à la juridiction du Tribunal constitutionnel allemand, des doutes surviennent quant à la constitutionalité de cette rétention de données pour un usage ultérieur à des fins qui ne peuvent être déterminées de manière suffisante.

Les commissaires de la conférence sur la protection des données au niveau fédéral et des Länder ont souvent ouvertement critiqué l'introduction légale de la rétention des données relatives au trafic des télécommunications pour un usage ultérieur ainsi que le renforcement des mesures d'investigation discrète en relation avec les procédures criminelles, également prévu par la loi.

De nombreuses plaintes ont été déposées à ce propos auprès du Tribunal constitutionnel allemand.

La loi amendant la loi sur les passeports et autres règlements du 20 juillet 2007 (BGBl. I, n° 35 du 27.7.2007, p. 1566 et seq.), qui a pris effet le 1er novembre 2007 en République fédérale d'Allemagne, a introduit la deuxième génération de passeports électroniques. Les empreintes des deux index, en plus de la photographie, sont enregistrées dans la puce électronique de ce passeport. La République fédérale se conforme par là au règlement du Conseil n° 2252/2004 du 13 décembre 2004 sur les normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres. Le législateur a exclu la création d'une base de données nationale (Art.4 §3 ligne 3 de la loi sur les passeports). En Allemagne, depuis le 1er novembre 2005, la photographie numérisée du visage était conservée dans une puce dans les passeports de première génération.

Le 1er mars 2007, la loi sur les médias électroniques (TMG) est entrée en vigueur. Cette loi rassemble les conditions en matière de services électroniques et de télécommunications reprises par différentes bases légales. Ceci inclut, d'une part, les règles orientées vers l'économie de la mise en œuvre de la directive sur le commerce électronique. Jusqu'à présent, ces règles étaient comprises dans la loi sur les services de télécommunications (TDG) et dans le traité relatif aux services des médias (MDStV). D'une part, sont également incluses les règles de protection des données de la loi sur la protection des données dans les téléservices (TDDSG), qui était déjà entrée en vigueur, et du traité mentionné

plus haut. Les télécommunications et services multimédias y sont repris sous le terme « télémédias ».
En ce qui concerne le contenu, les anciennes règles ont été pour la plupart transposées sans aucune modification, dont celles qui transposent les exigences de la directive sur le commerce électronique en droit allemand. Dans le domaine de la protection des données, une source d'incertitude juridique qui existait depuis longtemps a été écartée en spécifiant que seule la loi sur la protection des données relatives aux télécommunications était d'application pour les fournisseurs d'accès à Internet, les fournisseurs de services Internet et de télécommunications et de services e-mail. Afin de protéger les destinataires contre les communications commerciales non sollicitées, des règles ont été définies dans le but d'atteindre plus de transparence. Ces règles interdisent tout camouflage ou toute dissimulation de l'expéditeur et du caractère commercial d'un e-mail publicitaire. Elles stipulent également que toute infraction est passible d'une amende.

B. Jurisprudence

Le 13 février 2007, le Tribunal constitutionnel allemand a déclaré que les cours devaient refuser de considérer comme preuve tout test génétique obtenu secrètement pour déterminer la filiation, en raison de la violation du droit de l'enfant concerné à l'autodétermination informationnelle qu'il constitue. Afin de réaliser le droit légal du père de savoir si l'enfant est ou non de lui, le législateur doit prévoir une procédure spécifique qui aura pour unique but d'établir la paternité (en plus de la procédure de contestation de paternité). Cette décision renforce le droit à l'autodétermination informationnelle. La mise en équilibre par la cour des intérêts entre le droit de l'enfant à ne pas révéler ses données et celui du père à savoir s'il s'agit ou non de son enfant, qui est protégé par la Constitution, est conforme avec le principe constitutionnel de proportionnalité. La décision du Tribunal constitutionnel allemand évite également d'ouvrir la voie à des tests génétiques discrets dans d'autres domaines (par exemple, les assurances ou les relations dans le cadre du travail).

C. Questions diverses importantes

En ce qui concerne la lutte contre le terrorisme international, le débat politique s'est concentré en 2007 sur la question de la délimitation des pouvoirs accordés aux services de police et de renseignements pour mener des recherches discrètes en ligne sur des ordinateurs et d'autres systèmes de technologie de l'information, ainsi que de la pertinence des normes légales relatives à ces pouvoirs à créer dans ce domaine.

L'utilisation accrue de l'Internet dans le cadre de la préparation et de l'exécution d'activités terroristes pose de nouveaux défis aux autorités policières. En conséquence, des mesures de surveillance de l'Internet et d'intrusion secrète d'ordinateurs privés ont été prévues dans le but de déceler des activités terroristes ou criminelles à un stade précoce. La loi sur la protection de l'ordre constitutionnel de Rhénanie-du-Nord-Westphalie contient déjà des pouvoirs pertinents pour les investigations en ligne à destination des services de renseignements locaux.

Les partisans de cette loi n'indiquent toutefois que vaguement ce que « investigation en ligne » implique exactement. La seule évidence est que les autorités policières peuvent, à l'aide des connections Internet, s'introduire dans des ordinateurs et/ou systèmes afin d'accéder aux données qui y sont stockées.

Les investigations en ligne soulèvent de graves questions techniques et constitutionnelles, puisque presque tout le monde possède un ordinateur contenant des informations extrêmement personnelles, comme celles d'un agenda. Jusqu'à présent, la principale question reste de trouver le moyen de protéger efficacement l'information, qui fait partie du noyau de la vie privée protégé par la loi fondamentale, contre l'accès en ligne des autorités policières. Dans le courant de 2008, le Tribunal constitutionnel allemand étudiera l'admissibilité d'investigations discrètes en ligne, puisque les règles concernant les enquêtes en ligne du Land de Rhénanie-du-Nord-Westphalie font l'objet d'une plainte pertinente.

Grèce

A. Mise en oeuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

Directive 95/46/CE
La directive 95/46/CE a été transposée en droit national par la loi 2472/97 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel. En 2007, la loi 3625/07 a amendé la loi 2472/97 comme suit.

L'article 2 de la loi 2472/97 a été amendé afin d'autoriser la publication d'accusations au pénal ou de condamnations. Cette publication est en particulier autorisable sur ordonnance du procureur compétent du Tribunal de première instance, ou du parquet général si l'affaire est en instance devant la Cour d'appel, pour des faits qualifiés d'actes délictueux graves ou de délits intentionnels et surtout pour des attentats à la vie, des atteintes à la liberté sexuelle, des délits relatifs à l'exploitation sexuelle à des fins commerciales, des atteintes à la liberté, des atteintes au patrimoine, des atteintes au droit à la propriété, des violations de la législation sur les drogues, des conspirations contre l'ordre public ainsi que des délits sur mineurs. La publication d'accusations au pénal ou de condamnations vise à protéger la communauté, les mineurs et les groupes vulnérables ou défavorisés, ainsi qu'à permettre à l'État de sanctionner plus facilement de tels délits.

En vertu de l'amendement de l'article 3 de la loi 2472/97, lorsque les citoyens exercent leur droit de réunion, conformément à l'article 11 de la Constitution, l'utilisation de moyens d'enregistrement audio et vidéo ou d'autres moyens techniques spéciaux est autorisée sur ordonnance du ministère public et si l'ordre public et la sécurité sont gravement menacés. Les enregistrements précités sont uniquement destinés à être utilisés comme preuves de la perpétration d'un délit devant une autorité d'enquête, un représentant du ministère public ou un tribunal. Le traitement de tout autre matériel non nécessaire pour atteindre l'objectif précité dans le cadre de la vérification de délits commis est interdit, et le matériel concerné sera détruit sur ordre du procureur compétent.

Une traduction anglaise du texte amendé est disponible sur www.dpa.gr

Directive 2002/58/EC
La directive 2002/58/CE a été transposée en droit national par la loi 3471/2006 (sur le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques) et l'amendement de la loi 2472/97. La nouvelle loi a été présentée comme un nouveau texte législatif et non comme un amendement à la loi 2774/1999 (sur la protection des données à caractère personnel dans les secteurs des télécommunications), qui a été abrogée dans son intégralité par souci de clarté et pour éviter toute confusion.

Une traduction anglaise de la loi 3471/2006 sera bientôt disponible sur www.dpa.gr

Directive 2006/24/EC
Le Comité permanent du ministère de la Justice s'emploie actuellement à rédiger un projet de loi qui transposera la directive 2006/24/CE en droit national.

Principaux développements
À la fin de 2007, le HDPA (Office grec de la protection des données) a commencé à mettre en service le nouveau système informatique qui non seulement améliorera les fonctions administratives utiles aux utilisateurs internes mais offrira en outre un nouveau portail pour les services de cybergouvernement à l'attention des citoyens.

B. Jurisprudence

Décision 3/2007
Le HDPA a statué que les dispositions de la loi 2472/97 concernant *la protection des personnes physiques à l'égard du traitement des données à caractère personnel* s'appliquent à la collecte et au traitement de données à caractère personnel recueillies via un système de vidéosurveillance d'un lieu de résidence privé qui vise à surveiller les travailleurs qui y offrent leurs services professionnels ou dont le fonctionnement aboutit à une telle surveillance. Il est illégal d'installer et d'exploiter un système de vidéosurveillance sans respecter les conditions spécifiées et, en particulier, sans avertir le HDPA du fonctionnement d'un tel

système et sans en informer les personnes concernées ; le responsable d'un tel système s'expose aux sanctions prévues.

Décision 6/2007
La publication par le ministère de la Défense nationale des noms de personnes qui: a) ont été légalement exemptées du service militaire pour des raisons de santé; b) ont été considérées comme exemptées du service militaire après deuxième vérification des documents justificatifs; c) ont été illégalement exemptés du service militaire pour des raisons de santé viole les dispositions de la loi 2472/97 car les données susmentionnées ne relèvent d'aucune des exceptions à la loi, de sorte que leur traitement ne peut être autorisé.

Décision 62/07
Dans sa décision 62/2007, l'Office grec de la protection des données a jugé illégales l'utilisation d'un système biométrique pour le contrôle de l'entrée et de la sortie des travailleurs et l'utilisation d'un système de vidéosurveillance sur les lieux de travail. Il a en conséquence imposé une amende de 8 000 euros pour l'utilisation du système biométrique et de 6 000 euros pour celle d'un système de vidéosurveillance. Le HDPA a aussi sommé le responsable du traitement des données de désinstaller le système biométrique et de suivre la procédure décrite dans la directive 1122/2000 concernant l'exploitation de systèmes de vidéosurveillance.

Décision 64/07
Le HDPA a recommandé à TEIRESIAS Bank Information Systems SA et aux banques grecques d'instaurer une procédure pour signaler à TEIRESIAS, dans les 15 jours suivant le règlement, l'apurement de dettes à la fin de contrats de prêts personnels ou de prêts à la consommation consentis à des personnes physiques par des banques ou des institutions financières. TEIRESIAS amendera ses dossiers immédiatement et pas plus de 15 jours après avoir reçu notification du règlement, sans que la personne concernée ne doive entreprendre d'autres actions.

C. Questions diverses importantes

Le 19 novembre 2007, le président, le vice-président et sept membres du DPA grec ont remis leur démission en guise de protestation contre l'incident décrit ci-dessous.

L'Office de la protection des données avait rendu sa décision N°58/2005, par laquelle il autorisait l'utilisation de systèmes de vidéosurveillance C4I (293 caméras) et de 49 caméras préexistantes, uniquement pour la gestion du trafic dans des circonstances particulières et pour des motifs décrits en détail dans l'exposé des motifs de cette décision.

En particulier, il avait souligné que l'exploitation de ce système et l'utilisation des données recueillies et enregistrées via ce système étaient interdites pour tout autre motif que la vérification des délits, conformément à l'usage licite du système et aux conditions exposées dans la décision. Le fonctionnement de caméras installées à des carrefours ou sur des axes routiers est interdit lorsque le trafic de véhicules est interrompu, par ex. lors de manifestations, etc.

Le Ministre de l'Intérieur a déposé devant le Conseil d'État une requête en annulation contre la décision précitée. L'affaire a été entendue le 12.1.2007 et est depuis en instance devant la session plénière du Conseil d'État. Il convient de noter que la proposition du juge rapporteur rejetait cette requête en annulation. En outre, le *Suspension Committee* du Conseil d'État avait déjà rejeté la requête en suspension relative à l'interdiction de l'exploitation de caméras. En novembre 2007, alors que l'affaire était en instance et qu'une question avait été posée par le quartier général de la police hellène, l'avocat général près la Cour suprême civile et pénale hellène (*Areios Pagos*) a rendu son avis N° 14/2007 autorisant l'exploitation du système de vidéosurveillance précité, sous le contrôle d'un représentant du ministère public, dans tous les cas, même en l'absence de trafic routier ou si la circulation routière est interdite, par ex. pendant des manifestations, etc., sans toutefois que les images reçues ne soient enregistrées, sauf en cas d'infraction. L'Office grec de la protection des données, la seule autorité qui, en vertu de la Constitution, est compétente pour juger de cette question, conformément aux règles de

protection des données à caractère personnel, a publié un communiqué de presse sur le problème survenu, signalant que sa décision, n'ayant pas été annulée par le Conseil d'État, restait légale et, dès lors, applicable et contraignante. De plus, la violation de ses dispositions entraînerait l'application des sanctions administratives prévues par la loi 2472/97. En conséquence, la sanction administrative de l'amende a déjà été imposée deux fois au ministère de l'Intérieur. Malgré le traitement explicite, catégorique et unique de cette affaire sur la base de la Constitution, l'exploitation du système précité de vidéosurveillance s'est poursuivie sur ordre du ministère public. Dès lors, sous le contrôle de représentants du ministère public, des images ont été reçues de la manifestation et de la marche qui ont eu lieu le 17.11.2007, c'est-à-dire pendant la commémoration du soulèvement de l'École polytechnique d'Athènes, pendant laquelle le trafic a été interdit dans la zone concernée. Ce fait a été confirmé dans le rapport des auditeurs de l'Office de la protection des données. Après avoir reçu un ordre écrit, ces auditeurs se sont rendus à la direction de la police d'Attique pour procéder à un audit, selon les dispositions de l'article 19, paragraphe 1, de la loi 2472/97. Ainsi, les dispositions de la décision précitée de l'Office grec de la protection des données ont été ouvertement violées et l'indépendance de l'Office, garantie par la Constitution, en a été affectée et l'autorité de cette institution, diminuée.

Hongrie

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

L'an dernier, il y a eu une tentative de transposer la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques et modifiant la directive 2002/58/CE. Le commissaire à la protection des données a reçu plusieurs projets dans le cadre de la procédure de coordination administrative et a formulé des commentaires sur le droit à la vie privée, sur la confidentialité des communications et sur la protection des données à caractère personnel. Il a expliqué que la conservation massive de données ne répondait pas aux principes régissant la limitation des droits de l'homme tels qu'établis par la Cour européenne des droits de l'homme, sauf si la limitation était nécessaire, appropriée et proportionnée pour protéger l'ordre public, la sécurité nationale et la sécurité des citoyens et pour prévenir, instruire et combattre la criminalité et l'usage illégal du système de télécommunications électroniques dans un État constitutionnel démocratique. La lutte contre le terrorisme et la criminalité organisée ne peut servir de justification à toute action. Selon le commissaire, même si le droit européen laisse aux États membres une marge pour légiférer au niveau national, une application automatique des extrêmes (dans notre cas, le temps de conservation le plus long possible) est inacceptable ; il faut tenir compte des principes régissant la protection des données. Ce projet n'a pas été soumis au Parlement.

B. Jurisprudence

Le grand public s'est fort inquiété de la réforme des soins de santé qui a entraîné la fermeture et la fusion d'institutions. Le commissaire a lancé une enquête d'office sur le lieu où sont conservés des documents ayant appartenu à des institutions de santé aujourd'hui fermées car le contrôle de ces documents a une incidence majeure sur l'exercice des droits des patients à l'autodétermination informationnelle. L'enquête complète auprès des décideurs concernés et des directions des institutions fermées a conclu que la réforme institutionnelle menaçait gravement le droit des patients à l'autodétermination informationnelle parce qu'elle ne résolvait pas le problème du contrôle des documents détenus dans des institutions destinées à être fermées. Il est probable que les personnes concernées ne seront absolument pas en mesure de conserver la trace de leurs données médicales et des documents y afférents. En conséquence, elles seront privées non seulement de leur droit d'accès aux documents mais aussi de leurs droits prévus par la loi sur les soins de santé. De plus, les institutions (les médecins) prodiguant les soins ne pourront pas obtenir des informations sur les antécédents médicaux des patients, ce qui compromet la capacité de ces derniers à protéger leur propre santé, à recevoir un traitement et à se rétablir. Le commissaire à la protection des données a appelé le ministre de la santé à accorder une attention minutieuse à la question des documents médicaux et à prendre les mesures nécessaires pour garantir que toutes les institutions fermées tiennent compte des droits des patients lorsqu'elles décideront du traitement des documents médicaux. Pour assurer la poursuite de soins appropriés, le système des transferts de documents médicaux devrait être conçu de façon à permettre un accès continu aux informations relatives aux soins donnés aux patients et à aussi prendre en considération les documents conservés sur des supports autres que le papier.

Une des recommandations les plus importantes publiées par le commissaire en 2007 porte sur les exigences de protection des données en matière d'identification dans le cadre du cybergouvernement. Cette recommandation se borne aux critères minimums et ne vise pas à présenter la seule solution possible pour l'identification. L'objectif du document était de créer des conditions-cadres permettant aux clients de poursuivre leurs activités de façon efficace tout en profitant du même degré de protection de la vie privée que celui offert par les services administratifs traditionnels. Les principes et idées de mise en œuvre se sont avérés utiles pour le cybergouvernement, pour les autorités et, enfin et surtout, pour les citoyens.

L'utilisation de messages de courrier électronique dans des procédures pénales a constitué un problème récurrent en 2007. La législation applicable

considère le courrier traditionnel comme le moyen de communication général et le courrier électronique, comme le moyen de communication exceptionnel, même si ce dernier s'est popularisé. Diverses règles s'appliquent au courrier traditionnel distribué par la poste ou « encore en route », et des garanties suffisantes protègent les personnes concernées de fouilles secrètes. Le nœud du problème réside dans la difficulté d'appliquer ces règles au courrier électronique.

La forme « classique » de courrier électronique est, tout comme une lettre postée, une communication entre deux personnes précises dont le contenu n'est connu que de l'expéditeur et du destinataire mais, dans le cas de l'e-mail, les messages se trouvent dans les ordinateurs (systèmes informatiques) respectifs de l'expéditeur et du destinataire. Souvent, toutefois, les e-mails sont envoyés via un fournisseur de contenus. Dans ce cas, les données sont stockées non dans l'ordinateur de l'expéditeur ou du destinataire mais dans celui du fournisseur, auquel l'expéditeur et le destinataire peuvent accéder via l'Internet. Les logiciels d'e-mails gratuits appartiennent à cette catégorie car ils n'effectuent pas les transferts réels de données.

L'incertitude qui en découle souvent, notamment lorsque la police tente de déterminer qui satisfait à la définition d'un fournisseur de télécommunications, peut entraîner des erreurs dans le choix du motif juridique applicable. Les saisies policières pour accéder à des données stockées sur le serveur d'un fournisseur de services donnent aussi matière à inquiétude. L'application de termes traditionnels tels que « distribution » à une nouvelle technologie ou méthode ne manquera pas de poser des problèmes. Si le terme « distribution » est clair dans le contexte du courrier postal, il est ambigu lorsqu'il est appliqué aux e-mails. Il est facile de déterminer si le destinataire a ouvert sa liste d'e-mails ou un e-mail particulier mais, d'après l'interprétation des procureurs, ce moment est sans importance : les e-mails sont considérés comme « distribués » dès qu'ils ont été envoyés. Le commissaire à la protection des données a avisé le Procureur général qu'il n'était pas d'accord avec cette interprétation et a souligné que, dans les communications électroniques, ce sont les caractéristiques et le but du flux de données et non sa méthode qui devraient déterminer l'applicabilité des règles relatives au secret de la correspondance.

C. Questions diverses importantes

Les règles régissant le traitement des données par les autorités chargées de faire respecter la loi ont été considérablement modifiées sur plusieurs points en 2007, en partie en réaction aux problèmes rencontrés pendant les troubles politiques de 2006. Les amendements en matière de contrôles policiers, proposés dans le projet d'amendement de la loi sur la police, et la réduction de la durée excessive de conservation des données recueillies pendant les contrôles sont certes positifs mais l'autorisation donnée à la police de surveiller n'importe qui, n'importe quand, n'importe où dans les lieux publics est, elle, trop générale.

Un des points litigieux du projet amendant certains actes dans le domaine du droit pénal concerne l'utilisation d'équipements de surveillance électronique par les établissements pénitentiaires aux fins de faire respecter la loi. Ce projet autoriserait l'installation de tels équipements également hors des établissements pénitentiaires.

Il convient en outre de mentionner la préparation du nouveau Code civil, en cours depuis plusieurs années et toujours pas terminée en 2007. La nouvelle codification des règles sur le secret professionnel dans ce projet de Code civil soulève des doutes. Du point de vue de la protection des données, il faudrait aussi accorder de l'attention aux projets de règles sur le registre du cadastre.

En 2007, nous avons poursuivi les préparations de l'accession de la Hongrie à l'espace Schengen en vérifiant les pratiques de protection des données appliquées par les consulats de Hongrie pour la délivrance de visas (notamment à Saint-Pétersbourg, à Shanghai, à Hong Kong et à Chisinau). Les inspections se sont concentrées sur la nécessité de recueillir des données à caractère personnel pour évaluer les demandes de visas et sur le respect par les consulats des règles régissant la protection des données.

Irlande

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

Ces deux directives ont été entièrement transposées en droit irlandais. Parmi les nouveaux textes législatifs de 2007 ayant eu une incidence significative sur la protection des données en Irlande, il convient de mentionner de nouvelles réglementations amendant la désignation des responsables du traitement des données et du personnel chargé de ce traitement, désormais tenus de s'enregistrer auprès de l'Office. D'autres réglementations entrées en vigueur durant l'année stipulent que le traitement de données génétiques lié à l'emploi d'une personne doit avoir l'approbation préalable du commissaire à la protection des données. Depuis le 24 octobre 2007, toutes les dispositions des lois sur la protection des données s'appliquent à toutes les données encodées manuellement.

L'Irlande a remis en cause, devant la Cour européenne de justice, la base juridique de la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public (amendant la directive 2002/58/CE). Néanmoins, sans préjudice de la procédure en cours, cette directive (qui n'a pas encore été transposée) devrait être transposée au début de 2008.

B. Jurisprudence

Dans la plupart des cas, conformément à la section 10 des lois irlandaises de 1988 et de 2003 sur la protection des données, les plaintes soumises au commissaire sont résolues à l'amiable sans recours à une décision formelle. À titre de règlement amiable, le responsable concerné du traitement des données peut, par exemple, faire une donation à un organisme caritatif approprié ou un geste similaire. Des moyens plus énergiques peuvent être utilisés pour faire respecter la loi lorsque les responsables du traitement des données ne respectent pas les droits d'accès des personnes concernées, et certains responsables du traitement des données peuvent être cités dans des études de cas incluses dans le Rapport annuel du commissaire. Cependant, le commissaire a pris plusieurs décisions concernant des plaintes déposées en vertu des lois sur la protection des données. En voici quelques exemples :

a) La mise en demeure d'une société de cesser des « appels non sollicités » de marketing. À la suite de plaintes relatives aux appels non sollicités de marketing direct d'une société spécifique, l'Office a découvert que les procédures de marketing de cette société n'étaient pas assez solides pour respecter les droits des abonnés en matière de protection des données. Nous avons dès lors demandé à cette société de cesser tout marketing par « appels non sollicités » jusqu'à ce qu'elle ait remédié au problème, sous peine de recevoir une mise en demeure juridiquement contraignante à cette fin. La société s'est pliée à notre demande et a suspendu ses « appels non sollicités » pendant vingt jours jusqu'à ce qu'elle ait pris les mesures correctrices appropriées.
b) Une décision de notifier une demande d'information en réponse à une allégation de secret professionnel. L'Office avait reçu une plainte concernant un responsable du traitement de données qui refusait de donner suite à une demande d'accès, sous prétexte que les documents en question étaient protégés par le secret professionnel. Notre enquête a confirmé que le secret professionnel ne pouvait pas s'appliquer à un document précis demandé par la personne concernée. Comme le responsable du traitement des données continuait à opposer le secret professionnel, l'Office n'a eu d'autre option que de signifier une demande d'information exigeant qu'une copie du document concerné lui soit fournie. Après examen, l'Office a acquis la conviction que ce document contenait des données à caractère personnel sur la personne concernée et que les exemptions limitées prévues par les lois sur la protection des données quant au droit d'accès n'étaient pas d'application dans ce cas. Le document a ensuite été communiqué.

C. Questions diverses importantes

Durant l'été 2007, à la suite d'un grand nombre de plaintes reçues au sujet de certaines entreprises actives dans le secteur du marketing par sms, l'Office y a effectué des inspections sans préavis selon une stratégie visant à utiliser ses pleins pouvoirs pour s'attaquer au domaine des sms non sollicités. Dans le cadre du suivi de ces inspections, nous entamons maintenant des poursuites contre les entreprises qui ont envoyé ou permis d'envoyer des communications non sollicitées aux abonnés ou qui, d'une manière ou d'une autre, n'ont pas satisfait à leurs obligations en matière de respect de la vie privée des individus.

Italie

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La directive 95/46/CE a été transposée dans la législation italienne par la loi n° 675 du 31 décembre 1996, qui est entrée en vigueur six mois plus tard. En juin 2003, une nouvelle loi (Code de protection des données) a été adoptée dans le but de consolider et de remplacer entièrement la législation existante. Cette loi est entrée en vigueur le 1er janvier 2004.

La directive 2002/58/CE a été intégrée dans la législation nationale par le Code de protection des données. Son titre X traite des « communications électroniques » (sections 121 à 132).

Auditions parlementaires

La *Garante* (l'autorité en charge de la protection des données, APD en abrégé) a été entendue à plusieurs reprises en 2007 sur des questions majeures examinées par les commissions parlementaires compétentes. Elle a ainsi été entendue sur des questions du ressort de la commission parlementaire en charge de la supervision de l'Accord de Schengen, des activités d'Europol et de l'immigration et associée au débat autour du projet de loi sur le testament de vie. L'autorité a également participé aux auditions dans le cadre de l'examen du projet de loi relatif à la création d'un système de prévention des fraudes en matière de crédit à la consommation et dans le cadre d'un projet réglementant le secteur télévisé durant la phase de basculement vers les technologies digitales. L'APD s'est également associée à une enquête sur les rapports entre la liberté de la presse et la protection des droits personnels et à une enquête autour de la gestion et de l'exploitation des informations conservées par le département des recettes. Retenons également la participation de l'APD à une audition sur l'utilisation des systèmes Galileo et GPS de navigation par satellite visant à mettre en place un système satellitaire mondial à des fins non militaires.

Sensibilisation du Parlement et du gouvernement

Les tâches confiées à l'APD italienne par le Code de protection des données incluent la sensibilisation du Parlement et du gouvernement à la nécessité de réglementer certains secteurs. Mentionnons à cet égard la proposition faite par le gouvernement italien au Parlement en vue de la création d'une base de données ADN gérée par la police, pour des raisons de sécurité. Nous avons eu l'occasion d'attirer l'attention du Parlement et du gouvernement sur la nécessité de prévoir les garanties élémentaires en vue de la création de cette base nationale de données ADN. L'APD a notamment spécifié que cette base de données devait uniquement servir à l'identification d'individus particuliers. Il ne faut donc pas envisager de collecte obligatoire d'échantillons d'ADN, et, dans les cas où une telle collecte devait être prise en compte pour certaines catégories de personnes – comme les personnes arrêtées, interrogées, mises en examen et/ou condamnées –, des garanties proportionnées devront être définies ; la période de conservation de ces données d'identification devra être proportionnée aux objectifs de la collecte. Des garanties supplémentaires ont été mises en place concernant les mécanismes d'accès (cf. la recommandation portant sur un protocole des accès) et l'exercice des droits des personnes concernées. Durant le débat parlementaire, l'APD a également recommandé des garanties sur un projet de loi prévoyant d'exempter les PME et les indépendants de l'application de mesures de sécurité minimales. En effet, non amendé, ce projet de loi aurait considérablement limité les garanties applicables au traitement des données des membres du personnel dans de très nombreuses entreprises italiennes. L'APD a fait remarquer que le droit communautaire et international n'autorisait pas d'exempter une catégorie entière d'individus de l'application de règlements clés dans le domaine de la protection des données personnelles, pas plus qu'il n'autorisait de différences entre les opérations de traitement des données des organismes publics et des entreprises privées. L'APD a par ailleurs appelé le Parlement italien à amender le Code de protection des données afin de permettre la prise en compte d'instruments supplémentaires (en particulier les règles d'entreprise contraignantes), ceci afin d'assurer une protection adéquate des données personnelles, conformément aux dispositions de la directive européenne (article 26(20)).

Avis
Conformément au Code de protection des données, le Premier ministre doit consulter l'APD italienne chaque fois que de nouveaux règlements ou instruments administratifs sont susceptibles d'avoir un impact sur les questions de protection des données personnelles. En 2007, c'est arrivé à plusieurs reprises. L'APD italienne a ainsi rendu des avis dans les domaines ou pour les projets suivants : le répertoire informatisé des taxes automobiles ; la composition et les tâches de la Commission en charge des adoptions internationales (nous avons ici autorisé le traitement des données personnelles des enfants étrangers adoptés par des parents italiens ou confiés à leur garde, ces données personnelles se limitant aux données indispensables et les garanties du Code de protection des données étant respectées) ; l'utilisation du système financier aux fins du blanchiment de capitaux issus d'activités criminelles et du financement du terrorisme ; les règles techniques relatives aux cartes d'identité et aux cartes d'identité électroniques ; la coordination des activités des administrations publiques visant à protéger les mineurs contre l'exploitation et les abus sexuels ; les dispositions régissant les paiements effectués par des organismes de l'administration publique ; le code d'auto-réglementation dans le domaine des médias et des sports et les mécanismes visant à permettre aux autorités locales de participer aux contrôles fiscaux et autres dispositions visant à lutter contre l'évasion fiscale.

B. Jurisprudence

En 2007, la Cour de cassation italienne (Cour suprême) a rendu plusieurs décisions dans le domaine de la protection des données :

Compétence territoriale en matière de protection des données
Le Code de protection des données prévoit que le tribunal du lieu où le contrôleur de données est domicilié est territorialement compétent pour tout litige en rapport avec l'application des dispositions de ce Code. Cette compétence ne souffre aucune dérogation.

Accès au courrier électronique des employés
L'accès à la correspondance d'autrui est punissable si le courrier en question est « scellé ». Les courriers électroniques, quant à eux sont, sont « scellés » pour toute entité non autorisée à accéder aux systèmes informatiques utilisés pour l'envoi ou la réception de messages électroniques personnels. Les juges ont en particulier estimé que toute entité (y compris l'employeur) avait légalement accès aux courriers électroniques conservés dans le système informatique de l'entreprise étant donné qu'elle était légalement en possession des codes d'accès appropriés (identifiant + mot de passe), les instructions et les informations relatives à ces codes ayant été communiquées par l'entreprise à tous les membres du personnel afin de permettre l'accès en cas d'absence de l'employé concerné. Cette décision va dans le sens des orientations de l'APD publiées le 1er mars 2007 (voir ci-dessous). L'APD a en effet estimé que les supérieurs, dans les entreprises, ont légalement accès aux ordinateurs et au matériel informatique mis à la disposition du personnel lorsque les conditions légitimant l'accès ont été notifiées de manière détaillée aux employés en question. Inversement, et comme l'a estimé la Cour dans une autre affaire, un administrateur-système d'une entreprise ne peut utiliser ses privilèges « informatiques » – comme la possibilité d'affecter des mots de passe aux titulaires d'un compte utilisateur – pour lire les courriels électroniques des membres de l'entreprise. Ces derniers sont incontestablement libres de remplacer les mots de passe assignés par l'administrateur par les mots de passe de leur choix, ceci afin de protéger leur vie privée et la confidentialité de leurs données, l'administrateur-système n'étant alors plus autorisé à accéder aux comptes individuels. La Cour a souligné que l'interception frauduleuse de messages ne consistait pas à les intercepter de façon à rendre impossible ou extrêmement difficile l'identification de l'entité responsable de l'interception, mais bien à déjouer ou lever les mécanismes de sécurité déployés pour empêcher les tiers d'avoir accès aux messages.

Liberté de la presse et anonymat des sources
Un ordre de saisie émis par un tribunal romain portant sur un ordinateur utilisé par un journaliste a été cassé par la Cour de cassation, entre autres parce que le tribunal n'avait pas pris en compte le secret professionnel et les privilèges des journalistes. La Cour estime qu'il convient de faire preuve de prudence au moment d'ordonner des recherches ou des saisies impliquant des journalistes en raison des limites qu'elles risquent d'entraîner par

rapport à la liberté de la presse. Plus précisément, le secret professionnel des journalistes est destiné à protéger la liberté et l'impartialité de la presse. Le secret professionnel ne doit dès lors pas être considéré comme un privilège accordé à un journaliste à titre individuel.

Téléphonie mobile, vidéos et pédopornographie

La diffusion d'une vidéo pornographique (montrant des rapports sexuels entre une mineure et des jeunes hommes) par téléphone mobile répond à la définition légale de la pédopornographie. Pour les juges, la loi italienne punit non seulement l'exploitation commerciale de la pornographie enfantine, mais aussi tout acte susceptible de générer du matériel pornographique impliquant des mineurs. L'inculpé avait enregistré et diffusé, via son téléphone mobile, une vidéo montrant les ébats d'une jeune fille avec plusieurs jeunes hommes. Dans ce cas, il y avait bien pédopornographie puisqu'il était aisément prévisible que le matériel vidéo en question allait être diffusé à plus grande échelle par les premiers destinataires – aggravant ainsi le préjudice initial, en particulier en ce qui concerne la vie et la personnalité de la victime.

Retenons également une ***décision du Conseil d'État*** (la plus haute instance judiciaire en matière administrative) qui a établi la légalité de l'enregistrement d'une conversation à l'insu des autres interlocuteurs réalisée dans le but d'utiliser cet enregistrement comme preuve lors d'un procès. Les juges ont ainsi estimé qu'aucune sanction disciplinaire ne devait être infligée à un professeur d'université qui avait enregistré ses conversations avec d'autres enseignants et étudiants dans le but d'obtenir des preuves pouvant être légalement utilisées lors d'un procès. Condamner un tel acte reviendrait en effet à punir l'exercice légitime du droit à introduire et à défendre une action en justice.

C. Questions diverses importantes

Bases de données des services répressifs

En 2007, l'APD italienne a continué à concentrer son attention sur la gestion des grandes bases de données mises en place aux fins de l'application de la loi. L'autorité a également réalisé des enquêtes minutieuses en rapport avec le traitement des données par ceux qui exercent les fonctions juridictionnelles. Elle a ainsi mis en évidence la nécessité d'appliquer des mesures de sécurité plus strictes dans ce domaine, en particulier en ce qui concerne l'échange d'écoutes téléphoniques entre les opérateurs de téléphonie et les autorités judiciaires. L'APD a aussi confirmé l'absence de cadre approprié régissant la conservation et le traitement de données personnelles, entre autres à la suite des inspections auprès de la Cour de Rome, le premier tribunal italien en termes d'affaires traitées annuellement. L'APD a poursuivi sa coopération avec le ministère de la justice, le Conseil national de la magistrature et les autorités judiciaires en vue de faciliter le respect et l'application de la loi. Il convient par ailleurs de souligner que l'absence de ressources financières suffisantes est l'un des principaux obstacles auxquels se heurtent les autorités judiciaires en matière de protection adéquate des données personnelles des citoyens.

Sécurité des communications téléphoniques et électroniques

À la suite d'une enquête approfondie portant sur le traitement des données personnelles par les principaux opérateurs italiens de télécommunications, l'APD a mis au jour des anomalies dans la collecte et le traitement de données à caractère personnel relatives à l'utilisation de l'Internet. En particulier, certains opérateurs agissant en qualité de « fournisseurs d'accès à Internet » conservaient les historiques de navigation détaillés de leurs utilisateurs ou abonnés, arguant que la loi les y obligeait. Ces opérateurs utilisaient à cette fin divers outils, parmi lesquels des outils de détection du matériel, des serveurs proxy transparents et des techniques d'inspection de paquets, et pouvaient ainsi recueillir des informations extrêmement détaillées : couple d'adresse IP source/destination, logs HTTP « fine-grained », mots recherchés soumis par les utilisateurs aux moteurs de recherche, pouvoirs d'authentification transmis via de simples connections http et toute information sensible susceptible d'être spécifiée dans une adresse web de type URL. Ce type de traitement n'est toutefois pas justifié par des impératifs techniques liés à l'exécution des tâches confiées aux fournisseurs d'accès. Et c'est la raison pour laquelle l'APD a rendu trois décisions interdisant ce type de traitement des données et ordonné aux fournisseurs de supprimer dans les soixante jours toutes les données de navigation des utilisateurs ou

abonnés qui avaient été enregistrées illégalement. L'APD italienne a également adopté une disposition générale concernant le stockage et le traitement des données de trafic générées par les opérateurs de téléphonie et les fournisseurs d'accès à Internet. L'objectif était d'améliorer la sécurité en ce qui concerne les données de trafic conservées par les fournisseurs pour des raisons légales (y compris à des fins d'application de la loi). Les positions élaborées par la *Garante* précisent qui doit conserver quel type de données tout en établissant des dispositions techniques et organisationnelles visant à sécuriser le stockage des données concernées. L'APD a ainsi clarifié, en particulier, que les fournisseurs de contenu Internet, les gestionnaires de moteurs de recherche, les organismes et organisations publiques mettant des réseaux téléphoniques et Internet à la disposition de leur personnel ou utilisant les serveurs d'autres entités, ainsi que les cybercafés et autres établissements similaires ne sont pas soumis aux obligations de conservation des données, et ce conformément aux définitions exposées dans la directive 2002/22/CE concernant le service universel ainsi que dans les directives 2002/58/CE et 2006/24/CE. Plusieurs mesures techniques de protection des données ont été recommandées, parmi lesquelles des mesures plus strictes pour l'authentification et les procédures biométriques, l'audit à fins grains appliqué aux bases de données et aux systèmes informatiques, le codage des bases de données, la collecte centralisée et sécurisée des logs ainsi que des mesures visant à sécuriser physiquement les salles d'ordinateurs et les centres de données.

Plaintes officielles

316 plaintes officielles ont fait l'objet d'une décision en 2007. Tout comme les années précédentes, la majorité d'entre elles impliquait des banques, des sociétés financières et des établissements financiers de crédit. Un certain nombre d'affaires étaient en rapport avec le traitement des « informations commerciales » (avoirs et dettes, procédures de faillite et de liquidation, etc.) par des entreprises opérant dans ce secteur. Ces affaires ont donné lieu à des décisions obligeant ces entreprises à réaliser des contrôles approfondis avant de réutiliser les informations publiques, ceci afin de veiller à ce que les informations en question soient précises, complètes et actualisées.

Plusieurs plaintes en rapport avec le traitement de données à des fins journalistiques ont permis à l'APD italienne de clarifier davantage le concept de « données à caractère personnel ». Ainsi, en ce qui concerne la possibilité d'identifier des personnes, les données à caractère personnel de personnes n'étant pas explicitement identifiées mais qui sont susceptibles d'être reconnues à l'aide d'autres éléments d'information en possession du responsable du traitement des données (ou d'éléments d'information existant ailleurs) ont été considérées par l'APD comme des données à caractère personnel. L'APD a toutefois souligné qu'il fallait ici tenir compte de tous les moyens pouvant être raisonnablement utilisés par le responsable du traitement des données et/ou une autre entité pour identifier la personne en question.

Dans une autre affaire, les données personnelles de deux personnes – autres que le plaignant – ont été publiées. Plus précisément, il avait été rapporté que le mari de la plaignante était décédé dans un accident de voiture avec sa « compagne actuelle ». L'APD a estimé qu'il s'agissait là de données à caractère personnel concernant la plaignante, quoique de manière indirecte, puisque celle-ci en avait subi les conséquences.

On notera aussi avec intérêt que l'APD a estimé que la plainte déposée contre un hôpital n'était pas recevable parce que la demande d'accès ne visait pas à obtenir des données personnelles génétiques en possession de l'hôpital, mais plutôt un échantillon de tissu appartenant au père défunt du plaignant (en particulier, un « fragment de tissu inclus dans de la paraffine » et/ou un échantillon sanguin.)

Inspections

Les activités d'inspection menées par la *Garante* ont été renforcées en 2007, en partie conformément au programme semestriel d'inspections mis au point par l'APD.

Dans le cadre de ces inspections, la *Garante* peut également s'adjoindre les services d'un corps spécialisé au sein de la police financière (*Guardia di Finanza*), chargé de vérifier le respect des exigences en matière de notification, d'avis et de mesures de sécurité et l'application des résolutions adoptées par la *Garante*. Au

total, 452 inspections ont ainsi été effectuées en 2007. La plupart concernaient des entités privées et avaient pour objectif de s'assurer du respect des principales dispositions prévues par la législation en matière de protection des données. Le service des inspections de la *Garante* s'est penché, plus particulièrement, sur le traitement des données personnelles (médicales) par des sociétés pharmaceutiques et des établissements de soins de santé ; le traitement en ligne de donnés personnelles ; le traitement ayant pour finalité la fourniture de biens et de services par le biais de mécanismes de vente à distance (y compris les centres d'appel) ; les opérations de traitement effectuées par le département des recettes ; la conservation par les opérateurs télécoms des données des utilisateurs ou abonnés ainsi que les services de banque en ligne.

Ces inspections ont débouché sur 228 procédures de sanction administrative. Dans 15 cas, on a préféré porter plainte auprès des autorités judiciaires. Ces infractions pénales concernaient le non-respect des résolutions adoptées par la *Garante*, la non-application de mesures minimales de sécurité et la transgression de l'interdiction de contrôle à distance du personnel. Les sanctions administratives infligées devraient rapporter au minimum 725 000 euros de recettes.

Il convient également de mentionner les activités spécifiques réalisées par l'APD italienne dans le cadre de conventions et accords internationaux, et en particulier celles en rapport avec le fonctionnement des bases de données du Système d'information Schengen et d'Eurodac.

Secteur public

Données biométriques. L'APD a autorisé un organisme public (office du superintendant du patrimoine archéologique) à utiliser le contrôle du contour des mains afin de permettre aux employés d'avoir accès à une zone de haute sécurité. Le système que l'office entend déployer reposera uniquement sur les caractéristiques géométriques des mains des membres du personnel, à l'exclusion de toute autre donnée biométrique. Le contour de la main sera associé à un algorithme de codage et conservé dans la mémoire interne du système. Ce système opérera exclusivement en mode local, à l'aide d'un mot-clé digital que chaque employé devra sélectionner et saisir lui-même. L'APD a estimé que cette procédure était licite et proportionnée. Si les informations renseignées par le contour de la main ne permettent pas l'identification unique, comme c'est le cas, par exemple, pour les empreintes digitales, elles sont suffisamment détaillées pour être utilisées dans des situations particulières demandant un contrôle de l'identité.

Questions en rapport avec l'emploi. Des lignes directrices ont été publiées sur le traitement des données à caractère personnel des salariés du secteur public. Elles ont trait au traitement des données médicales des employés du secteur public, à la collecte d'empreintes digitales pour l'accès au lieu de travail et à la diffusion de données sur Internet.

Autorités locales. L'APD a publié des lignes directrices sur le traitement des données personnelles aux fins de la publication et de la diffusion de documents par les autorités locales. Des garanties spécifiques ont été mises en place en ce qui concerne les données relatives aux personnes citées, par exemple, dans les décisions et résolutions du tableau d'affichage municipal, dans des documents accessibles au public ou dans des documents postés sur Internet, et ce de manière à tenir dûment compte du principe de transparence.

Établissements scolaires. L'APD a apporté la clarification suivante : les parents sont autorisés à filmer et à photographier leurs enfants participant à des spectacles scolaires, car les images et photos en question ne sont pas destinées à être diffusées en dehors du cercle familial et amical. En coopération avec le ministère de l'éducation, l'APD a également préparé des lignes directrices relatives à l'utilisation des vidéophones par les étudiants ou élèves des établissements scolaires.

Soins de santé

- L'APD italienne a ordonné aux agences locales de soins de santé ne pas inclure d'informations relatives au diagnostic médical sur les certificats d'incapacité de travail délivrés à des personnes devant s'inscrire au chômage ou qui sont exemptées du paiement des frais de scolarité ou du minerval.
- L'APD a aussi interdit la diffusion des noms de 4 500 patients ainsi que des informations sur leur état de santé sur le site Internet d'une région italienne.

- L'APD a clarifié que les autorités municipales locales ne peuvent demander aux médecins de leur communiquer le nom ou d'autres éléments d'information permettant d'identifier les patients auxquels ils rendent visite à domicile.
- Une inspection a été ordonnée par l'APD et réalisée par celle-ci avec le concours de la Police financière à la suite de reportages diffusés dans les médias indiquant que des centaines de dossiers médicaux avaient été retrouvés dans une décharge. Une information judiciaire a été lancée à l'encontre des responsables de la collecte de données qui s'étaient révélés incapables de prendre un minimum de mesures de sécurité.
- L'APD a demandé à un organisme public de ne faire aucune référence aux pathologies dans les formulaires de virement, en particulier dans le cas de patients séropositifs. L'Autorité a recommandé l'inclusion d'une formulation générale et/ou de codes numériques.
- L'Autorité a publié et diffusé un prospectus (« Protection des données personnelles: du côté du patient ») afin de sensibiliser les citoyens à l'importance de la protection des données dans les opérations de traitement de données effectuées par le personnel médical, les organismes de soins de santé et/ou les laboratoires médicaux. Cette brochure contient des informations succinctes sur les droits des patients en matière de protection des données à caractère personnel et sur les mécanismes destinées à les faire respecter.

Traitement des données génétiques.
Le traitement de données génétiques suppose l'autorisation *ad hoc* de la *Garante* (après consultation avec le ministère de la santé qui recherchera, à cette fin, l'avis du Conseil supérieur pour les soins de santé) et, en règle générale, également le consentement écrit de la personne concernée.

L'autorisation générale émise par la *Garante* en février 2007 afin de permettre ce type de traitement a comblé un vide juridique majeur. Elle s'applique à différentes catégories de responsables du traitement des données, essentiellement aux fins de la fourniture de soins de santé et de la réalisation d'activités de recherche scientifique. L'APD s'est également intéressée à la question de l'utilisation des données génétiques afin de faciliter le regroupement familial.

Après avoir défini les principaux concepts (données génétiques, échantillon biologique, test génétique), le document de l'APD énumère les entités autorisées à traiter les données génétiques aux fins spécifiées dans les cas individuels (praticiens des soins de santé, organismes publics et privés de soins de santé, laboratoires de génétique médicale, personnes physiques et/ou morales à des fins de recherche scientifique). L'autorité a réaffirmé le principe selon lequel les données génétiques ne peuvent être traitées qu'à ces fins et uniquement si ce traitement est réellement indispensable et a rappelé la nécessité d'obtenir le consentement écrit de la personne concernée. Cette règle n'admet comme exception que le cas où ces données génétiques sont nécessaires pour protéger l'identité génétique d'un tiers appartenant à la même lignée génétique que la personne concernée (en vue d'un choix de conception ou d'un traitement) et où le consentement ne peut être obtenu pour des motifs précis (incapacité légale, handicap physique ou mental) et le cas où des enquêtes statistiques sont en cours ou de la recherche est prévue par la loi.

Les contrôleurs de données doivent remplir des certaines obligations, qui sont particulièrement strictes en ce qui concerne les avis informatifs. Le conseil génétique est obligatoire si ces données sont traitées à des fins de soins de santé ou de réunification familiale, tant avant que pendant le test génétique. Les dispositions spécifiques relatives au traitement devront être respectées et des mesures strictes de sécurité adoptées – y compris le stockage et la communication sous forme d'un code des données génétiques et la séparation des données génétiques et des données d'identification.
La période de conservation des données en question ne pourra excéder la période absolument nécessaire. Enfin, ces données génétiques ne pourront être diffusées.

Secteur privé
L'APD a consenti de réels efforts en 2007 afin de simplifier l'application de la législation sur la protection des données dans le secteur privé.

Transfert massif de dettes et titrisation
Une décision (publiée au Journal officiel italien des lois et des règlements) a permis de traiter plusieurs demandes introduites auprès de l'Autorité de protection des données pour que les contrôleurs de données

soient exemptés de communiquer aux personnes concernées des informations sur les transferts massifs de dettes et / ou la titrisation. Ces opérations entraînent en effet la divulgation, par le cédant au cessionnaire, de données personnelles relatives aux débiteurs. En vertu du Code de protection des données, l'APD pourra donc, dans des cas précis, exempter le contrôleur de données de ses obligations d'information, à condition que le traitement en question fasse l'objet d'une publicité adéquate, conformément aux mécanismes que l'APD devra mettre en place. L'APD italienne a estimé que la communication d'informations aux personnes concernées (les débiteurs) entraînait dans ce cas un effort disproportionné et a donc décidé que les contrôleurs de données seraient exemptés des obligations qui s'appliquent mais à deux conditions : un avis informatif complet doit être publié dans le Journal officiel au plus tard au moment où le transfert a lieu, et il faut notifier individuellement aux débiteurs que le cessionnaire s'est procuré leurs données personnelles auprès de tiers, et ce à la première occasion après le transfert (par exemple au moment de l'envoi du relevé bancaire ou lors d'une demande de paiement).

Lignes directrices pour le contrôle de l'utilisation de la messagerie électronique et de l'Internet

L'APD a publié une décision générale (datée du 1er mars 2007) applicable au contrôle de l'utilisation de la messagerie électronique et de l'Internet par les employeurs du secteur public comme du secteur privé. Cette décision a été rendue à la lumière à la fois de la jurisprudence de la CEDH (affaire Copland c. Royaume-Uni) et de la position du Groupe de travail « Article 29 ». Conformément au cadre constitutionnel italien, les employeurs sont tenus d'assurer à leurs salariés un niveau raisonnable de respect de la vie privée de façon à leur permettre leur épanouissement personnel. Les lignes directrices de l'APD ont donc tenté de concilier les intérêts des deux parties en réaffirmant, d'une part, le droit de l'employeur à fixer les conditions de l'utilisation du matériel informatique mis à la disposition du personnel – y compris en prévoyant des mesures disciplinaires proportionnées – et, d'autre part, le droit des salariés à faire l'objet de contrôles proportionnés et à être informés de manière appropriée du traitement de données personnelles les concernant, ce traitement devant être réduit au minimum. Des recommandations et des interdictions particulières ont été mises en place, parmi lesquelles la nécessité, pour les employeurs, d'adopter une politique interne adaptée à la taille de l'entreprise et d'informer de manière appropriée les membres du personnel des conditions régissant l'utilisation du courrier électronique, de l'Internet et des autres outils électroniques. Les employeurs doivent également spécifier si des contrôles sont effectués et dans quelle mesure et, en ce qui concerne spécifiquement l'Internet, déterminer les catégories de sites Internet jugés en rapport avec le contexte de l'emploi et déployer des mécanismes de configuration et/ou des filtres en vue de prévenir certaines opérations (par exemple des téléchargements). En outre, des comptes partagés doivent être mis à la disposition des membres du personnel ainsi qu'un compte e-mail *ad hoc* pour la réception des e-mails privés. Les membres du personnel doivent par ailleurs être invités à désigner un tiers de confiance (par exemple un autre salarié) et lui autoriser l'accès à leur courrier électronique ainsi que le transfert de certains messages en cas d'absence. L'autorité a interdit toute initiative de l'employeur visant à contrôler le personnel à distance. Dans le cas où des exigences de contrôle sont motivées par la production, l'organisation ou la sécurité sur le lieu de travail, l'accord des syndicats doit être obtenu, comme le prévoient d'ailleurs d'autres textes de loi. Soucieuse de concilier les intérêts des deux parties, l'APD a estimé que des contrôles préventifs pouvaient être réalisés sans l'accord de l'employé, même à un stade précoce, c'est-à-dire indépendamment de l'existence ou de l'ouverture prévue d'une action en justice, mais à condition que toutes les garanties spécifiées ci-dessus aient été mises en place et que le contrôle soit proportionné compte tenu du contexte (par l'existence de risques sur le plan de la sécurité).

Mécanismes simplifiés de protection des données dans le secteur des assurances

L'APD italienne a autorisé les compagnies d'assurances à mettre en place une nouvelle procédure, simplifiée, pour informer leurs clients du traitement de leurs données personnelles. L'Autorité a ici tenu compte de l'expérience accumulée au cours de ces dernières années dans le cadre de la « chaîne de l'assurance » qui inclut plusieurs parties prenantes comme les coassureurs et les sociétés de réassurance.

Concrètement, il a été décidé que l'avis d'information devra être fourni une fois pour toutes par la compagnie d'assurance qui conclut le contrat avec le particulier. La compagnie d'assurance sera donc tenue d'informer le client de toute utilisation ultérieure ou prolongée de ses données personnelles – en mentionnant aussi les objectifs du transfert de données et les bénéficiaires – au nom également des autres entités de la « chaîne de l'assurance » qui n'ont souvent pas de contacts directs avec les personnes concernées, même si elles sont autorisées à traiter les données personnelles recueillies auprès de la compagnie d'assurance. L'APD a prévu des garanties spécifiques afin de permettre aux entreprises d'utiliser ces mécanismes d'information simplifiés. La compagnie d'assurance devra ainsi informer les clients sur les entités traitant leurs données à caractère personnel dans le cadre de contrats. Une liste, de ces entités, régulièrement mise à jour devra être postée sur le site Internet de la compagnie d'assurance, entre autres pour faciliter l'exercice des droits d'accès par les personnes concernées. Tout objectif poursuivi par les entreprises/entités en question autre que ceux en rapport avec la gestion du risque devra être spécifié dans l'avis d'information. Enfin, les exigences particulières en matière de consentement devront être respectées chaque fois que le consentement est nécessaire – ce qui n'est pas souvent le cas –, par exemple parce que les données du client sont indispensables pour la conclusion et le respect du contrat.

L'APD a rappelé en particulier que le traitement des données des clients à des fins de marketing exigeait leur consentement approprié et que les données sensibles (y compris les données médicales) ne pouvaient être traitées par les compagnies d'assurance qu'avec le consentement écrit du client.

Lignes directrices pratiques pour les PME
L'APD italienne a publié des lignes directrices tenant compte des besoins spécifiques des PME en matière de protection des données. Partant du constat que certaines exigences prévues par la législation relative aux données personnelles sont parfois considérées comme pesantes, en particulier pour les PME, et afin de promouvoir l'idée selon laquelle la protection des données peut devenir un atout commercial majeur – en améliorant la confiance des consommateurs et des utilisateurs –, l'APD a ainsi doté les PME d'un outil susceptible de faciliter le respect de ces exigences tout en les sensibilisant aux procédures simplifiées disponibles.

Ces lignes directrices clarifient les principales obligations applicables à toute entité traitant des données à caractère personnel ainsi que les concepts de base en matière de protection des données (contrôleur de données ; avis d'information ; consentement et mécanismes garantissant le consentement éclairé, en particulier pour le traitement de données sensibles). En outre, elles exposent clairement les cas dans lesquels une notification à l'APD s'impose ainsi que les mesures de sécurité que doit prendre une entreprise se livrant à des activités commerciales courantes. Les lignes directrices décrivent aussi les possibilités existant actuellement pour les flux de données transfrontaliers, y compris l'utilisation de clauses contractuelles standard. Une liste de contrôle est par ailleurs proposée pour aider les entreprises à vérifier si toutes les mesures ont été prises pour garantir le respect des dispositions légales.

Utilisation des données des clients par les centres d'appel et les opérateurs télécoms (services passifs et actifs)
Des contrôles approfondis réalisés aux quatre coins de l'Italie (avec l'aide de la police financière) auprès des principaux opérateurs téléphoniques et centres d'appel ont mis en évidence plusieurs cas de traitement illégal des données personnelles ainsi que l'existence de pratiques de traitement déloyales. En juin 2007, la *Garante* a rendu cinq décisions exposant des mesures à mettre en place par certains des principaux opérateurs téléphoniques et centres d'appel afin de garantir le respect du droit à la vie privée et d'autres droits des utilisateurs. Les opérateurs télécoms et les centres d'appel fournissant des services actifs doivent ainsi mettre fin à toutes leurs activités illégales de traitement des données (visant en particulier l'activation de services non sollicités comme des connections Internet à grande vitesse) et informer la *Garante* des mesures prises pour mettre en œuvre les dispositions organisationnelles, techniques et de procédures de ces décisions (avis d'information aux utilisateurs et obtention de leur consentement préalablement à l'utilisation de leurs données à des fins publicitaires ; respect de la transparence lors du premier contact avec

les utilisateurs quant à la source de leurs données et aux mécanismes d'utilisation ; prise en compte du refus de l'utilisateur de tout contact ultérieur ; contrôles des activités dans les centres d'appel désignés responsables du traitement des données). En cas de non-respect de ses prescriptions, la *Garante* se réservait le droit de prendre des mesures plus sévères, comme le blocage ou l'interdiction d'activités de traitement de données.

En ce qui concerne spécifiquement les services passifs, des procédures simplifiées ont été mises en place en décembre 2007, en partie sur base des conclusions des inspections précitées. L'APD a précisé que les centres d'appel de type passif n'étaient pas tenus d'informer les clients du traitement de leurs données personnelles, sauf si les données collectées par l'opérateur prenant l'appel devaient être utilisées à d'autres fins (par exemple marketing), auquel cas le consentement éclairé de la personne devra être obtenu.

Médias

En 2007, la *Garante* s'est intéressée à diverses questions en rapport avec la protection des données et le journalisme. Dans le domaine du « journalisme judiciaire », l'APD a estimé que la publication, par certains médias, de transcriptions (y compris la transcription d'écoutes téléphoniques) provenant d'enquêtes judiciaires en cours violait la législation relative à la protection des données. Celles-ci contenaient en effet des données personnelles (dont certaines relevant de la vie sexuelle), et leur diffusion ne respectait pas le principe selon lequel les informations publiées doivent être « d'intérêt public ». Ce principe est actuellement aussi inscrit dans le Code de pratique pour le traitement des données personnelles par les journalistes. Dans d'autres cas, l'APD a montré que des données à caractère personnel avaient été recueillies de manière illicite et en violation du principe de l'équité – c'est notamment le cas de photos prises de manière importune ou de vidéos enregistrées à l'insu des personnes concernées. À noter que le traitement en question violait également les obligations d'équité et de transparence exposées dans le Code de pratique des journalistes précité. Dans une affaire concernant la publication d'informations sur une dame décédée d'une grave maladie, divulguant un nombre excessif d'éléments d'identification, l'APD a estimé que les garanties inscrites dans le Code sur la protection des données et le Code de pratique des journalistes avaient été violées étant donné qu'elles s'appliquaient également à la défunte. Pour terminer, il convient de faire référence à la protection spéciale dont bénéficient les enfants au titre du Code dans le domaine des médias et du journalisme. Un code de bonnes pratiques (Charte de Trévise) a en effet été adopté à cette fin il y a quelques années par l'Association des journalistes italiens. Ce code a ensuite été adopté par l'autorité italienne de protection des données. De nombreuses affaires étaient en rapport avec la publication de données permettant l'identification – inutile – d'enfants impliqués dans des litiges (séparation, divorce) ou dans des procédures pénales en rapport avec des abus sexuels.

Lettonie

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La directive 95/46/CE a été transposée dans le droit national par la loi sur la protection des données à caractère personnel qui est entrée en vigueur le 20 avril 2000 et dont les derniers amendements remontent à 2007. Un projet de loi relatif à l'Inspection nationale des données a été élaboré en vue de garantir l'indépendance totale de l'inspection. Le projet de loi sera soumis au gouvernement letton d'ici la mi-2008.

Amendements à la loi relative sur les données à caractère personnel

La loi sur la protection des données à caractère personnel a été amendée le 1er mars 2007, entres autres afin de déterminer les dérogations à l'obligation de notification et de simplifier la procédure de notification du traitement des données à caractère personnel. Les modifications sont les suivantes :

1. les dérogations à la notification ont été précisées ;
2. ce ne sont plus les systèmes de traitement des données personnelles qui reçoivent les notifications, mais les contrôleurs de données ;
3. un institut des responsables de la protection des données à caractère personnel est mis en place ;
4. les conditions pour les transferts de données à caractère personnel vers les pays tiers ont été spécifiées et des projets de règlement du Cabinet ministériel ont été élaborés pour prendre en compte cette modification.

Règlements du Cabinet ministériel

En ce qui concerne les amendements à la loi sur la protection des données à caractère personnel, l'Inspection nationale des données a rédigé plusieurs projets de règlement du Cabinet ministériel :

- Accréditation de contrôleurs des données personnelles ;
- Amendements aux exigences organisationnelles et techniques en matière de protection des données à caractère personnel ;
- Conditions pour la formation des responsables de la protection des données ;
- Norme à respecter pour les autorisations de transferts de données à caractère personnel vers des pays tiers.

Amendements au droit pénal

Afin de faciliter la protection du traitement des données à caractère personnel et de prévenir tout traitement illégal de ces données, des travaux législatifs ont démarré, l'objectif étant d'engager la responsabilité pénale en cas de violations en matière de traitement des données à caractère personnel. Les projets d'amendements ont été soumis au Parlement en 2007.

Le projet de loi instaure la responsabilité pénale en cas de traitement illicite de données à caractère personnel lorsqu'il en découle un préjudice important et que le traitement illicite a été motivé par un désir de vengeance, l'exercice d'un chantage ou d'autres intentions malveillantes ou s'il s'accompagne de violence, de fraude ou de menaces ; en cas de non utilisation des moyens techniques et organisationnels requis pour protéger lesdites données à caractère personnel et prévenir le traitement illicite de celles-ci – manquement ayant entraîné un préjudice substantiel – ainsi qu'en cas de préjudice substantiel suite au traitement illicite de données à caractère personnel.

La responsabilité administrative est aujourd'hui engagée en cas de violation des dispositions relatives au traitement des données personnelles. Les contrevenants s'exposent à des avertissements, amendes, suspension du traitement des données à caractère personnel et confiscation des moyens techniques utilisés.

Règlements relatifs à la conservation des données aux fins de l'application de la loi

La directive 2002/58/CE a été transposée dans la législation nationale par la loi sur les communications électroniques.

En vue de son application, le Cabinet des ministres a publié, le 4 décembre 2007, le règlement n° 820 « Conditions imposées aux demandes d'information émanant d'institutions chargées de l'instruction préparatoire, de personnes faisant l'objet d'une enquête, de la sécurité de l'État, de procureurs et de tribunaux ainsi que sur le transfert de données conservées par les fournisseurs de services de communications électroniques, ainsi que l'ordonnance relative à la façon de résumer les informations statistiques sur les données demandées et à la façon de les soumettre. » Depuis 2007, l'Inspection nationale des données est ainsi

mandatée pour résumer les statistiques relatives à la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou d'un réseau public de communications et dont le traitement a été assuré par des fournisseurs de services de communications électroniques, conformément à l'article 19 de la loi sur les communications électroniques et à l'article 10 de la directive 2006/24/CE *sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications modifiant la directive 2002/58/CE*.

B. Jurisprudence

En 2007, les plaintes reçues par l'Inspection nationale des données faisant état de violations à la loi sur la protection des données à caractère personnel ont eu trait surtout à des traitements de données ne reposant sur aucune base légale.

Violations les plus fréquentes des dispositions relatives au traitement des données à caractère personnel mises en évidence en 2007 :

1) traitement incorrect et souvent explicitement illicite de données personnelles dans le cadre des procédures de recouvrement de créances et d'arriérés de paiement (listes noires) et publication de données à caractère personnel des services d'entretien et de rénovation;
2) violation des droits des personnes concernées à l'accès à l'information – non-communication d'informations aux personnes concernées et refus de communication des informations, y compris la non-information d'une procédure de vidéosurveillance;
3) violation du principe de proportionnalité dans le traitement de données personnelles, le traitement allant au-delà de l'objectif initial du traitement des données, ainsi que la photocopie de passeports.

C. Questions diverses importantes

En 2007, 120 plaintes ont été soumises à l'Inspection nationale des données. Les contrôles menés en 2007 dans le domaine de la protection des données à caractère personnel ont mis en évidence, dans 30 cas, un non-respect de la loi. Les plaintes avaient trait, pour la plupart, à l'absence de base légale au traitement de données à caractère personnel (50 % des infractions en 2007) ainsi qu'à la violation des droits des personnes concernées (articles 10 et 11 de la directive 95/46/CE) et la violation du principe de proportionnalité dans le traitement des données.

Aucune des décisions de l'Inspection nationale des données n'a été annulée par le tribunal et les appels interjetés ont tous été rejetés.

Contrôle du spam

Conformément à la loi relative aux services de la société d'information, l'Inspection nationale des données, depuis le 1er juin 2007, surveille les spams sur le plan des violations de la protection des données à caractère personnel.

En 2007, l'Inspection nationale des données a rendu une première décision, interdisant l'envoi de courriels publicitaires non sollicités (article 13 de la directive 2002/58/CE).

Liberté d'information et protection des données

L'accès aux informations relatives aux travaux d'entretien et aux installations réalisés par une agence publique dans l'appartement de l'ancien président de Lettonie a fait l'objet d'un débat. Cet appartement allait être mis à la disposition de l'ancien président au terme de son mandat.

L'Inspection nationale des données a estimé que, comme les installations et les travaux d'entretien avaient été financés par les deniers publics, les informations relatives au coût des travaux étaient publiques et qu'il ne devait donc y avoir aucune restriction à l'accès à celles-ci.

Une autre affaire concernait un magazine qui avait publié certaines données sensibles dans le domaine de la santé (radiographie). L'Inspection nationale des données a estimé que des données médicales sensibles ne devaient pas être publiées dans un magazine à sensation sans l'accord de la personne concernée et que ce magazine avait donc enfreint la loi sur la protection des données à caractère personnel ainsi que la loi relative à la presse et aux médias qui interdit

la publication dans les médias de données relatives à la santé.

Système d'information Schengen (SIS)

Avant que la Lettonie ne rejoigne l'espace Schengen en décembre 2007, l'Inspection nationale des données était chargée de procéder à des contrôles auprès des institutions et des autorités qui allaient avoir accès au Système d'information Schengen (SIS). L'état de préparation de ces institutions a été évalué, et des discussions ont eu lieu sur la façon de faire appliquer le droit des personnes concernées en ce qui concerne l'accès au SIS.

La loi lettone sur le SIS est entrée en vigueur en 2007. Elle intègre les exigences en matière de protection des données à caractère personnel. L'Inspection nationale des données a également participé à la rédaction des règlements du Cabinet ministériel relatifs au traitement des données à caractère personnel et au droit des personnes concernées à demander la communication des informations recueillies à leur sujet et/ou l'ajout, la rectification ou la suppression de ces données personnelles du SIS.

L'Inspection nationale des données a par ailleurs produit la brochure intitulée « Les données à caractère personnel dans le Système d'information Schengen ». Une brochure similaire a été publiée en anglais et en russe en coopération avec le Commissaire slovène à l'information.

Recherche dans des domaines particuliers intéressant la protection des données personnelles

L'Inspection nationale des données a organisé des séminaires sur la protection des données dans les écoles, l'un à l'attention des directeurs d'école et l'autre pour les enseignants. Suite à cette activité, l'Inspection nationale des données personnelles a décidé de faire de la protection des données dans les écoles sa priorité de recherche pour 2008.

Lituanie

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

1. Le 19 décembre 2006, le Seimas de la République de Lituanie (le Parlement) adoptait un amendement à la loi sur les documents et les archives (entrée en vigueur le 11 janvier 2007), en vertu de laquelle l'accès aux documents de la partie spéciale du Fonds documentaire national n'est pas limité. Cette partie spéciale du Fonds documentaire national comprendra les rapports d'activité de divers organismes : les structures de l'opposition (résistance) aux régimes d'occupation de l'URSS et de l'Allemagne, le Commissariat populaire aux affaires intérieures de la République socialiste soviétique (RSS) de Lituanie (de 1940 à 1941 et de 1944 à 1946), le Commissariat populaire à la sécurité de l'État de la RSS de Lituanie (en 1941 et de 1944 à 1946), le ministère en charge de la sécurité de l'État de la RSS de Lituanie (de 1946 à 1953), le ministère des affaires intérieures de la RSS de Lituanie (de 1946 à 1954), la Commission en charge de la sécurité de l'État de la RSS de Lituanie (de 1954 à 1991), le Commissariat populaire à la sécurité de l'État de l'URSS (NKGB), le ministère en charge de la sécurité de l'État de l'URSS (MGB), les divisions de la Commission en charge de la sécurité de l'État de l'URSS (KGB), qui ont opéré en Lituanie de 1940 à 1991, les divisions du Commissariat populaire aux affaires intérieures de l'URSS (NKVD) et le ministère des affaires intérieures de l'URSS (MVD), actifs en Lituanie de 1946 à 1954, les divisions du Commissariat populaire à la défense de l'URSS (NKO) et le Commissariat populaire (ministère) de la marine (NKVMF), actifs en Lituanie en 1941 et de 1943 à 1946, les divisions de la Direction des renseignements centraux du Personnel général de l'Armée soviétique (GRU) active en Lituanie de 1940 à 1991, le parti communiste lituanien ainsi que des structures dépendant de ces organisations.

Toute personne souhaitant prendre connaissance de ces documents doit en faire la demande par écrit à l'organisme concerné, en joignant à sa requête un document attestant de son identité. Nul n'est tenu de motiver la raison pour laquelle il souhaite avoir accès aux documents. L'accès n'est autorisé qu'à l'intérieur des locaux du conservateur des documents. L'amendement à cette loi limite également l'accès aux documents contenant des informations relatives à des personnes ayant reconnu avoir collaboré en secret avec les agences de renseignement de l'URSS et qui figurent dans les fichiers des personnes ayant reconnu cette collaboration, ainsi qu'aux documents relatifs à des personnes ayant souffert des agences de renseignement de l'URSS et qui souhaitent un accès limité aux données les concernant, et ce jusqu'à leur décès.

2. Le 3 avril 2007, le Seimas de la République de Lituanie a adopté un amendement à la loi relative au registre des résidents. Aux termes de l'amendement, les données relatives aux liens de parenté et aux liens de parenté par alliance (belle-soeur, beau-frère) pourront être communiquées, en de rares occasions et à condition que l'objectif de l'utilisation de ces données soit spécifié au personnel des autorités en charge du respect de la loi et aux commissions du Seimas, et ce pour leur permettre d'exercer leur mission conformément à la procédure légale, consignée dans les résolutions du Seimas. L'amendement stipule également que les données relatives à ces liens pourront être communiquées au responsable de la Commission d'éthique dans le cadre de l'exercice direct de ses fonctions ; aux notaires dans le cadre des affaires de succession qu'ils ont à traiter et pour leur permettre de déterminer s'il existe des dispositions légales limitant la conclusion d'accords entre proches du défunt ; aux personnes autorisées par la loi à examiner des affaires en rapport avec la citoyenneté de la République de Lituanie aux fins de statuer sur celles-ci.

3. Le Bureau de protection des données a publié des Règles relatives au traitement des données à caractère personnel dans les établissements scolaires, règles qui ont été approuvées par le décret n° 1T-45 du 4 juillet 2007 du directeur du Bureau. Ces Règles relatives au traitement des données personnelles dans les écoles ont pour objectif de réglementer le traitement des données personnelles dans les écoles afin de garantir le respect et la mise en œuvre de la loi sur la protection des données à caractère personnel de la République de Lituanie, ainsi que d'autres lois et décrets régissant le traitement et la protection des données à caractère personnel.

B. Jurisprudence

Arbre généalogique

Lors qu'il a eu à examiner une plainte individuelle, le Bureau de protection des données a constaté que des officiers de police avaient vérifié les données personnelles et dressé l'arbre généalogique du requérant, alors détenu pour contravention au code de la route, aux fins de révéler l'identité de cette personne. Les données relatives aux liens de parenté du requérant avaient été imprimées et jointes au dossier de contravention au droit administratif, afin de prouver que ce délit administratif avait bien été commis par cette personne. Le Bureau de protection des données a ordonné à la Direction de la police de révoquer la mesure relative au logiciel permettant (autorisant) l'association de données personnelles figurant dans le registre des résidents et la réalisation de l'arbre généalogique des personnes. Les fonctions du moteur de recherche en ligne sont en effet légalement non fondées et ne respectent dès lors pas l'article 3, partie 1 (2) de la loi relative à la protection légale des données à caractère personnel de la République de Lituanie.

La Direction de la police a interjeté appel contre la décision du Bureau de protection des données, arguant que ce logiciel de recherche en ligne était nécessaire à l'exercice des compétences lui ayant été confiées par la loi sur les activités de police de la République de Lituanie, et à la mise en œuvre des dispositions de la loi sur la prévention du crime organisé, de la loi sur les activités opérationnelles et de la loi sur le contrôle des armes et des munitions de la République de Lituanie.

Dans ses conclusions, le Tribunal administratif de district de Vilnius a affirmé que l'utilisation de ce logiciel respectait le critère de traitement licite des données à caractère personnel établi par l'article 5, partie 1 (6) de la loi relative à la protection légale des données à caractère personnel de la République de Lituanie. En l'espèce, le logiciel permettant d'associer les données du registre des résidents et la réalisation d'un arbre généalogique était nécessaire à la poursuite d'intérêts légitimes, pour permettre à la police de réaliser les tâches qui lui sont confiées par la loi. Le tribunal a donc reconnu ici que les intérêts de la personne intéressée n'étaient pas prépondérants. Le tribunal a donc ordonné l'annulation de la décision du Bureau de protection des données.

Appel a ensuite été interjeté devant le Tribunal administratif suprême de Lituanie contre la décision du tribunal administratif du district de Vilnius.

Le Tribunal administratif suprême de Lituanie a conclu que la Direction de la police ne s'était pas contentée de recueillir et de traiter des données personnelles mais qu'elle avait également intégré des arbres généalogiques dans la base de données des infractions au code de la route. Une partie des données recueillies et traitées concernait non seulement le contrevenant au code de la route et les membres de sa famille, mais également des proches des grands-parents, oncles, tantes, sœurs, frères, cousins et enfants des cousins du contrevenant. Par ailleurs, aucune période de conservation n'avait été fixée. De plus, aucun texte de loi ne stipule que l'arbre généalogique des contrevenants au code de la route doit ou peut être intégré dans la base de données des infractions de roulage. Les personnes concernées ne sont pas informées de cette forme de traitement de leurs données personnelles. Le tribunal a estimé que l'établissement de l'arbre généalogique de contrevenants au code de la route impliquait ici le traitement de données relatives à un certain nombre d'autres personnes n'étant pas impliquées dans l'infraction de roulage et qu'il ne relevait pas des dispositions de l'article 5 (1) de la loi sur les activités de police de la République de Lituanie, de l'article 7, partie 1 (11) de la loi sur les activités opérationnelles, ni de l'article 17, partie 1 (9) de la loi sur le contrôle des armes et des munitions de la République de Lituanie. Les données obtenues par composition d'un arbre généalogique ne peuvent être traitées qu'à propos d'une personne faisant l'objet d'une enquête opérationnelle et non à propos de quelqu'un qui n'a pas respecté le code de la route. Le tribunal a reconnu comme valable la décision du Bureau de protection des données.

Présence de documents bancaires dans des sacs poubelles

Le Bureau de protection des données a reçu un courrier électronique l'informant que des documents bancaires contenant des données personnelles et des copies de

documents d'identité avaient été trouvés dans des sacs poubelles à proximité d'une banque.

Une inspection effectuée dans les locaux de la banque en vue de déterminer le caractère licite du traitement des données à caractère personnel a montré que les documents trouvés dans des sacs poubelles à proximité de la banque n'avaient pas été correctement détruits, de même que les photocopies des documents contenant des données personnelles. Les documents et les photocopies avaient été détruits sans rendre impossible l'identification des données personnelles, et il était donc encore possible d'identifier une personne physique à partir des données personnelles figurant encore sur des morceaux de documents et des photocopies. Cette inspection a permis d'établir que la banque, sur la base des exigences de l'article 24 (1) de la loi relative à la protection légale des données personnelles de la République de Lituanie, avait mis en œuvre les mesures organisationnelles et techniques appropriées en vue de protéger les données personnelles de toute destruction, altération ou divulgation accidentelle ou illicite, ainsi que de tout autre traitement illicite. Toutefois, durant le traitement des données à caractère personnel, et plus précisément au moment de détruire les documents et photocopies de documents contenant des données personnelles qui n'étaient pas nécessaires à la poursuite de leur travail, les employés X n'ont pas opéré de façon à rendre impossible l'identification des informations personnelles. Comme la destruction des documents n'avait pas été réalisée correctement, des données personnelles ainsi que des photocopies de documents contenant des données personnelles jetés dans les poubelles sont devenus accessibles à des tiers. Les données personnelles figurant encore sur les morceaux de documentes détruits et les photocopies permettaient d'identifier les personnes physiques, auxquelles ces documents appartenaient, ce qui était contraire à la loi relative à la protection légale des données personnelles de la République de Lituanie ou tout autre texte de loi. Au moment du traitement des données personnelles, les employés X de la banque n'ont pas préservé la confidentialité des données personnelles et ont ainsi violé l'article 24 (5) de la loi relative à la protection légale des données personnelles de la République de Lituanie. Les employés X ont donc été sanctionnés administrativement. Dans son jugement, le Tribunal de première instance a confirmé les délits administratifs dans le chef des employés de la banque.

C. Questions diverses importantes

Traitement des données personnelles aux fins d'une campagne électorale

En 2007, lors de la campagne électorale pour l'élection des conseils municipaux, une série d'électeurs indignés ont contacté le Bureau de protection des données, affirmant que, pendant la campagne électorale, des électeurs avaient reçu des lettres leur demandant de voter en faveur du parti ou du candidat à l'origine de ce courrier. Suite à ces plaintes, le Bureau de protection des données a décidé d'enquêter sur la légalité du traitement des données à caractère personnel dans le cadre d'une campagne électorale et des données figurant sur les listes électorales, dans les partis, dans des organisations politiques et dans des syndicats.

La loi relative aux élections des conseils municipaux de la République de Lituanie stipule que les partis figurant dans le registre national des contrôleurs des données personnelles peuvent se procurer des listes électorales générales (sous format électronique ou en version papier) qui spécifient les nom, prénoms, adresse et date de naissance des électeurs. Si un électeur s'oppose à la mention de son adresse ou de sa date de naissance dans ces listes générales, comme la loi l'y autorise, seuls son nom et son prénom y figureront. La loi stipule en outre que les partis ne sont pas autorisés à soumettre des listes électorales à des tiers et à les utiliser à des fins autres que la campagne électorale. Les données obtenues doivent être détruites dans les 30 jours suivant la proclamation des résultats électoraux finaux.

Huit partis, qui envisageaient de traiter les données personnelles des électeurs aux fins de la campagne électorale, s'étaient inscrits au registre national des contrôleurs de données personnelles. Les inspections menées par le Bureau de protection des données ont révélé que deux des huit partis repris dans le registre n'avaient pas utilisé la possibilité qui leur avait été donnée de se procurer les registres électoraux.
Six partis ont reçu ces registres, mais quatre seulement ont envoyé des lettres personnalisées aux électeurs durant la campagne électorale.

Seulement un parti sur les six avait enfreint la loi sur la protection légale des données personnelles de la République de Lituanie. Diverses violations de cette loi ont été identifiées dans les cinq autres partis : pas de réglementation documentée pour les mesures organisationnelles et techniques destinées à protéger les données personnelles contre toute destruction, altération ou divulgation illicite ou accidentelle ainsi que contre tout autre traitement illicite ; absence de mesures visant à s'assurer que les données étaient bien exclusivement traitées par des personnes autorisées et que ces personnes avaient bien reçu l'instruction par écrit de préserver la confidentialité des données ; non transmission d'informations précises relatives au traitement des données personnelles au Bureau de la protection des données ; non-sélection de responsables appropriés pour le traitement des données, lesquels n'ayant pas été dûment autorisés à traiter les données personnelles. En outre la sécurité des données personnelles n'avait pas été assurée et aucune mesure technique appropriée de protection des données n'avait été prise pour assurer la destruction adéquate de toutes les données personnelles soumises aux responsables du traitement des données. Les partis ont été informés des violations à la loi sur la protection légale des données personnelles de la République de Lituanie qui avaient été identifiées.

Contrôles du traitement des données de vidéosurveillance dans des centres commerciaux

Le Bureau de protection des données a procédé, de sa propre initiative, à des contrôles dans quatre grandes surfaces afin de se rendre compte de l'importance du traitement des données de vidéosurveillance et de sa légalité. Des violations de la loi relative à la protection légale des données à caractère personnel de la République de Lituanie ont été mises en évidence dans tous ces centres commerciaux. Aucun supermarché n'avait notifié au Bureau de protection des données qu'il surveillait ainsi les visiteurs du centre commercial. Les trois contrôles effectués dans ces centres commerciaux ont révélé que la zone balayée par le dispositif de vidéosurveillance couvrait une superficie s'étendant au-delà de leur propriété (couvrant, par exemple des carrefours, maisons d'habitation, stations-service, distributeurs automatiques de billets, locaux loués à d'autres entités, etc.). Un volume excessif de données personnelles faisait donc l'objet d'un traitement.

Dans trois centres commerciaux, les visiteurs n'avaient nullement été informés qu'ils faisaient l'objet de contrôles par vidéosurveillance. Dans un centre commercial, les visiteurs en étaient informés aux entrées, mais ils devaient entrer dans la zone contrôlée pour pouvoir lire l'information (à savoir dans le parking). En outre, aucun document ne régissait le traitement des données personnelles obtenues par vidéosurveillance, les mesures de sécurité installées et la localisation de caméras de vidéosurveillance.

Dans un centre commercial, des photos de voleurs à l'étalage avaient été découvertes à proximité d'une caméra de vidéosurveillance, ainsi que les noms, photocopies de documents d'identité et photocopies de documents contenant des informations personnelles préparés par la police. Des photos de voleurs à l'étalage arrêtés et de leurs enfants ont été aussi trouvées près d'une autre caméra. Ces deux centres commerciaux ont affirmé que ces données étaient nécessaires à l'identification des coupables et à la prévention des vols à l'étalage dans le centre, indiquant qu'ils n'avaient pas l'intention de les rendre publiques ou de les diffuser à des tiers, et que ces données étaient uniquement accessibles au personnel de sécurité. Le Bureau de protection des données a estimé qu'une quantité excessive de données à caractère personnel était recueillie (photos d'enfants sans lien avec la prévention des vols ; codes d'identification personnelle, dossier des condamnations, état civil…) pour la prévention des vols à l'étalage. Les centres commerciaux ont reçu notification concernant les violations de la loi sur la protection légale des données personnelles de la République de Lituanie dont ils s'étaient rendus coupables.

Sensibilisation du public

1. Des événements marquant la Journée européenne de protection des données organisée par le Bureau de protection des données et le Centre d'information du Seimas sur l'UE ont eu lieu le 26 janvier 2007. Ces activités se sont déroulées dans le centre d'information de la Commission aux affaires européennes du Seimas de la République de Lituanie. Parmi celles-ci, nous retiendrons la conférence de presse « Protection des données à caractère personnel en Lituanie », une conférence intitulée « Protection des données à caractère personnel : problèmes et perspectives » et des discussions avec

des spécialistes du Bureau de protection des données. La conférence de presse et les présentations ont permis d'aborder des problématiques d'actualité, comme l'utilisation des données biométriques, la vidéosurveillance et la protection des données dans le domaine des communications électroniques. Au cours de cette journée, les experts du Bureau de protection des données ont pris part à des débats et ont proposé des consultations sur des questions en rapport avec la protection des données à caractère personnel.

2. En 2007, le Bureau de protection des données célébrait également son dixième anniversaire. Le 15 novembre 2007, à cette occasion, le Bureau a présenté un bilan de ces 10 années d'activités devant les institutions publiques du pays. Les 13 et 14 novembre 2007, c'est une conférence internationale qui était organisée autour du thème des tendances en matière de protection des données dans la société de l'information. La conférence a permis de sensibiliser le public à l'évolution rapide des technologies de l'information, à la rapidité de leur déploiement dans le pays, aux aspects positifs de cette évolution et aux mesures visant à prévenir la menace croissante que constitue le traitement des données personnelles pour le droit des personnes au respect de la vie privée. La menace en matière de respect de la vie privée suscite une réflexion croissante sur la façon de garantir la protection des données dans ce domaine. Les présentations organisées dans le cadre de la conférence ont abordé la question de l'identification personnelle dans l'environnement électronique et les services d'e-gouvernement ; la conservation des données conformément à la directive 2006/24/CE et la transposition de cette directive ; la protection du respect de la vie privée dans la publication des décisions de justice et des institutions publiques ; et le traitement des données personnelles des salariés et des données issues de la vidéosurveillance. La conférence a permis de nombreux échanges d'expériences, non seulement entre médiateurs des institutions publiques et privées du pays, mais aussi entre responsables de la protection des données et représentants d'instituts de protection des données d'autres pays.

Luxembourg

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (transposition de la directive 95/46/CE)

La loi du 27 juillet 2007 portant modification de la loi du 2 août 2002 est entrée en vigueur le 1er septembre 2007. L'objectif du législateur était de simplifier profondément certaines dispositions, jugées inutilement pesantes sur le plan administratif et n'apportant pas de valeur ajoutée tangible en matière de protection des personnes concernées. Les principales modifications concernent les aspects suivants :

- une réelle extension des cas d'« *exemption de notification* » conditionnelle en ce qui concerne des situations de traitement des données particulièrement courantes ;
- une extension des cas d'« *exemption de notification* » pour certaines professions ;
- la simplification du mode de nomination de la personne détachée à la protection des données, fonction pouvant désormais être exercée par un employé du responsable du traitement des données ;
- l'exclusion des personnes morales du champ d'application de la loi ;
- la modification de la définition de certains termes clés (à savoir les concepts de consentement, de données à caractère personnel, de surveillance, etc.) ;
- la modification des dispositions relatives au traitement de certaines catégories particulières de données ;
- l'introduction de motifs supplémentaires légitimant le traitement de données à des fins de surveillance ;
- la vidéosurveillance de tiers sans enregistrement d'images, qui est désormais exclue de l'« examen préalable » obligatoire (autorisation de la Commission nationale pour la protection des données, en abrégé CNPD).

Loi du 30 mai 2005 sur les réseaux et les services de communications électroniques (transposition de la directive 2002/58/CE)

La loi précitée du 27 juillet 2007 introduit également certains amendements à la loi du 30 mai 2005. Le législateur luxembourgeois a tenu à clarifier certaines dispositions du texte de loi initial afin de transposer avec plus de précision les dispositions de la directive 2002/58/CE. En outre, la période de conservation des données relatives au trafic a été explicitement réduite de 12 à 6 mois.

Règlements et législation secondaire

Le règlement grand-ducal du 12 juin 2007 fixe le mode d'établissement du répertoire des personnes morales prestataires de services conservé la Chambre de commerce luxembourgeoise. Ce règlement spécifie entre autres les catégories précises de données devant être conservées dans ledit répertoire.

Le règlement grand-ducal du 1er août 2007 autorise la création et l'exploitation par la police d'un système de vidéosurveillance dans des « *zones de sécurité* » publiques. Le règlement a mis en place de nombreuses garanties en vue de protéger les droits des personnes concernées. Il stipule ainsi entre autres que l'accès à ce système de surveillance est strictement contrôlé et que la durée de conservation des données ne peut excéder deux mois. Le règlement administratif du 27 septembre 2007 définit explicitement les zones considérées par la loi comme étant des « *zones de sécurité* » au sein desquelles le système de vidéosurveillance pourra être exploité.

Enfin, le règlement grand-ducal du 21 décembre 2007 fixe les montants et les modalités de paiement des redevances pour les notifications et les modifications de notifications à la CNPD.

Autres nouvelles mesures législatives

Le gouvernement a demandé à la CNPD de rendre un avis sur le projet de loi concernant la coopération administrative et judiciaire entre les administrations publiques. Dans ses recommandations initiales et de suivi, la CNPD a indiqué que la notion de « *rapprochement de données* » – telle qu'exposée dans le projet de texte législatif – ne respectait pas selon elle les dispositions de la loi 2002 et que ce type de traitement ne pouvait dès lors pas être considéré comme conforme à la loi. La CNPD a dès lors recommandé au législateur de revoir les définitions du projet de loi, d'introduire des garanties concernant des catégories spécifiques de données, de définir les différents types de coopération entre administrations et de mettre en place des garanties pour la confidentialité des données. Ces recommandations

de la Commission nationale ont été suivies par le gouvernement luxembourgeois.

La CNPD a également adressé au gouvernement des recommandations en ce qui concerne des thèmes d'actualité et des affaires en cours, comme les projets de législation concernant l'établissement d'un cadastre des loyers, la création et l'exploitation du système d'information général de la police, le projet de loi introduisant une nouvelle allocation en faveur des enfants et le projet de règlement grand-ducal déterminant les dix bases de données, gérées par des personnes morales publiques, auxquelles les magistrats et les officiers de police auront un accès direct.

B. Jurisprudence

Jurisprudence civile et pénale

Tribunal d'arrondissement de Luxembourg, Cour d'appel siégeant en 10e chambre correctionnelle sur la validité de la preuve (images de vidéosurveillance) recueillie en violation de la loi de 2002 relative à la protection des données.

La décision de la 9e chambre correctionnelle (du 13 juillet 2006) stipulant qu'en matière pénale, la preuve obtenue ou recueillie en violation de la loi de 2002 relative à la protection des données n'est pas recevable et doit donc être rejetée des débats a été confirmée le 28 février 2007 par la Cour d'appel siégeant en 10e chambre correctionnelle.

L'arrêt susmentionné de la Cour d'appel a ensuite été soumis à la Cour de cassation, qui a cassé la décision de la Cour d'appel. La Cour de cassation a invoqué l'article 6 de la Convention européenne des droits de l'homme, et plus particulièrement le droit à un jugement équitable. Après avoir énuméré les différentes hypothèses selon lesquelles un juge peut rejeter des débats une preuve illicite, la Cour a affirmé qu'un juge avait néanmoins le droit de déterminer l'admissibilité d'une preuve obtenue ainsi illégalement s'il tient compte de l'entièreté des éléments de l'affaire, y compris la méthode d'obtention de la preuve et les circonstances dans lesquelles l'acte illicite a été perpétré. Dans son arrêt, la Cour de cassation conclut que la Cour d'appel a refusé de manière péremptoire de prendre en considération tous les éléments de l'affaire et qu'elle a dès lors violé l'article 6 de la Convention européenne des droits de l'homme. La Cour de cassation a par conséquent cassé et annulé le jugement et renvoyé l'affaire devant une nouvelle Cour d'appel.

Le 28 février 2008, une nouvelle Cour d'appel a déclaré que la production d'une preuve obtenue de manière illicite (*c'est-à-dire sans l'autorisation préalable de la CNPD*) associée à une procédure n'étant elle-même pas conforme aux dispositions régissant l'exercice de l'action pénale et l'instruction judiciaire constituait une violation du droit à un procès équitable.

Tribunal d'arrondissement de Luxembourg, 12e chambre correctionnelle se prononçant sur la violation des articles 5 et 6 de la loi de 2002 relative à la protection des données.

Le 11 octobre 2007, le tribunal d'arrondissement de Luxembourg, siégeant en 12e chambre correctionnelle a, pour la première fois, condamné pénalement un individu sur la base de la loi de 2002. Un journaliste luxembourgeois avait divulgué, diffusé et vendu une liste reprenant les noms de membres de la Grande Loge de France (liste contenant les noms de francs-maçons de France) par le biais de son hebdomadaire ainsi que de son site Internet. La publication de telles listes avait précédemment été interdite en France par la Commission nationale de l'informatique et des libertés (CNIL). La CNIL a donc officiellement dénoncé cette violation à la CNPD. Après avoir examiné l'affaire, la Commission nationale, estimant que la loi de 2002 avait été violée, a donc porté plainte auprès du procureur d'État. Dans son jugement, le tribunal luxembourgeois d'arrondissement a confirmé que le journaliste avait violé l'article 6, alinéa 5 (communication de catégories spéciales de données à des tiers) et l'article 5, alinéa 2 (le traitement des données réalisé par le journaliste ne satisfait à aucune des conditions de légitimité prévues par la loi) de la loi de 2002 relative à la protection des données.

Jurisprudence administrative

Le 21 mai 2007, le tribunal administratif a rejeté la demande d'annulation d'une décision prise par la Commission nationale, laquelle avait autorisé la vidéosurveillance générale au sein d'un grand

centre commercial mais refusé la vidéosurveillance permanente de deux salles d'interrogatoire. Le tribunal administratif a confirmé l'argument avancé par la Commission nationale selon lequel aucune disposition de la loi de 2002 n'autorisait l'entreprise propriétaire du centre commercial à filmer et à enregistrer l'interrogatoire de personnes suspectées de vol à l'étalage. Le 13 décembre 2007, la Cour d'appel administrative a confirmé la décision précitée.

C. Questions diverses importantes

En 2007, la CNPD a procédé à un audit approfondi auprès des principaux opérateurs luxembourgeois de télécommunications. La CNPD souhaitait se faire une idée des mesures et actions prises par les opérateurs télécoms pour garantir le respect, dans le cadre de leurs activités, des dispositions de la loi du 30 mai 2005 transposant la directive 2002/58/CE.

En 2007, la Commission nationale a utilisé les pouvoirs d'enquête lui ayant été octroyés par la loi de 2002 pour contrôler le respect d'une décision refusant la vidéosurveillance. L'enquête a mis en évidence que les magasins avaient bien respecté cette décision du tribunal. Aucune vidéosurveillance n'était en effet effectuée dans les établissements contrôlés.

La CNPD a poursuivi sa campagne d'information et de sensibilisation, entre autres en participant activement à la première Journée de la protection des données organisée par le Conseil de l'Europe. La Commission nationale a ainsi fourni des informations sur les nouvelles dispositions de loi via son site Internet et des interviews publiées dans les médias luxembourgeois.

Malte

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE

La directive 95/46/CE a été transposée dans la législation maltaise par la loi sur la protection des données, chapitre 440 des lois de Malte. La loi est entrée en vigueur en juillet 2003, avec une période de transition pour que la notification des opérations de traitement se fasse avant juillet 2004. Certaines dispositions relatives aux systèmes d'archivage manuel ne sont effectives que depuis octobre 2007.

La directive 2002/58/CE a été transposée en partie par la loi sur la protection des données, en vertu de la notice légale 16 de 2003, mais aussi par la loi sur les communications électroniques, en vertu de la notice légale 19 de 2003. Ces deux règlements d'application sont entrés en vigueur en juillet 2003.

Autres nouvelles mesures législatives

Aucune.

B. Jurisprudence

Aucune.

C. Questions diverses importantes

Au cours de l'année de référence, le bureau du Commissaire à la protection des données a reçu trente-sept plaintes, la plupart dénonçant l'utilisation illicite de la vidéosurveillance. Dans le cadre de cette enquête, le bureau a procédé à sept inspections, dont trois suite à une plainte et les autres dans le cadre du contrôle périodique des exigences communautaires.

En 2007, le Commissaire a rencontré régulièrement des représentants de divers secteurs afin d'examiner des questions en rapport avec la protection des données et d'élaborer des lignes directrices en vue de réglementer le traitement des données dans les divers secteurs concernés, parmi lesquels les institutions financières, la presse, les assurances, la sécurité sociale, l'enseignement, la sécurité, les jeux d'argent et la police. Des consultations ont eu lieu, en particulier avec des représentants du secteur des communications électroniques, à propos de la transposition de la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux de communication. La coopération étroite avec les autorités de régulation et diverses associations et fédérations s'est par ailleurs poursuivie.

Tout au long de l'année, le bureau a apporté sa contribution aux plateformes européennes et internationales. Elle a ainsi participé au Groupe de travail « Article 29 » sur la protection des données, à la conférence européenne des commissaires à la protection des données personnelles, à la conférence internationale sur le respect de la vie privée et la protection des données à caractère personnel, aux réunions des trois autorités communes de contrôle européennes (Schengen, Douanes, Europol et Eurodac), au Case Handling Workshop (atelier sur les expériences dans le traitement de cas pratiques), à l'agence Eurojust du Conseil de l'Europe ainsi qu'au Bureau de la Commission consultative de la convention pour la protection des personnes à l'égard du traitement automatique des données à caractère personnel.

Des présentations ont été données dans différentes organisations et organes dotés d'une personnalité juridique en vue de mieux sensibiliser et mieux associer les acteurs clés à l'évolution de la culture de la protection des données. Des articles et des présentations traitant de divers aspects de la protection des données ont été publiés dans la presse locale, et des reportages ont été présentés à la radio et à la télévision. Le bureau a par ailleurs répondu à un nombre substantiel de demandes de renseignements par téléphone et par courrier électronique.

Le 28 janvier, le Commissaire à la protection des données s'est associé aux autres autorités européennes de protection des données pour célébrer la première Journée européenne de la protection des données. Ce jour est aussi celui de l'ouverture à la signature de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatique des données à caractère personnel (convention 108), qui a eu lieu à Strasbourg en 1981. Cette journée européenne

entend sensibiliser les citoyens européens à leur droit au respect de la vie privée en termes de protection des données à caractère personnel.

Dans une résolution publiée à l'occasion de cet événement, le Groupe de travail « Article 29 » – la plateforme des autorités en charge de la protection des données en Europe – a expliqué qu'en cette ère d'omniprésence du traitement des données, cette journée européenne offrait une excellente occasion de montrer et de comprendre comment garantir cette nécessaire protection de la vie privée au sein d'une société démocratique. Les autorités européennes de protection des données ont également déclaré qu'à l'avenir, le Conseil de l'Europe devrait davantage promouvoir la coopération pour faire de cette journée de la protection des données un succès et souligner le rôle fondamental des autorités de protection des données dans la défense des droits fondamentaux.

Pour faire la promotion de l'événement, le bureau avait fait diffuser un communiqué de presse par l'intermédiaire du département de l'information afin d'annoncer la journée européenne. Il a aussi participé à un programme télévisé local d'éducation et distribué du matériel d'information aux élèves, notamment des affiches et des règles. Aidé par le cabinet du Premier ministre maltais, le commissaire s'est aussi adressé à tous les délégués à la protection des données dans le secteur public.

Pays-Bas

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE

La directive 95/46/CE a été transposée dans la législation nationale par la loi sur la protection des données (*Wet bescherming persoonsgegevens*, abrégé en Wbp). Cette loi du 6 juillet[9] 2000, entrée en vigueur le 1er septembre 2001, remplace l'ancienne loi sur l'enregistrement des données (*Wet persoonsregistraties*, abrégé en Wpr) du 28 décembre 1988.

La directive 2002/58/CE a été transposée dans la législation nationale des Pays-Bas, essentiellement par la nouvelle loi sur les télécommunications (*Telecommunicatiewet*), entrée en vigueur le 19 mai 2004[10]. D'autres dispositions de cette directive ont également été transposées dans la loi sur la criminalité économique (*Wet op de Economische Delicten*), qui met en œuvre l'article 13, 4e paragraphe, de la directive 2002/58/CE.

B. Jurisprudence et questions diverses importantes

Le respect de la loi néerlandaise sur la protection des données ne vise pas uniquement l'intérêt des citoyens. Le respect de la vie privée sert également un intérêt collectif : vivre dans une société au sein de laquelle nous pouvons supposer que nos données personnelles ne seront pas détournées ou utilisées à mauvais escient, gage de confiance envers le gouvernement, les entreprises, les institutions et les uns envers les autres.

En 2007, l'autorité néerlandaise de protection des données (*College Bescherming Persoonsgegevens*, abrégé en CBP) a recentré sa stratégie sur les enquêtes et les mesures répressives – la principale mission de toute autorité de contrôle indépendante – afin de promouvoir une meilleure sensibilisation à l'existence de normes en la matière et un plus grand respect de la législation. Toute mesure répressive doit bien entendu être précédée d'une mise au point visant à clarifier les critères justifiant cette mesure de notre part. Pour pouvoir concrétiser ce changement de cap et la nouvelle priorité accordée aux normes, aux enquêtes et à l'application des lois compte tenu du budget qui nous a été alloué, nous avons décidé de nous intéresser surtout, en ce qui concerne les demandes d'aide et d'assistance, aux graves violations du droit, de nature structurelle, ainsi qu'à celles qui entraînent des préjudices majeurs pour un grand nombre de citoyens ou des groupes de citoyens. Le site de l'agence néerlandaise de protection des données a ainsi été enrichi et étendu de façon à encourager et aider les citoyens à résoudre eux-mêmes les problèmes, et si nécessaire, entreprendre eux-mêmes des actions.

Plus concrètement : en notre qualité d'autorité de contrôle et pour influencer au maximum le respect des dispositions légales dont la surveillance nous a été confiée, nous avons commencé, l'année passée, à intensifier notre politique d'information générale, en sensibilisant mieux les citoyens, les spécialistes et les organisations, à l'existence de leurs droits et de leurs obligations et en leur donnant davantage de moyens pour les respecter (ou les faire respecter). Nous avons également commencé à donner la priorité aux tâches incombant à toute autorité de contrôle efficace, et nous avons donc examiné dans quelle mesure les dispositions légales applicables sont respectées et, en cas de violation de celles-ci, nous avons pris les mesures nécessaires pour faire respecter la loi.

À l'instar des années précédentes, la collecte et le traitement à grande échelle de données ont figuré en bonne place dans l'agenda de l'APD en 2007. Les problèmes de respect de la vie privée posés par la carte à puces pour les transports publics (*OV-chipkaart*) et le dossier médical informatisé (*Elektronisch Patiëntendossier*) ont été en tête des préoccupations. Dans notre aperçu ci-dessous de nos activités en 2007, nous vous proposons un examen succinct de ces deux problématiques, à côté d'autres aspects particuliers.

Soins de santé

L'APD néerlandaise a rendu un avis critique sur un projet de loi prévoyant l'introduction d'un dossier médical informatisé. Selon elle, le fait que les dossiers médicaux deviennent ainsi accessibles à tous les dispensateurs de soins constitue un risque bien trop élevé, notamment

[9] Loi du 6 juillet 2000 sur les règlements applicables à la protection des données à caractère personnel (*Wet bescherming persoonsgegevens*), Staatsblad 2000, 302. Une traduction non officielle de la loi est disponible sur le site Internet de l'autorité néerlandaise en charge de la protection des données à l'adresse www.dutchDPA.nl ou www.cbpweb.nl (en néerlandais).

[10] Loi du 19 octobre 1998 concernant les règles en matière de télécommunications (*Telecommunicatiewet*), Staatsblad 2004, 189.

face à la protection dont doivent bénéficier les données personnelles sensibles. À l'exception des situations d'urgence, seul le personnel soignant impliqué dans le traitement du patient doit pouvoir avoir accès au dossier de ce dernier. Dans les autres cas, le risque existe que des tiers non autorisés utilisent abusivement ces données médicales ou les détournent.

En 2007, l'APD néerlandaise a aussi rendu un avis négatif sur un projet de loi dans le domaine des soins de santé des jeunes et des maladies infectieuses. Ce projet prévoit de rendre obligatoire le dossier électronique de l'enfant dans le domaine des soins de santé (*elektronisch kinddossier jeugdgezondheidzorg*). L'autorité de protection des données a en effet estimé que la nécessité d'un enregistrement informatisé central de ces données n'avait pas été suffisamment étayée. Suite à cela, le cabinet néerlandais a déclaré qu'il abandonnait l'idée d'un dossier électronique de l'enfant dans le domaine des soins de santé et a annoncé qu'il rechercherait d'autres pistes pour l'échange d'informations dans ce domaine.

Administration publique

Le numéro d'identification nationale (*BSN*) a été introduit à la fin novembre 2007, marquant le début d'une nouvelle ère pour l'APD néerlandaise. Un guichet de services publics sera mis en place au sein du centre de gestion du BSN afin de permettre aux autorités locales et aux citoyens d'y poser toutes leurs questions. En tant qu'autorité responsable de la surveillance de la bonne gestion des données à caractère personnel, l'APD est aussi compétente pour intervenir en cas de problème réel lié à la mise en œuvre de cette nouvelle loi.

L'APD a par ailleurs formulé des critiques concernant la proposition relative à un indice national de référence pour les jeunes à risque (*verwijsindex risicojongeren*, abrégé en VIR). Si elle approuve vivement tout effort visant à aider plus rapidement et plus efficacement les enfants et les jeunes à problèmes, l'autorité se demande toutefois si cet indice a bien pour seule finalité l'offre d'une aide, ou si un objectif de maintien de l'ordre public n'est pas poursuivi de manière concomitante. L'APD demande dès lors une clarification complète des termes clés et des critères.

Autorités judiciaires et de police

La sécurité et le respect de la vie privée sont tous deux essentiels pour les citoyens. Toutefois, comme c'est bien trop souvent le cas dans les débats publics, ces valeurs sont souvent mises en opposition, de façon par trop simpliste. Pour recentrer les débats dans le bon sens, l'APD a commandé une étude, en collaboration avec le ministère de la justice et le ministère de l'intérieur et des relations du Royaume, en vue d'identifier le meilleur équilibre entre les efforts visant à mettre en place une société sûre et ceux visant à protéger le droit au respect de la vie privée. Un rapport de recherche indépendant, qui intègre des lignes directrices pour améliorer le dialogue, a ainsi été rédigé. Il a été présenté le 1er novembre 2007 lors d'un symposium.

Lorsque la police procède à des écoutes téléphoniques dans le cadre d'une enquête criminelle, les conversations entre les avocats et leurs clients sont elles aussi souvent enregistrées. Il faut dès que possible effacer ces conversations avec des personnes détenant des informations confidentielles et qui ont droit à un privilège. Mais une inspection menée par l'APD néerlandaise dans le centre national des écoutes téléphoniques a révélé que, dans la plupart des cas, cette obligation n'était pas correctement suivie ou que les délais n'étaient pas respectés. L'Openbaar Ministerie (Parquet) a annoncé que des mesures seront prises afin de remédier à cette situation.

Dans ses recommandations relatives à des propositions de loi, ou autres réglementations dans le domaine pénal, l'APD néerlandaise soulève régulièrement la question suivante : la nécessité réelle de la réglementation en question a-t-elle été démontrée? A-t-il été mis en évidence que les dispositions existantes ou proposées précédemment étaient insuffisantes ? L'APD a ainsi estimé, à la lumière des possibilités d'identification toujours plus pointues, que le ministère de la justice n'avait pas suffisamment étayé sa proposition visant à créer une banque de données centrale pour le stockage de l'identité de tous les suspects et de tous les condamnés. Quant au projet émanant de la police – ministère public et Maréchaussée royale (*Koninklijke Marechaussee*, en abrégé *KMar*) visant à enregistrer la plaque d'immatriculation de tous les automobilistes – avec ou sans casier- entrant à Amsterdam via le pont

d'Utrecht, contribue-t-il vraiment à rendre la société plus sûre?

Fin 2007, à la demande du Sénat, l'APD néerlandaise a rendu un avis sur un projet de lois visant à renforcer les compétences des services de renseignement et de sécurité, dans le cadre de la lutte contre le terrorisme, de façon à leur permettre d'obtenir des données sur les déplacements, les paiements et l'utilisation d'Internet par les citoyens. Selon elle, la nécessité de telles mesures, qui viendraient s'ajouter aux nombreuses mesures existantes, n'a pas été démontrée tandis que les conséquences de cette analyse de données – pour les citoyens, mais aussi pour les responsables et les services concernés – n'ont pas été (suffisamment) prises en compte.

Commerce et services

Suite à l'annonce faite par l'APD selon laquelle des mesures répressives seraient prises en cas de stockage illicite du nom et des coordonnées des voyageurs en association avec leurs données de déplacement, les sociétés néerlandaises de transports publics semblent avoir enfin reconnu que l'*OV-chipkaart* était contraire à la loi (Wbp). En 2007, une étude a été réalisée dans le cadre d'un projet pilote mené au sein du réseau de métro amstellodamois afin de déterminer l'impact de la carte à puce du voyageur. L'étude a conclu à l'illégalité de l'utilisation de cette carte.

La société des transports municipaux (*Gemeentevervoerbedrijf*, en abrégé GVB) et d'autres sociétés de transports publics s'emploient à présent à assurer la conformité de cette pratique par rapport aux dispositions de la Wbp. La conception technique du stockage des données fera désormais la distinction entre d'une part les coordonnées – du titulaire de la carte (nom et adresse) et les déplacements d'autre part. Le risque d'un contrôle illégal des habitudes de déplacement des citoyens sera ainsi considérablement réduit.

Internet

Des données personnelles sont publiées sur l'Internet de diverses façons et sont généralement accessibles dans le monde entier, vingt-quatre heures sur vingt-quatre, à un public très large et très diversifié. Une accessibilité qui peut avoir des conséquences graves et inattendues pour les Internautes – dont beaucoup d'enfants ! –, dont les données personnelles se retrouvent ainsi publiées. En 2007, l'APD néerlandaise a rédigé et publié des lignes directrices visant à clarifier ce qui est permis et ce qui ne l'est pas en matière de publication de données à caractère personnel sur le Web. Les responsables peuvent ainsi utiliser ces lignes directrices pour déterminer si la publication de données personnelles sur Internet est autorisée. L'APD néerlandaise a elle-même publié de très nombreuses informations sur son site Internet. En ce qui concerne les mineurs d'âge, l'APD néerlandaise a opté pour une approche proactive en proposant les règles applicables aux réseaux sociaux et à la vente en ligne.

Le gouvernement utilise lui aussi l'Internet. En 2007, l'APD néerlandaise a réalisé une enquête sur la publication des données relatives aux permis de bâtir par la ville de Nimègue Des copies scannées en entier de formulaires de demandes se sont ainsi retrouvées en ligne, contenant non seulement des informations relatives aux biens en question et aux modifications envisagées, mais aussi des données personnelles des demandeurs, y compris leur signature. L'APD a estimé que la municipalité ne pouvait publier sur l'Internet que les données obligatoires, à savoir sur le bien en question et les aménagements proposés.

La bonne exécution d'une mission de droit public ne justifie pas davantage la publication sur l'Internet de toutes les données en possession d'un organisme administratif. En 2008, l'APD néerlandaise publiera également des lignes directrices sur les aspects relatifs à la vie privée lors de divulgation active par les services publics dans le cadre de la Loi relative à la transparence de l'administration (*Wet openbaarheid van bestuur*, abrégé en Wob).

Emploi et sécurité sociale

Les citoyens ne deviennent pas automatiquement des suspects sous le seul prétexte qu'ils bénéficient d'une aide sociale ou au logement. Dans le cadre du projet *Waterproof*, des retraités ainsi que des bénéficiaires d'une aide sociale de 65 municipalités de Frise, de Groningue et de la Drenthe ont fait l'objet d'un contrôle de lutte anti-fraude sur la base de données relatives à leur consommation d'eau et du montant de leur taxe sur la pollution des eaux. Les données collectées ont également été utilisées pour contrôler

d'éventuelles fraudes dans le cadre de l'aide au logement. Après enquête, l'APD néerlandaise a déclaré illicite ce rapprochement de fichiers de données. Il est nécessaire de lutter contre la fraude aux allocations, mais les contrôles basés sur le rapprochement de fichiers informatiques ne sont autorisés que sur la base d'une analyse du risque dûment effectuée et montrant effectivement qu'il est nécessaire de surveiller de plus près un groupe de citoyens pour lesquels il y a un risque plus important qu'ils ne soient dans la zone de fraude. Suite à la décision de l'APD néerlandaise, le service de sécurité sociale et d'enquête (*Sociale Inlichtingen* en *Opsporingsdienst*, en abrégé SIOD) travaille à présent à la mise au point d'un outil d'analyse du risque utilisant les technologies de protection des données personnelles (PET, *Privacy Enhancing Technology*). L'idée est d'associer la lutte contre la fraude et la protection des données personnelles, qui ne sont donc pas incompatibles.

Une autre façon de démasquer la fraude aux allocations consiste à faire appel à des inspecteurs de la sécurité sociale, chargés de procéder à des observations secrètes. La méthode de traitement utilisée pour les données personnelles en rapport avec ces activités a été consignée dans une description de procédure approuvée par l'APD. La recherche réalisée en 2006 a montré que le respect de l'obligation d'informer les citoyens du fait qu'ils étaient observés laisse quelque peu à désirer. La description de la procédure a donc été renforcée en 2007.

Et dans le cas de transfert vers un nouveau fournisseur de services d'amélioration des conditions du travail, l'ancien prestataire de services est-il autorisé à transférer le dossier de l'employé au nouveau fournisseur si la loi ne le prévoit pas? L'APD néerlandaise a répondu par la négative en 2006. Suite à des indications émanant du secteur selon lesquelles cet avis avait posé problème, l'autorité a examiné en 2007 si une autre approche était envisageable compte tenu du cadre légal actuel. L'APD a conclu qu'une distinction devait être faite entre les transferts de données soumises au secret médical et les données n'étant pas soumises à ce secret. Dans le premier cas, les transferts de données ne sont autorisés que dans certaines conditions, alors qu'ils sont autorisés dans le deuxième cas.

Pologne

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

Loi sur les télécommunications
Au cours de la période de référence, des travaux ont porté sur les amendements à la loi du 16 juillet 2004, loi sur les télécommunications qui transpose dans la législation polonaise les dispositions de « la directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE ».

Il a ainsi été proposé d'étendre de 2 à 5 ans la période de stockage des données de trafic relatives aux abonnés et aux utilisateurs finaux pouvant être transmises aux organismes autorisés responsables de la défense et de la sécurité nationale ainsi que de la sécurité publique. Cette proposition se fonde sur le fait que la prolongation de la période précitée permettrait d'améliorer l'efficacité des actions menées par les autorités chargées de faire respecter la loi durant les poursuites et l'enquête. Les données de facturation et autres données relatives aux télécommunications constituent en effet de solides moyens de preuve. Toutefois, les propositions d'amendements à la loi sur les télécommunications n'ont finalement pas été adoptées.

Loi bancaire
L'amendement à la loi bancaire du 29 août 1997 (texte unifié paru dans le Journal des lois 2002 n° 72, point 665) est entré en vigueur en 2007. Le législateur a entre autres modifié l'article 105 point a de la loi précitée. Les banques et autres institutions autorisées à accorder des prêts peuvent ainsi traiter, à des fins statistiques, les données des personnes physiques couvertes par le secret bancaire sans le consentement de la personne concernée, et ce une fois que l'obligation prévue par le contrat avec la banque ou toute autre institution autorisée à accorder des prêts a pris fin et pour une période de 12 ans à compter de l'extinction de l'obligation contractuelle. Jusqu'à présent, les banques et les institutions précitées ne pouvaient traiter les données relatives aux personnes physiques couvertes par le secret bancaire que pour une période n'excédant pas 5 ans à compter de l'expiration de l'obligation.

Espace Schengen
Le 24 août 2007 a vu l'adoption de la loi relative à la participation de la République de Pologne au système d'information Schengen et au système d'information sur les visas mettant en œuvre l'acquis de Schengen. Cette loi fixe, entre autres, les obligations des autorités autorisées à lancer un message d'alerte et à rendre accessibles les données intégrées dans le système d'information Schengen et dans le système d'information sur les visas via le système d'information national. La Pologne est entrée dans l'espace Schengen le 21 décembre 2007.

Loi sur les coopératives de logement
La disposition régissant la publication (via l'Internet) de la documentation des coopératives de logement, y compris les données personnelles, a été introduite par la loi du 14 juin 2007 amendant la loi sur les coopératives de logement et autres lois. Ces données peuvent être transmises à des tiers ne faisant pas partie de coopérative en question et n'étant pas en charge des activités de celle-ci. Dès que ces informations sont publiées, les données personnelles (parfois même des données sensibles) peuvent être obtenues et exploitées par des tiers.

Aide sociale
La loi du 16 septembre 2007 relative à l'assistance aux personnes ayant droit à une pension alimentaire ne précise pas les critères que le ministère en charge de la protection sociale doit prendre en compte pour préparer un règlement d'exécution précisant les données à conserver dans le Fichier central des personnes devant une pension alimentaire. Les vives réserves formulées par l'Inspecteur général pour la protection des données à caractère personnel n'ont pas été prises en compte pendant les travaux législatifs en vue de la rédaction de la loi précitée. Par conséquent, un projet de règlement du ministère de l'emploi et de la politique sociale relatif à la nature des données enregistrées dans le fichier central des personnes devant une pension alimentaire prévoit un éventail de données particulièrement large, y compris des données sensibles.

B. Jurisprudence

Base de données centrale des numéros de portable à carte prépayée
L'inspecteur général pour la protection des données à caractère personnel a pris part aux débats autour de la proposition visant à créer une base de données centrale de tous les abonnés et utilisateurs enregistrés de téléphone portable à carte prépayée dont l'exploitation est régie par le président du Bureau des communications électroniques. Les auteurs de la proposition ont souligné qu'une telle base de données jouerait un rôle capital puisqu'elle permettrait aux services d'urgence de recevoir les informations nécessaires relative à un appelant et sa localisation. L'Inspecteur général a indiqué que de telles informations pourraient également être obtenues conformément à la procédure prévue par l'article 78 de la loi sur les télécommunications. Celle-ci prévoit que les opérateurs du réseau public de téléphonie doivent communiquer les informations en leur possession sur la localisation d'un point du réseau à partir duquel le 112 ou tout autre numéro d'urgence a été composé à la demande des services d'urgence mandatés par la loi pour fournir assistance, l'objectif étant de garantir une intervention immédiate.

Inspection du site Internet de réseau social « Nasza-klasa »
L'Inspecteur général pour la protection des données à caractère personnel a contrôlé le site Internet de réseau social « Nasza-klasa » (sur lequel plus de 6 millions de personnes ont créé un profil) afin de s'assurer que les exigences de la loi relative à la protection des données étaient bien respectées. Cette inspection approfondie a montré que le portail respectait pratiquement toutes les exigences de la loi relative à la protection des données (l'introduction de mesures de sécurité supplémentaires ayant toutefois été recommandée pour la connexion au portail) et qu'il traitait les données personnelles conformément à sa propre politique en matière de respect de la vie privée. Les propriétaires du portail, qui avaient précédemment fait enregistrer leur système d'archivage de données, ont annoncé qu'ils amélioreraient leurs opérations de traitement des données en tenant compte de toutes les remarques et recommandations formulées par l'Inspecteur général au terme de l'inspection.

C. Questions diverses importantes

Journée de la protection des données
Le 28 janvier 2007 a vu la célébration de la première Journée de la protection des données, organisée à l'initiative du Conseil de l'Europe. L'événement a été prétexte à la tenue de nombreux événements, auxquels l'Inspecteur général s'est activement associé. Parmi les principales manifestations, nous retiendrons la Conférence « Protection des données à caractère personnel : garantie ou menace pour le respect de la vie privée ? », co-organisée par l'Inspecteur général pour la protection des données à caractère personnel, M. Michał Serzycki, et par le président de l'école de commerce Kozminski de Varsovie. L'événement était placé sous le haut patronage du Maréchal de la Diète et a réuni de nombreux représentants de cercles scientifiques spécialisés dans la protection des données personnelles ainsi que des membres du Parlement et des représentants des autorités gouvernementales. L'Inspecteur général pour la protection des données à caractère personnel a aussi annoncé une série d'initiatives dans le domaine de l'éducation visant à mieux sensibiliser le public à la question de la protection des données à caractère personnel et au droit à la vie privée, l'objectif ultime étant d'améliorer la protection des données à caractère personnel en Pologne. Le 31 janvier, des cérémonies ont eu lieu dans les locaux de la représentation permanente de la Pologne auprès de l'Union européenne à Bruxelles. De nombreuses personnes concernées par les problèmes de protection des données et de la vie privée au sein des institutions de l'Union européenne et du Conseil de l'Europe, ainsi que des membres polonais du Parlement européen, des représentants des agences diplomatiques polonaises en Belgique ainsi que des journalistes polonais et étrangers y ont été conviés.

L'Inspecteur général a également accordé une série d'interviews, dans la presse et à la télévision.

Campagne de sensibilisation
En 2007, l'Inspecteur général a lancé une vaste campagne visant à sensibiliser les citoyens à l'importance de la protection des données. Parmi les actions mises en œuvre, nous retiendrons un concours de dessin pour enfants autour du thème « Le respect de la vie privée

autour de moi » et un concours récompensant le meilleur mémoire de maîtrise ayant pour thème la protection des données. L'Inspecteur général a par ailleurs signé un accord avec l'une des écoles de commerce de Varsovie en vue de l'organisation d'un cursus postuniversitaire dans le domaine de la protection des données.

Le personnel de l'Inspecteur général pour la protection des données a réalisé une série d'ateliers destinés au personnel d'autres institutions, y compris de hautes instances gouvernementales, comme la Chancellerie de la Diète et du Sénat, le ministère des affaires étrangères, l'Office des douanes et la Banque nationale de Pologne. Le personnel a également participé activement aux événements organisés par d'autres entités. Afin de rapprocher les questions de protection des données du grand public, le personnel a également pris part à la Conférence du service des douanes à Olsztyn et à la conférence scientifique « Dix ans de législation de protection des données en Pologne », organisée par l'université de Torun. Une série de rencontres éducatives avec des étudiants issus de diverses universités polonaises a également eu lieu.

Le Bureau de l'Inspecteur général pour la protection des données à caractère personnel organise également des ateliers sur la protection des données à caractère personnel en coopération avec les membres polonais du Parlement européen. Parmi les actions de sensibilisation prévues en 2007, mentionnons également la conférence « Le droit au respect de la vie privée ans la société de surveillance » qui a eu lieu à Varsovie, les 22 et 23 octobre.

Conférence – Le droit au respect de la vie privée dans une société de la surveillance

La conférence commémorant le dixième anniversaire de l'adoption de la loi polonaise de protection des données a eu lieu les 22 et 23 octobre 2007, dans la salle des colonnes de la Diète (Parlement polonais).

Elle a été accompagnée d'ateliers intitulés autour du thème « Vie privée et Médias » organisé en coopération avec la Commission. Celui-ci a permis d'examiner les questions de vie privée et de protection des données dans le contexte des médias

Un grand nombre d'éminents conférenciers, polonais et étrangers, ont dressé un état des lieux de la protection des données personnelles et du respect de la vie privée.

L'objectif était d'examiner des aspects clés de la loi relative à la protection des données, qui sont particulièrement importants dans le contexte du développement rapide des nouvelles technologies, notamment les technologies de l'information.

Les trois sessions du 22 octobre 2007 ont abordé des questions comme les nouvelles technologies – de nouvelles possibilités de surveillance, les systèmes européens d'information –, ainsi que le rôle des commissaires de la protection des données dans la société de surveillance. La première session s'est concentrée sur divers aspects en rapport avec les nouvelles technologies et les possibilités de surveillance ainsi créés. La seconde session s'est penchée sur les systèmes européens d'information. Le rôle toujours plus important des commissaires en charge de la protection des données, qui veillent au droit à la protection des données à caractère personnel et à la vie privée dans les pays européens a fait l'objet de la troisième session.

Lors de la deuxième journée de la conférence, les ateliers « Vie privée et médias » ont permis d'examiner les questions d'actualité dans le domaine de la protection de la vie privée et des données dans le contexte des activités de la presse. Les présidences des diverses sessions – représentants de la Commission européenne et des autorités européennes de protection des données – ont permis aux participants de réfléchir à la protection de la vie privée des personnalités publiques et des utilisateurs d'Internet.

Portugal

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE

La directive 95/46/CE a été transposée dans la législation nationale par la loi n° 67/98 du 26 octobre relative à la protection des données.

La directive 2002/58/CE a quant à elle été transposée dans la législation nationale par le décret-loi (uniquement l'article 13) n° 7/2004 et par la loi n° 41/2004 du 18 août.

Aucune autre disposition légale concernant directement la transposition des directives précitées n'a été adoptée. Toutefois, plusieurs lois dans le domaine de la protection des données sont entrées en vigueur, comme la loi n° 7/2007 relative à une nouvelle carte d'identité pour tous les citoyens âgés de plus de six ans. Cette carte mentionne le numéro d'identification nationale, le numéro d'identification fiscale, le numéro de sécurité sociale ainsi que le numéro de la carte de santé des citoyens. Elle intègre également une empreinte digitale et une photographie digitale. La nouvelle carte du citoyen – tel est son nom – permet l'identification physique et électronique des individus. Son introduction soulève toutefois une série de questions clés en matière de protection des données, questions exprimées dans les avis rendus en 2006 par l'APD.

La loi n° 33/2007 relative à la vidéosurveillance dans les taxis est également entrée en vigueur en 2007. Elle autorise les chauffeurs de taxis à installer des caméras vidéo dans leur véhicule mais ne leur permet d'actionner le dispositif que lorsqu'ils se sentent en danger. Les images sont alors transmises à une unité centrale privée, à laquelle le taxi est relié, qui va ensuite les enregistrer et éventuellement les communiquer aux autorités répressives pour enquête, et ce en cas de problème de sécurité ; dans tous les autres cas, les images seront effacées.

La loi stipule que les unités centrales jouent le rôle de contrôleur de données. Elles devront notifier ce traitement à l'APD, qui vérifie également les mesures de sécurité installées et la fiabilité du matériel utilisé.

B. Jurisprudence

En 2007, un tribunal administratif central a rendu une décision importante suite à un appel interjeté contre une décision de l'APD concernant l'utilisation de la vidéosurveillance dans une copropriété. La décision est allée dans le sens de celle de l'APD.

Compétente pour autoriser l'utilisation de la vidéosurveillance aux fins de protéger les personnes et les biens, l'APD ne permet toutefois l'installation de ces systèmes dans les copropriétés qu'avec l'accord des occupants et des propriétaires. Dans l'affaire en question, l'APD avait autorisé l'utilisation de systèmes de vidéosurveillance, partant du principe d'un accord unanime, sur la base des informations obtenues auprès du contrôleur de données. Il s'est toutefois avéré que le consentement de tous les résidents n'avait pas été obtenu, de sorte que l'APD a révoqué l'autorisation, fondée sur de fausses bases. Le contrôleur de données a rejeté cette décision, arguant qu'il était excessif que l'APD exige l'unanimité pour donner son autorisation et que celle-ci ne pouvait dès lors pas être révoquée. Le tribunal a estimé que la décision d'autorisation pouvait être modifiée (étant donné qu'elle était basé sur des faits incorrects) et qu'il était relativement pertinent et proportionné de subordonner l'utilisation de tels systèmes dans les copropriétés à l'accord unanime de tous les résidents, vu l'intrusion dans la vie privée que représente la vidéosurveillance.

C. Questions diverses importantes

Avis sur des projets de loi
Conformément à la loi sur la protection des données, tout projet de loi intéressant la protection des données, qu'il soit de niveau national ou international, doit être soumis à l'APD pour avis.

En 2007, l'APD a ainsi rendu 62 avis dans le domaine de la coopération des autorités de police ainsi que dans plusieurs autres domaines en rapport avec la protection des données ; plusieurs de ces avis portaient sur des accords bilatéraux conclus entre le Portugal et des pays tiers. Les domaines concernés sont notamment : le développement de mesures d'e-gouvernement (simplification des procédures, remplacement des copies-papier par des documents digitaux, accès en

ligne, rapprochement de données), la réglementation du système national de statistiques, la banque centrale de données sur les bénéficiaires d'une assurance-vie, les formulaires de nuitée à l'hôtel pour les étrangers, la banque centrale de données sur l'évaluation du risque de crédit.

L'APD a également rendu un avis à propos de la transposition de la directive 2006/24/CE sur la conservation du trafic de données, suggérant d'importants amendements, notamment la nécessité de préciser clairement l'objectif du traitement de données, de définir les « crimes graves » aux termes de la loi nationale et de raccourcir la période de conservation des données, qui était de deux ans dans le projet de loi. L'avis de l'APD a été en grande partie pris en compte, et la période de conservation a finalement été fixée à douze mois.

En 2007, l'APD a rendu deux avis pertinents sur la mise en place de banques de données ADN aux fins de l'enquête criminelle et de l'identification civile, cette dernière n'étant autorisée que sur une base volontaire. L'APD a soulevé une série de préoccupations par rapport à cette proposition. Certaines recommandations ont été intégrées dans un nouveau projet de loi, mais l'un des points les plus controversés – la banque de données ADN à des fins d'identification civile – a néanmoins été adopté.

Lignes directrices pour les études cliniques

En 2007, l'APD portugaise a publié d'importantes lignes directrices pour les contrôleurs de données en ce qui concerne le traitement des données en vue de la réalisation d'études dans le domaine de la santé et des essais cliniques de médicaments sur l'homme. Ces lignes directrices ont permis d'accélérer la procédure d'autorisation tout en fixant les exigences auxquelles les contrôleurs de données doivent satisfaire. Elles aident en même temps les personnes concernées à prendre conscience des conditions régissant le traitement de leurs données et leurs droits.

Vidéosurveillance dans les lieux publics

L'APD portugais a rendu son premier avis concernant l'utilisation de systèmes de vidéosurveillance dans les rues. Cette possibilité découle de la loi n° 1/ 2005, qui régit l'utilisation de la vidéosurveillance par les autorités chargées de faire respecter la loi. Ce texte autorise également les municipalités à demander l'installation de tels dispositifs dans les rues après avis positif de la police locale. En cas d'avis négatif, l'APD émet un avis qui devient contraignant. Par contre, dans le cas d'une opinion positive de l'APD, la décision finale incombe au ministère des affaires intérieures.

Les autorités municipales de la ville de Porto ont donc demandé l'autorisation de pouvoir, pour des raisons de sécurité, installer des caméras de vidéosurveillance dans certaines rues très fréquentées du centre-ville, abritant de nombreux restaurants, bars et esplanades. Le système prévoyait l'utilisation de zones blanches à hauteur des immeubles d'habitation. Toutes les images devaient être transmises directement à un commissariat. L'APD a rendu un avis favorable sauf pour l'utilisation du système pendant la journée : le système doit alors être éteint, la criminalité étant dans ces quartiers un phénomène essentiellement nocturne. L'enregistrement sonore n'est pas autorisé non plus : l'APD a en effet estimé que ce type d'enregistrement est disproportionné et relativement invasif, en particulier dans une zone de loisirs où les conversations de personnes se trouvant en dehors de l'esplanade auraient pu aussi être entendues et enregistrées.

Le ministère des affaires intérieures a donc donné son autorisation finale à l'utilisation du système de vidéosurveillance, sous réserve toutefois des conditions posées par l'APD. Ainsi que le prévoit la loi, cette autorisation n'est valable que pour un an, la poursuite du système devant ensuite être évaluée afin de déterminer si les conditions ayant conduit à l'installation du système sont encore pertinentes, et si l'objectif (prévention et poursuites criminelles) a été atteint.

Protocole avec le ministère de l'éducation

Lors de la célébration de la première Journée européenne de la protection des données, l'APD portugaise a signé un protocole avec le ministère de l'éducation en vue d'inclure des matières en rapport avec la protection des données dans les programmes scolaires de tous les niveaux d'enseignement (1-12) des établissements publics.

Ce protocole revêt une importance majeure étant donné qu'il permettra d'introduire, sur le long terme et de manière systématique, un programme scolaire axé sur la protection des données. L'objectif est de contribuer à la sensibilisation des citoyens aux questions de protection des données, de promouvoir une utilisation correcte des nouvelles technologies et de développer et de renforcer chez les jeunes une culture de la vie privée afin de les aider à se prendre pleinement en main en tant que citoyens actifs.

Par le biais de ce protocole, le ministère de l'éducation encourage une dynamique favorable à l'adoption de ce projet pédagogique dans le réseau scolaire. Avec le soutien du ministère, l'APD produit le matériel pertinent destiné aux élèves.

Suite à la signature de ce protocole, l'APD a distribué sur l'Internet une affiche qui s'adresse aux jeunes âgés de 10 à 15 ans. Elle a aussi commencé à élaborer un programme structurel spécifique pour les enfants de ces catégories d'âge. Ce programme a été présenté au ministère en octobre 2007. Le projet a été lancé dans les écoles en janvier 2008.

Essai sur la protection des données – concours
L'année dernière, l'APD a lancé un concours annuel dans le domaine de la protection des données. Il s'agit d'un prix décerné à un ouvrage traitant de la protection des données, que ce soit d'un point de vue juridique, sociologique ou technique.

L'objectif est d'encourager l'analyse, la réflexion et la production d'une œuvre originale dans le domaine de la protection des données. Le lauréat verra son œuvre publiée. La cérémonie officielle de remise des prix doit avoir lieu chaque année le 28 janvier dans le cadre de la Journée européenne de la protection des données.

En cette première année, le prix a été accordé, avec les honneurs, en décembre 2007.

5e réunion ibéro-américaine sur la protection des données
En novembre, l'APD portugaise a accueilli la 5e réunion ibéro-américaine sur la protection des données. L'événement a eu lieu à Lisbonne en présence de pays lusophones d'Afrique en qualité d'observateurs. Les participants ont approuvé les directives relatives à l'harmonisation de la protection des données au sein de la communauté ibéro-américaine ainsi que la déclaration de Lisbonne, qui souligne l'importance, dans le contexte de la mondialisation, de promouvoir une simplification des mécanismes visant garantir des flux transfrontaliers des données respectueux du droit fondamental à la protection des données.

Cette réunion a également souligné que cette communauté a été vivement incitée à signer la Convention 108.

Roumanie

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

Les dispositions de la directive 95/46/CE du Parlement européen et du Conseil ont été transposées dans la législation roumaine le 12 décembre 2001 avec l'adoption de la loi n° 677/2001 sur la protection des personnes à l'égard du traitement de leurs données personnelles et sur la libre circulation de ces données.

La loi n° 677/2001 a accordé une indépendance totale à l'autorité de contrôle, qu'elle a investie de compétences en matière d'enquêtes, de contrôles et d'interventions ainsi que dans le domaine de la réglementation et de l'information du public, reprenant ici les principes établis par la directive 95/46/CE.

Les compétences de l'autorité de contrôle étaient jusqu'ici du ressort du Bureau de l'avocat populaire (le « médiateur »). Conformément à demande de la Commission européenne de mettre en place une autorité de contrôle indépendante et autonome, capable d'assumer les tâches spécifiques de suivi et de contrôle dans le domaine de la protection des données à caractère personnel, comme le prévoit la directive 95/46/CE, le Parlement a adopté la loi n° 102/2005 relative à la création, à l'organisation et au fonctionnement de l'Autorité nationale de contrôle pour le traitement des données à caractère personnel. Cette loi a été publiée dans le Journal officiel de la Roumanie n° 391 du 9 mai 2005. Cette loi fait de l'Autorité nationale de contrôle une autorité publique dotée de la personnalité juridique, autonome et indépendante vis-à-vis de toute autre autorité publique ainsi que vis-à-vis de toute autre personne physique ou morale de droit public ou privé.

La loi n° 102/2005 a introduit un amendement important aux dispositions de la loi n° 677/2001, à savoir la suppression de son article 27, paragraphe 5, qui stipulait que l'autorité de contrôle devait obtenir le consentement du ministère public ou du tribunal compétent avant de pouvoir ouvrir une enquête en rapport avec le traitement des données personnelles dans le domaine du droit pénal.

La loi n° 677/2001 a également été modifiée par la loi n° 278/2007 qui a aboli les redevances de notification pour le traitement des données personnelles relevant de la loi n° 677/2001.

La 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 a quant à elle été transposée dans la législation nationale par la loi n° 506/2004 relative au traitement des données personnelles et à la protection de la vie privée dans le secteur des communications électroniques.

Cette loi garantit la protection des données à caractère personnel faisant l'objet d'un traitement au sein du réseau public des communications électroniques et par les fournisseurs de services de communications électroniques, ainsi que par les fournisseurs de répertoires d'abonnés. Elle complète et précise le cadre juridique mis en place par la loi 677/2001 relative aux exigences spécifiques du secteur des communications électroniques.

Conscient du fait que le traitement de certaines données est souvent effectué dans l'intérêt de la loi ou de la personne concernée et que ce traitement n'est pas de nature à porter atteinte aux droits des personnes concernées, le président de l'Autorité de contrôle a rendu deux décisions (décision n° 90/2006 et décision n° 100/2007) publiées au Journal officiel. Celles-ci précisent les cas dans lesquels la notification du traitement de données à caractère personnel n'est pas requise.

L'autorité de contrôle est consultée lors de la rédaction de tout projet de loi en rapport avec la protection des droits et les libertés des personnes en ce qui concerne le traitement de leurs données personnelles, et ce conformément aux dispositions de la loi n° 677/2001, telle qu'elle a été modifiée et amendée. L'Autorité de contrôle a donc été amenée à rendre un avis sur plusieurs propositions, parmi lesquelles le projet de décision du gouvernement roumain relatif à l'approbation de normes méthodologiques d'application uniforme des dispositions légales relative à la preuve, à la résidence et aux documents d'identification des citoyens roumains ; le projet de décision du gouvernement roumain relatif à la forme et au contenu des documents d'identité,

de l'étiquette auto-adhésive lors de l'établissement des dossiers de nouvelle résidence et de nouveaux immeubles ; le projet de loi relative à l'obligation des transporteurs aériens de communiquer les données relatives aux passagers ; le projet de loi du gouvernement roumain relatif à la libre circulation sur le territoire roumain des citoyens de l'UE et de l'EEE et fixant la forme et le contenu des documents d'identité délivrés aux citoyens de l'UE et aux membres de leur famille ; et enfin le projet de loi relatif à l'établissement et à l'organisation du Système national sur les données génétiques.

L'autorité de contrôle a également rendu plusieurs avis sur les codes de conduite de diverses associations professionnelles, parmi lesquelles l'Association des agents de change roumains, l'Association roumaine des stomatologues privés et l'Association des banques roumaines, qui intègrent des normes appropriées sur la protection des personnes dont le traitement des données à caractère personnel est en cours.

Tenant compte de la nécessité de protéger efficacement les droits des personnes dont les données personnelles font l'objet d'un traitement au sein d'établissements de type agences de crédit, et conscient des risques que pose cette forme de traitement automatique pour le respect de la vie privée et familiale, en raison de la nature des données traitées et des objectifs de ce traitement, le président de l'Autorité de contrôle a publié en 2007 la décision n° 105/2007 relative au traitement des données à caractère personnel au sein d'établissements de type agences de crédit.

Cette décision établit les catégories de participants à ce type de système d'archivage, les données qui peuvent être traitées au sein de ceux-ci et les conditions dans lesquelles ces données peuvent être transmises ainsi que la période de conservation et les obligations des participants, notamment l'obligation de garantir la confidentialité et la sécurité des données personnelles intégrées dans ces systèmes.

B. Jurisprudence

Il convient de remarquer qu'en 2007, les tribunaux ont adopté des pratiques similaires dans les affaires en rapport avec la protection des données à caractère personnel, même si, au départ, les tribunaux inférieurs avaient suivi des approches quelque peu différentes.

1. Suite à une enquête réalisée au sein de l'Inspectorat général de la police roumaine, l'autorité de contrôle a pu mettre en évidence une infraction, à savoir l'absence de notification d'une procédure de traitement de données à caractère personnel préalablement à l'installation de caméras de surveillance sur l'une des principales routes nationales permettant l'identification des plaques minéralogiques. L'Inspectorat général de la police a toutefois contesté l'amende infligée par l'Autorité de contrôle et porté l'affaire devant un tribunal. L'affaire a finalement été jugée devant la Cour suprême de Roumanie. La Cour de cassation et de justice a toutefois confirmé la décision de l'Autorité de contrôle.

2. Un tribunal a également été amené à se prononcer après que l'Autorité de contrôle eut infligé une amende à un jardin d'enfants qui avait procédé au traitement de données personnelles sans le notifier à cette Autorité. Des données à caractère personnel avaient été traitées par un système de vidéosurveillance qui avait enregistré des images de tous les enfants fréquentant ce jardin d'enfants. Comme des données personnelles des enfants et du personnel avaient ainsi été traitées sans notification préalable à l'Autorité de contrôle, le tribunal saisi a confirmé la sanction initiale de l'Autorité de contrôle, car ces faits constituaient une infraction mineure (absence de notification).

3. En 2007, une agence de voyage qui transmettait automatiquement les adresses électroniques de ses clients a aussi été condamnée par l'Autorité de contrôle à s'acquitter d'une amende pour non notification de ce type de traitement. La décision de l'autorité a été considérée légale et fondée par la Cour suprême, qui a donc confirmé l'amende infligée par l'autorité.

4. Une affaire particulière a eu comme point de départ la plainte déposée par une personne qui affirmait avoir reçu des messages électroniques publicitaires non sollicités (spams) d'une société privée, et ce en violation des dispositions de la loi n° 506/2004 relative au traitement des données à caractère personnel et à la protection de la vie privée dans le domaine

des communications électroniques. Avec cette loi, le législateur roumain a interdit la communication de messages commerciaux par le biais de systèmes automatisés n'exigeant pas l'intervention d'un opérateur humain, par fax, courrier électronique ou toute autre méthode impliquant des services de communication électroniques accessibles au public, excepté dans le cas où la personne concernée a clairement exprimé son consentement. Le texte stipule également que la communication de messages publicitaires par le biais du courrier électronique est interdite dans tous les cas où l'identité de l'expéditeur (ou de la personne au nom de laquelle le message est envoyé) est dissimulée ou s'il n'y est pas mentionné que le destinataire est autorisé à demander l'arrêt des envois à son adresse.

En ce qui concerne les activités de publicité et de marketing, l'enquête a révélé que les messages intégraient en fait une commande pour se désinscrire. Or, alors que le plaignant avait utilisé cette possibilité, des messages publicitaires continuaient à parvenir à son adresse. Le contrôleur de données a ainsi été sanctionné pour avoir enfreint les dispositions légales relatives aux messages commerciaux non sollicités et donc aussi le droit à la vie privée des clients. Cette affaire doit encore être examinée devant un tribunal.

Malgré la diversité des affaires soumises aux tribunaux, les tribunaux et l'autorité de contrôle ont rendu une interprétation similaire concernant le cadre juridique régissant la protection des données à caractère personnel.

C. Questions diverses importantes

L'autorité de contrôle s'est intéressée de près à la mise en œuvre appropriée du cadre juridique relatif à la protection des données à caractère personnel, et les activités de contrôle ont dès lors constitué un volet clé de ses activités en 2007. 280 enquêtes ont été réalisées en 2007, dont 235 enquêtes d'office et 45 suite à des plaintes (21) ou des notifications (24) introduite par les citoyens.

La majorité des enquêtes d'office ont eu lieu conformément au plan annuel de l'Autorité, qui avait identifié et sélectionné des thématiques spécifiques sur la base de son expérience préalable. L'autorité a ainsi mis en évidence la connaissance insuffisante des dispositions de la loi n° 677/2001 ; elle signale le faible nombre de notifications soumises par les contrôleurs de données et dénonce le risque potentiel que ces opérations de traitement représentent pour les droits et les libertés des individus. Chaque trimestre a été consacré à un domaine d'action :

1) **télémarketing** – traitement des données personnelles par les services d'informations commerciales ;
2) **recouvrement de créances** – traitement des données personnelles des débiteurs en vue du recouvrement ;
3) **sélection et affectation du personnel** – traitement des données personnelles des candidats à un emploi à l'échelon national ou à l'étranger ;
4) **agences de voyage** – traitement des données à caractère personnel lors de la réservation ou l'offre d'autres services touristiques.

Suite aux investigations menées conformément à ce plan annuel, une augmentation significative du nombre de notifications a été enregistrée par rapport aux périodes précédentes. Ces investigations ont également abouti à un plus grand respect des droits fondamentaux et des libertés individuelles, notamment en ce qui concerne la protection des données et de la vie privée.

Outre les investigations réalisées conformément au plan annuel, 2007 a vu également un certain nombre d'enquêtes réalisées dans le cadre de la collaboration avec d'autres autorités européennes au sein du Groupe de travail « Article 29 ». Mentionnons ici entre autres le traitement des données personnelles dans le cadre du système SWIFT de transactions financières internationales.

Un nombre important de notifications soumises chaque année à l'Autorité de contrôle concernent les activités de marketing et de publicité.

En ce qui concerne les opérations de **marketing direct**, l'Autorité de contrôle a poursuivi les actions démarrées en 2006 à l'échelon de l'Association roumaine de marketing direct, en vue de la mise en œuvre des mesures requises pour garantir le droit des personnes à s'opposer à la réception de matériel publicitaire.

Le **télémarketing** apparaît désormais comme une forme spécifique de marketing direct de plus en plus souvent utilisée. Tout au long de 2007, dix enquêtes ont été réalisées afin de déterminer les conditions dans lesquelles les données personnelles étaient traitées dans le cadre de ce type d'activités et les sanctions infligées en cas de non-respect des dispositions légales applicables. Ces enquêtes ont permis de mettre en évidence les conclusions suivantes :

- D'une manière générale, les grandes entreprises de Roumanie mettent en œuvre ce type d'activités par le biais de leurs propres départements (« télémarketing passif »), ou par le biais de sociétés spécialisées (sur une base contractuelle). Les enquêtes ont montré que dans ce domaine, les contrôleurs de données notifiaient généralement leurs opérations de traitement par le biais d'autres entreprises, spécialisées dans les services de télémarketing. Dans certains cas, lorsque l'obligation de notification n'avait pas été respectée, les contrôleurs de données ont été sanctionnés conformément à l'article 31 de la loi n° 677/2001.

Les enquêtes réalisées dans des entreprises spécialisées dans le recouvrement de créances ont montré que les données personnelles des débiteurs sont conservées même après remboursement de la dette. L'autorité de contrôle a donc ordonné la suppression des données qui ne sont plus nécessaires eu égard à l'objectif spécifique du traitement (à savoir le recouvrement de créances). Dans d'autres cas, l'autorité de contrôle a même constaté que les contrôleurs de données avaient continué à conserver les données des débiteurs afin de dresser des « listes noires », qui, dans certains cas, étaient même publiées sur l'Internet, sur le site du contrôleur. Les principes de légitimité et de traitement proportionné n'ayant pas été observés dans ce cas, l'Autorité de contrôle a mis fin à ces opérations de traitement et ordonné la suppression des données conservées et publiées jusqu'au moment de l'enquête. Une attention particulière a été accordée à d'autres obligations des contrôleurs de données dans ce domaine : elles concernent la période de conservation des données et l'adoption de procédures de sécurité écrites.

46 investigations ont été menées en 2007 auprès de contrôleurs de données réalisant des activités dans le domaine de la sélection et de l'affectation de travailleurs, l'objectif étant de vérifier comment les dispositions de la loi n° 677/2001 étaient respectées. Les contrôleurs de données ont respecté les recommandations formulées par l'Autorité de contrôle suite à ces enquêtes. Les violations les plus souvent observées dans ce domaine sont l'absence d'informations adéquates transmises aux personnes concernées par les contrôleurs de données et le non-respect des exigences minimales de confidentialité et de sécurité des données traitées.

35 enquêtes ont par ailleurs été réalisées dans le secteur des agences de voyage en 2007. Les infractions aux dispositions légales relatives à la protection des données à caractère personnel mises en évidence sont les suivantes :

- dans de rares situations, les notifications ont été soumises par les agences de voyage ;
- les personnes concernées n'ont pas été correctement informées de leurs droits ;
- aucune notification n'a été soumise dans ce domaine pour le transfert transfrontalier de données personnelles, et, suite à toutes ces infractions, les contrôleurs de données ont été sanctionnés.

L'année 2007 a également été marquée par la participation de l'Autorité de contrôle à des activités en milieu universitaire, dans le cadre de sa campagne de sensibilisation aux problèmes spécifiques en rapport avec la protection des données à caractère personnel. Suite aux événements organisés en l'honneur de la Journée européenne de la protection des données, la faculté de droit « Simion Bărnuțiu » de Sibiu et l'Autorité de contrôle ont signé un protocole de coopération. Cette initiative a permis l'introduction d'un nouveau module de cours postuniversitaires, axé sur la « Protection des données à caractère personnel ». Ces cours sont dispensés par le président de l'Autorité de contrôle lui-même.

Les nombreuses réunions entre membres de l'institution académique et le président de l'Autorité de contrôle ont renforcé l'intérêt des étudiants pour la protection de la vie privée et des données à caractère personnel. On étudie ainsi de près la possibilité d'introduire des cours axés sur la protection des données personnelles et les activités de police. Des négociations sont par ailleurs en cours en vue d'inaugurer un cours sur la protection des données personnelles à l'université privée Hyperion.

Slovaquie

A. Mise en oeuvre de la directive 95/46/CE et autres développements législatifs

Transposition de la directive 95/46/CE

De sa propre initiative, le Bureau de la protection des données personnelles de la République slovaque tenait à harmoniser au mieux la loi n° 428/2002 Coll. sur la protection des données à caractère personnel, telle qu'amendée selon des dispositions récentes (ci-après désignée, « loi sur la protection des données personnelles ») avec la directive 95/46/CE. Il a donc consulté à ce propos la direction générale de la justice, de la liberté et de la sécurité de la Commission européenne. En janvier 2007, sur la base de ces consultations, la Commission européenne estimait que la situation en République slovaque était satisfaisante du point de vue de la protection des données personnelles. En 2008, la loi sur la protection des données personnelles sera néanmoins amendée pour tenir compte des développements juridiques et technologiques les plus récents au sein de l'Union européenne et de l'expérience acquise dans le domaine de l'application des dispositions légales en matière de protection des données personnelles.

Autres nouvelles mesures législatives

Le Bureau a rendu son avis sur 223 projets de lois, de réglementations et d'arrêtés du Gouvernement de la République slovaque. Ces propositions émanent pour la plupart du ministère de l'intérieur, du ministère de la santé et du ministère de l'agriculture de la République slovaque. Cette évolution montre une augmentation substantielle du nombre d'organismes de l'administration publique associés au processus législatif national mais aussi, une meilleure sensibilisation à ces questions, notamment la nécessité d'une coopération plus étroite avec l'Autorité de contrôle de la protection nationale des données à caractère personnel.

Fin 2007, la directive 2006/24/CE (directive sur la conservation des données) avait été transposée dans la législation slovaque, et la loi sur les communications électroniques amendée. La période de conservation des données opérationnelles, des données de localisation et des données sur les parties communicantes a été fixée à 6 mois pour les données transmises par l'Internet et à 12 mois pour les autres formes de canaux de communication.

En ce qui concerne les activités législatives en rapport avec la préparation à l'adhésion à Schengen, quelques amendements ont été proposés et apportés à une loi spéciale et à un décret gouvernemental, à savoir la loi du corps de police et un décret du ministère de l'intérieur. La proposition du Bureau de confier au ministère de l'intérieur le contrôle du Système d'information Schengen ainsi que de tous les autres systèmes d'information de la police a été acceptée. L'adoption de ce texte achève avec succès l'inclusion de la République slovaque au sein de l'espace Schengen.

B. Jurisprudence

En 2007, deux affaires remontant à plusieurs années ont refait surface. L'une d'elle concernait le ministère de la République slovaque, qui avait intenté une action contre le Bureau suite à sa décision, en 2006, déclarant illégale la publication du numéro national d'identification (le « numéro de naissance ») sur les pages Internet du Bulletin commercial. Conformément aux dispositions de la loi sur la protection des données personnelles, le Bureau avait ordonné que tous les numéros de naissance publiés sur Internet soient retirés du Web ou rendus illisibles. Le ministère a émis une objection et, s'opposant à cette décision, a demandé au Bureau de l'annuler, ce que celui-ci a refusé. Le ministère a donc utilisé son droit à la protection judiciaire et a porté l'affaire devant le tribunal régional. Fin janvier 2008, le tribunal a entièrement rejeté la plainte du ministère et confirmé la décision du Bureau.

Dans une affaire plus récente, une personne dont les données avaient été traitées a poursuivi en justice le Bureau, pour n'avoir pas pris de mesure légale à l'encontre d'une entreprise de publication de quotidiens qui avait autorisé la publication de données personnelles d'une personne sur son site Internet sans en informer cette dernière. Dans le même temps, le site Internet autorisait également toute personne à publier diverses opinions. Le requérant a avancé qu'une personne inconnue avait posté ses données personnelles, y compris son nom, son prénom et son adresse sur le site Internet. Il demanda donc au tribunal régional de dire que ses droits, tels

que stipulés dans la loi sur la protection des données personnelles, avaient été violés, alors qu'il était notoire qu'il avait lui-même et à plusieurs reprises déjà publié ses données personnelles sur d'autres sites. En novembre 2004, le tribunal régional estima que la procédure du Bureau s'alignait sur la loi relative à la protection des données personnelles. Le requérant interjeta appel contre le jugement. En mai 2007, la Cour suprême a totalement confirmé le verdict rendu par le tribunal régional, donnant ainsi raison au Bureau.

C. Questions diverses importantes

En 2007, 121 notifications ont été introduites auprès du Bureau par des personnes, parmi lesquelles certaines dont les données avaient été traitées. Elles affirmaient que les droits inscrits dans la loi sur la protection des données personnelles n'avaient pas été respectés. 27 autres notifications ont été reçues pour suspicion de violation de la loi sur la protection des données. L'inspecteur en chef du Bureau ordonna 125 actions d'office. Au total, le Bureau a ainsi traité 290 notifications en 2007. Ce nombre assez élevé inclut également des affaires datant de la fin 2006 qui n'avaient pas encore été résolues.

Il convient ici d'indiquer qu'en 2007, le département des inspections du Bureau a procédé au total à 102 inspections de contrôleurs et de responsables du traitement des systèmes d'information, et que 62 « demandes d'explication » ont été introduites. Il s'agit là d'une augmentation de 65% par rapport à 2006. In 2007, 104 avis contraignants ont par ailleurs été rendus. Le Bureau a aussi contrôlé des systèmes de vidéosurveillance existants, notamment ceux de la police urbaine.

En 2007, le Bureau a infligé sept amendes, les sanctions se situant dans la partie inférieure du barème des amendes.

En ce qui concerne les préparatifs en vue de l'adhésion au système Schengen et conformément aux dispositions de la loi sur les données personnelles obligeant les contrôleurs de données à communiquer aux personnes concernées des informations détaillées sur la collecte des données, le Bureau a procédé à des inspections au sein des représentations diplomatiques et des services consulaires de la République de Slovaquie en Serbie (Beograd), en Croatie (Zagreb), en Ukraine (Uzhorod), en Biélorussie (Minsk), dans la Fédération de Russie (Saint-Pétersbourg) et en Turquie (Ankara, Istanbul). Des inspections ont également eu lieu à l'Office de la police des douanes et des frontières de la République slovaque, à l'Office de criminalistique et d'expertise (département utilisant EURODAC) et auprès de la Direction des douanes de la République slovaque.

Affaire Swift

Dans un courrier électronique datant du 20 avril 2007, l'unité « Protection des données » de la direction générale de la Commission européenne en charge de la justice, de la liberté et de la sécurité avait sollicité la coopération du Bureau dans le cadre de l'enquête sur l'affaire SWIFT. L'unité demandait entre autres l'avis officiel du Bureau sur les mesures prises actuellement par les banques pour respecter leur obligation légale d'informer leurs clients (personnes concernées) du traitement de leurs données personnelles collectées dans le cadre des paiements bancaires effectués par le biais de SWIFT.

L'inspecteur en chef du Bureau a donc adressé un courrier à 24 institutions bancaires leur demandant d'examiner leurs obligations en rapport avec les systèmes de paiement transfrontaliers Swift, et ce dans le cadre des résultats de la supervision au titre de la section 19, paragraphe 4 de la loi n° 428/2002 Coll., qui permet de déterminer si le traitement des données personnelles implique ou non une quelconque violation des droits et des libertés de leurs clients (les personnes concernées).

La Banque nationale de Slovaquie a elle aussi reçu un courrier. Au moment de la collecte, du traitement et du transfert transfrontalier ultérieur des données personnelles, chaque banque est obligée d'informer suffisamment les personnes concernées des conditions dans lesquelles leurs données personnelles seront traitées (section 10, paragraphes 1 à 3 de la loi 428/2002 Coll. et articles 10 et 11 de la directive 95/46/CE). Le Bureau a demandé aux institutions bancaires de lui soumettre leurs positions détaillées indiquant les mesures et mécanismes particuliers qui ont déjà été

mis en œuvre ou qui doivent l'être pour respecter les tâches précisées aux points 5 et 6 de l'avis n° 10 sur le traitement des données SWIFT en se concentrant sur les points 5.3.2, 5.5, 6.1, 6.2, 6.5 et 6.6. Une institution bancaire ne prenant pas de mesure à cet effet était ainsi tenue de spécifier les mécanismes et les mesures particulières qu'elle compte prendre en sa qualité de responsable du traitement des données personnelles, et ce pour le 31 mai 2007 au plus tard. Sur la base de ces conclusions, le département des inspections du Bureau a formulé un avis pour la Commission européenne, lequel a été envoyé le 14 mai 2007 par le Président du Bureau à la CE. Fin août 2007, le questionnaire relatif au respect de l'obligation d'informer les clients respectifs des banques quant aux transferts de paiements internationaux exécutés par SWIFT était transmis à la CE.

Le traitement des données personnelles des clients d'entreprises de pompes funèbres

Le Bureau a inspecté les systèmes informatiques de plusieurs entreprises de pompes funèbres, l'objectif étant de s'assurer que tous les services de pompes funèbres étaient proposés et que les données personnelles des clients étaient traitées dans le respect de la loi sur la protection des données personnelles. Le Bureau a constaté que certains contrôleurs des systèmes d'information ne respectaient pas, à plusieurs égards, la législation slovaque en matière de protection des données personnelles.

Enregistrement spécial pour les données personnelles biométriques

Lors d'une inspection effectuée chez un célèbre fabricant d'électronique, le Bureau a constaté que le contrôleur n'avait pas fait enregistrer son système informatique de données biométriques. Or, la loi sur la protection des données personnelles oblige le contrôleur à soumettre le système informatique à un enregistrement spécial s'il envisage de procéder ou s'il procède déjà au traitement de données biométriques, sauf en ce qui concerne l'analyse ADN et du profil ADN de personnes physiques aux fins d'enregistrement ou d'identification préalable à l'accès à des installations sensibles spécialement protégées, à des locaux avec accès réservés ou à des appareils ou dispositifs techniques à haut risque et pour les besoins purement internes du contrôleur. Dans ce cas particulier, le Bureau a infligé une amende importante de 30 000,-SKK.

Communication illégale de données à caractère personnel par une société non bancaire de crédit

Une entreprise de recouvrement de crédits avait l'habitude d'envoyer à ses débiteurs un rappel en envoi non clos au moyen d'une carte de correspondance en couleur indiquant expressément que le destinataire était un «MAUVAIS PAYEUR» et qui indiquait le montant en souffrance. Un tel procédé équivalait en fin de compte à divulguer à des tiers la situation économique des personnes concernées, ce que n'exigeait pas l'objectif du traitement des données. Le Bureau a imposé au contrôleur de mettre fin à ce type de traitement de données personnelles. Le contrôleur s'y est opposé, car il perdait ainsi son instrument de pression psychologique à l'égard des débiteurs. Comme le contrôleur n'a pas introduit de recours dans les délais prévus par la loi, l'entreprise a finalement raté l'occasion de demander une protection efficace au tribunal. Le contrôleur a donc introduit auprès du Procureur général de la République slovaque une motion demandant l'examen de la légalité de l'avis du Bureau ainsi que l'annulation de l'avis. Le contrôleur avait invoqué comme raison la violation de son droit constitutionnel à la libre entreprise. Le Procureur a confirmé la légalité objective de l'ordre et son bien-fondé en l'espèce. Le contrôleur a alors interjeté appel auprès du Procureur supérieur, demandant un réexamen de l'affaire. Ce dernier a lui aussi confirmé le caractère correct de la procédure du Bureau et notifié au contrôleur qu'il n'examinerait plus aucune autre motion dans le cadre de cette affaire.

Divulgation illicite du numéro d'identification nationale (numéro de naissance)

En 2007, le Bureau a continué de suivre en permanence la situation en matière de protection des données personnelles en se concentrant tout particulièrement sur la publication des numéros d'identification nationale, le «numéro de naissance», sur Internet. Le Bureau a ordonné à plusieurs organes de remédier aux manquements identifiés, par exemple la direction fiscale de la République tchèque, une association de football, l'Office antitrust de la République slovaque, etc.

Scan et photocopie de documents sans le consentement de la personne concernée
Les documents ne peuvent être photocopiés ou scannés sans base juridique appropriée, à savoir, en Slovaquie, soit une loi spéciale, soit le consentement écrit de la personne concernée. Des inspections menées par le Bureau auprès de diverses entités publiques et privées ont montré que la grande majorité des contrôleurs ignoraient cette règle. Ils réalisaient donc généralement ce type de traitement en allant au-delà du seul objectif du traitement des données personnelles et ne sollicitaient pas le consentement en bonne et due forme des personnes concernées. Le Bureau a ainsi rendu des ordonnances contraignantes dans ce domaine.

Flux de données transfrontaliers
En 2007, le Bureau a publié plus de 30 déclarations officielles (explications, interprétations de la loi) en rapport avec les flux transfrontaliers de données à l'intérieur et à l'extérieur de l'Union européenne. La détermination arbitraire du statut de contrôleur ou de responsable du traitement des données, observée dans diverses relations contractuelles, voire l'absence de définition contractuelle, oblige le Bureau à fournir des explications claires. Les données relatives à l'emploi figurent parmi les catégories de données personnelles les plus souvent transférées à l'étranger. Toutefois, les banques exigent également certaines données personnelles sensibles, comme le numéro d'identification nationale, ce qui semble excessif eu égard au service à réaliser. Les banques se justifient en évoquant leur système informatique interconnecté à l'échelon international et «en miroir». L'approbation du Bureau pour ces transferts a été requise essentiellement par des personnes du secteur financier (bancaire), et ces transferts ont été approuvés (neuf approbations au total). Dans d'autres cas, les motifs fort incomplets invoqués par les contrôleurs sollicitant l'accord du Bureau pour les transferts de données ayant lieu à l'échelon international ont abouti à un refus d'approbation. Au début du mois de janvier 2008, un accord a été délivré à un opérateur international de téléphonie mobile.

En vue de l'application précise des sections de la loi relative à la protection des données personnelles en rapport avec les flux transfrontaliers, le Bureau a publié sur son site Internet des lignes directrices pour les contrôleurs demandant l'accord du Bureau pour des transferts internationaux de données personnelles.

Sondage d'opinion publique
Un sondage d'opinion axé sur la sensibilisation aux questions en rapport avec la protection des données à caractère personnel a été réalisé par l'Institut d'enquêtes d'opinion de l'Office statistique de la République slovaque. Le sondage a montré que plus de la moitié des personnes interrogées sont conscientes de leurs droits en matière de protection des données personnelles. C'était la première fois, depuis 1999 qu'un imposant groupe de personnes interrogées (51%) se montrait à ce point conscientes de leurs droits en la matière, la sensibilisation ayant augmenté de 31%. Une augmentation de 6% avait été observée par rapport à 2005.

La plus forte prise de conscience a été observée chez les citoyens titulaires d'un diplôme universitaire (78%), les entrepreneurs (70%), les salariés (65%), et les titulaires d'un diplôme de l'enseignement secondaire (59%), ainsi que chez les citoyens vivant dans des villes de 50.000 à 100.000 habitants (59%). Les personnes n'ayant achevé que l'enseignement primaire sont par contre moins sensibilisées (30%). Un pourcentage relativement élevé de sensibilisation (entre 57% et 59%) a été mis en évidence dans une large frange de la tranche d'âge des 35 à 49 ans.

L'étude portant sur le sondage d'opinion publique est un document complexe axé sur divers aspects des obligations et des droits inscrits dans la loi sur la protection des données personnelles, par exemple la vulnérabilité des données personnelles à une possible mauvaise utilisation, la photocopie de documents originaux d'identité, la confiance des citoyens à l'égard de divers groupes de contrôleurs des données, les transferts de données personnelles aux pays tiers, le risque d'utilisation frauduleuse des données personnelles communiquées via l'Internet, le consentement des citoyens aux écoutes téléphoniques autorisées ou le contrôle des communications Internet dans le cadre de la lutte contre le terrorisme. Les détails de cette analyse figurent dans le Rapport annuel pour l'année 2007 du Bureau, qui est publié sur nos pages Web à l'adresse : www.dataprotection.gov.sk

Coopération internationale

Le 21 mars 2007, la seconde mission d'évaluation Sch–Eval de la Commission européenne s'est rendue en Slovaquie. Le Bureau, ainsi que d'autres autorités compétentes, ont fait l'objet d'une visite.

L'objectif de la mission d'évaluation était d'évaluer la mise en œuvre des recommandations formulées par la première mission d'évaluation, en février 2006. Les aspects suivants ont fait l'objet d'une évaluation :

1. Cadre législatif de mise en œuvre du SIS (système d'information Schengen), en particulier SIS One4All;
2. Les compétences, la capacité et le bon fonctionnement du Bureau;
3. Les procédures Schengen de délivrance des visas;
4. L'information du grand public à propos de l'application des droits des personnes dont les données personnelles font l'objet d'un traitement au sein du système d'information Schengen et sur les changements introduits avec l'entrée de la République slovaque dans l'espace Schengen.

Le Bureau s'est révélé capable d'assumer pleinement ses compétences en matière d'inspection des bases de données de la police. La Slovaquie a rejoint l'espace Schengen une minute après minuit, le 21 décembre 2007.

Dans le cadre de la mise en place de partenariats avec les autorités de protection des données d'Europe centrale et de l'Est, en plus de la Conférence annuelle des commissaires d'Europe centrale et de l'Est qui a eu lieu à Zadar en 2007, deux journées de négociations ont eu lieu en présence de délégués de l'autorité roumaine à Bratislava, en avril 2007. Cette réunion a aussi permis d'examiner les principaux aspects de la protection des données à caractère personnel, y compris les conditions réalisées et les mesures à prendre pour une adhésion à part entière de la République à l'espace Schengen. Les deux autorités ont conclu un accord de coopération.

Dans le cadre du projet international visant à créer et à améliorer les activités de la Direction pour la protection des données personnelles et l'application de la protection des données personnelles de l'ancienne République yougoslave de Macédoine, un employé du département des relations publiques du Bureau est intervenu en tant qu'expert des technologies de l'information et de la sécurité. En juin 2007, ce représentant du Bureau a été élu à la présidence de l'autorité de contrôle commune pour le système d'information douanière.

Slovénie

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La loi sur la protection des données personnelles (ci-après désignée LPD)[11] adoptée le 15 juillet 2004 par l'Assemblée nationale de la République de Slovénie a été amendée en 2007. L'adoption de la loi sur la protection des données personnelles, de la loi sur la Commissaire à l'information et la mise en place de la Commissaire à l'information ont assuré la transposition complète de la directive 95/46/CE dans la législation slovène.

La loi sur la protection des données personnelles a été amendée en 2007 par la loi portant modification de la loi sur la protection des données personnelles, adoptée par le Parlement de la République slovène le 12 juillet 2007[12]. Conformément à ces amendements, les contrôleurs de données comptant moins de 50 salariés (contre 20 précédemment) ne sont pas tenus de satisfaire aux obligations inscrites au second alinéa de l'article 25 de la loi sur la protection des données personnelles (obligation de fixer, dans la réglementation interne, les procédures et les mesures visant à garantir la sécurité des données personnelles et de définir les personnes responsables des systèmes d'archivage ainsi que les personnes qui, en raison de la nature de leur travail, procéderont au traitement de données personnelles). Ils ne doivent pas davantage s'acquitter des obligations énoncées aux articles 26 et 27 de la loi sur la protection des données personnelles (mise en place, pour chaque système de classement, d'un fichier relatif au système de classement et obligation de notifier à l'organisme national de contrôle – la Commissaire à l'information – l'établissement d'un système de classement ou de l'avertir préalablement à l'introduction d'un nouveau type de données personnelles dans le système de classement existant). Ces exemptions ne s'appliquent toutefois pas aux systèmes de classement conservés par les contrôleurs de données du secteur public, les notaires, les avocats, les détectives, les huissiers, les entreprises privées de sécurité, le personnel soignant privé, les prestataires de soins de santé ni les contrôleurs de données qui conservent des fichiers contenant des données personnelles sensibles et qui traitent des données personnelles sensibles dans le cadre de leur activité agréée.

Ces amendements ont également modifié la fréquence des demandes d'accès à l'information (art. 31 de la LPD). Ces demandes peuvent toujours être introduites en suivant la même procédure que celle applicable avant la modification de la loi, à savoir une fois tous les trois mois, mais une fois par mois pour les données personnelles sensibles et les données personnelles régies par les dispositions du chapitre 2, partie VI de cette loi (traitement des données dans le cadre de la vidéosurveillance). L'amendement ajoute toutefois la disposition suivante : lorsqu'il s'agit de garantir le traitement équitable, légal ou proportionné des données, particulièrement lorsque les données personnelles d'un individu conservées dans un fichier sont fréquemment mises à jour ou envoyées ou sont susceptibles d'être fréquemment mises à jour ou envoyées à des destinataires de données, le contrôleur de données devra autoriser la personne concernée à introduire sa demande dans un délai plus court, qui ne pourra cependant être inférieur à cinq jours à compter de la date à laquelle il a pu prendre connaissance des données personnelles le concernant ou à laquelle l'accès à cette information lui a été refusé.

L'amendement spécifie en outre que, de manière générale, le contrôleur de données doit permettre à toute personne qui le souhaite de consulter, transcrire et copier les données le concernant et obtenir un certificat conformément aux points 1 et 2 du premier paragraphe de l'article 30 de la LPD le jour même de la réception de la demande (alors que précédemment, le délai était de quinze jours à compter de la réception de la demande) et en tout cas dans les quinze jours. Ou alors, le contrôleur de données doit informer la personne par écrit, au plus tard dans les quinze jours, des raisons pour lesquelles il ne permet pas la consultation, la transcription, la copie ou la délivrance d'un certificat.

Concernant les dispositions relatives aux coûts des matériaux se rapportant aux demandes d'accès à des informations et que le contrôleur de données peut demander à la personne de payer pour la transcription, pour la copie

[11] Journal officiel de la République de Slovénie n° 86/2004.

[12] Journal officiel de la République de Slovénie n° 67/2007.

ou pour le certificat : l'extrait, la liste ou les informations se trouvent aux points 5 et 6, et l'explication, au point 7 du premier paragraphe de l'article 30 de cette loi. Le contrôleur de données ne peut demander à la personne de payer les coûts des matériaux que conformément à un tarif préalablement spécifié (publié par le ministère en charge de la justice, sur proposition de la Commissaire à l'information), tandis que la confirmation orale et la communication orale d'informations, ainsi que les explications données oralement seront gratuites. La loi précise par ailleurs que si malgré cette confirmation, cette information ou cette explication orale, la personne demande une confirmation, une information ou une explication sous forme écrite, le contrôleur de données devra la lui fournir.

Par ailleurs, la nouvelle loi convertit en euros toutes les amendes infligées pour des violations à la loi sur la protection des données à caractère personnel.

En 2007, la Commissaire à l'information a participé régulièrement à cinq groupes de travail de l'UE, tous axés sur la protection des données à caractère personnel, et il a rejoint les organes de protection des données personnelles des États membres (Groupe de travail « Article 29 », autorité de contrôle commune Europol, autorité de contrôle commune Schengen, autorité de contrôle commune des douanes et supervision d'Eurodac par le CEPD, réunion de coordination des autorités de protection des données (APD) sur le traitement des données à caractère personnel et dans différents contextes au sein de l'UE). Au sein du Groupe de travail « Article 29 », la Commissaire à l'information est également représenté dans le sous-groupe ITF.

La législation slovène a transposé la directive 2002/58/CE en amendant la loi sur les communications électroniques[13], adoptée le 9 avril 2004, et entrée en vigueur le 1er mai 2004. Le chapitre X de cette loi réglemente essentiellement la protection des données personnelles, le respect de la vie privée et la confidentialité dans les communications électroniques.

Le 28 novembre 2006, la Slovénie a adopté la loi portant modification de la loi sur les communications électroniques[14], transposant la directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications. Cette loi est entrée en vigueur le 27 décembre 2006. En vertu de celle-ci, tous les fournisseurs de services de télécommunications (accès à l'Internet, messagerie électronique, téléphone, téléphone mobile, etc.) de Slovénie doivent conserver pendant une période de deux ans les données relatives au trafic générées par les activités de leurs clients. Les dispositions de la loi relative à la conservation des données téléphoniques sont entrées en vigueur le 15 septembre 2007, tandis que celles relatives à l'accès à l'Internet, aux messageries électroniques et au protocole de téléphonie vocale sur Internet (VoIP, *Voice over Internet Protocol*) devraient entrer en vigueur le 15 mars 2009.

En 2007, la Commissaire à l'information a participé à l'équipe d'inspection chargée du contrôle annuel d'Europol par l'autorité de contrôle commune Europol. La commissaire a également inspecté l'unité nationale Europol.

Enfin, la Commissaire à l'information doit également contrôler l'application de l'Accord de Schengen, conformément à l'article 128 de la convention d'application, et assurer ainsi la fonction d'institution chargée d'exercer un contrôle indépendant sur la transmission de données à caractère personnel prévue par ladite convention.

B. Jurisprudence

La loi sur la protection des données à caractère personnel décrit également les conditions en vertu desquelles les mesures biométriques sont autorisées. La réalisation des mesures biométriques n'est autorisée qu'après réception de la permission de l'autorité de contrôle.

Il convient de souligner la tendance observée en 2007 à une augmentation de demandes en ce sens. En 2007, la Commissaire à l'information a ainsi reçu 40 demandes,

[13] Journal official de la République de Slovénie, n° 43/2004 et 86/2004.

[14] Journal officiel de la République de Slovénie, n° 129/2006.

dont 31 émanant du secteur privé et 9 du secteur public (contre 15 demandes au total seulement en 2006).

En 2007, la Commissaire à l'information a rendu au total 35 décisions en rapport avec la réalisation de **mesures biométriques**, dont 24 autorisant la réalisation de mesures biométriques. 2 demandes d'autorisation ont été rejetées, 1 demande n'a fait l'objet que d'une autorisation partielle et 10 autres demandes ont été refusées. La Commissaire à l'information a ainsi autorisé l'utilisation de mesures biométriques à l'entrée de locaux où était entreposé du matériel relatif à des programmes protégés et à l'entrée de zones où étaient conservés des documents contenant des secrets commerciaux d'entreprise et d'autres informations protégées. La Commissaire à l'information a par contre refusé la réalisation de données biométriques d'employés visant uniquement à contrôler leur présence sur le lieu de travail.

On remarquera également l'augmentation des autorisations de **connexion de systèmes de classement**. En 2007, la Commissaire à l'information a ainsi reçu 12 demandes (contre 7 en 2006) de connexion de systèmes de classement, et, au total, il a rendu 7 décisions en rapport avec la connexion de systèmes de classement.

Conformément à la loi sur la protection des données personnelles, le Contrôleur doit pouvoir s'appuyer, d'une manière générale, sur une base légale appropriée ou le consentement personnel de la personne concernée pour procéder au traitement des données ou pour les publier dans les médias. Toutefois, si, conformément au principe de proportionnalité, le droit à l'information garanti par la constitution l'emporte sur le droit à la protection des données à caractère personnel, la publication de données personnelles pourrait dans ce cas être licite. La LPD ne prévoyant pas d'exemption spécifique pour les médias, la mise en œuvre de la protection des données à caractère personnel et donc les dispositions de la LPD relatives à la liberté d'expression garantie par la constitution (mise en œuvre en pratique par la loi sur les médias publics[15]) doivent être interprétées comme obligeant les médias à respecter la LPD et donc le principe de proportionnalité tel qu'il est défini à l'article 3 de cette loi. En 2007, la Commissaire à l'information a lancé plusieurs procédures contre des médias qui violaient les dispositions de la loi relative à la protection des données à caractère personnel.

1. Dans un programme d'informations quotidien diffusé en soirée, un journaliste de l'une des principales chaînes de télévision a publié le contenu d'une plainte pénale, de manière non anonyme, rendant ainsi publiques les données personnelles suivantes des personnes dénoncées : nom, date de naissance, adresse et numéro d'identification personnelle. Le contrevenant ne disposait d'aucune base légale ni du consentement des personnes intéressées l'autorisant à publier ces données personnelles. En outre, dans ce cas, il n'y avait pas prévalence du droit du public à avoir connaissance des données à caractère personnel ayant été publiées. La quantité de données personnelles publiées n'était pas appropriée compte tenu de l'objectif de leur publication, ce qui constituait dès lors une violation du principe de proportionnalité. La violation du droit a consisté dans le traitement de données personnelles – en l'occurrence les dates de naissance, adresses et numéros d'identification personnelle de trois personnes – qui avaient été publiées de manière illicite. Le journaliste a immédiatement retiré du site Internet les informations controversées et pris les mesures pour éviter toute nouvelle violation du droit.

2. La Commissaire en charge de l'information a mis en évidence, lors d'une procédure d'inspection, une violation de la LPD commise par la publication d'une carte d'identité révélant les données personnelles suivantes d'une personne : photo, nom, date et lieu de naissance, numéro d'identification personnelle, lieu d'émission, date d'émission et d'expiration de la carte d'identité et signature. Comme il ne s'agissait pas d'une personne publique *par excellence*, les médias n'avaient pas le droit de porter ainsi atteinte à sa vie privée. Clairement, les détails figurant sur la carte d'identité n'ont pas susceptibles d'être intéressantes dans un débat public sur des questions d'intérêt général ou d'intérêt public. Par ailleurs, dans un cas précis, la Commissaire a avancé que, pour l'intérêt public, en ce qui concerne l'information relative aux affaires courantes, et même en vue de délivrer un mandat visant à amener ou arrêter une personne accusée, il suffit de révéler certains éléments de son identité (photo et nom) et non toutes les données

[15] Journal officiel de la République de Slovénie, n° 110/2006.

à caractère personnel la concernant. La publication d'une partie seulement des données personnelles garantissait en ce cas une information suffisante du public. Toutes les autres données relatives à cette personne ne constituent pas des informations importantes du point de vue de l'intérêt public et de la liberté d'expression puisqu'il suffit de publier des photos avec le nom complet pour que la personne puisse être identifiée.

Le principe de proportionnalité n'était pas respecté étant donné qu'il n'existait aucune base légale appropriée autorisant la publication des données personnelles susmentionnées de la personne concernée. La publication de ces données sur le site Internet constituait dès lors une violation de l'article 3 de la LPD. La publication des données personnelles n'était pas proportionnée au but poursuivi.

Après avoir servi la décision réglementaire de la Commissaire, les médias ont retiré dans les délais les irrégularités identifiées et ont pris les mesures pour éviter de nouvelles violations de la LPD.

3. Une autre entreprise du monde des médias a elle aussi publié les données personnelles de la personne dont question au point 2, à savoir la photo, le nom, la date et le lieu de naissance, le numéro d'identification personnelle (EMŠO), le sexe, le numéro de la carte d'identité, le lieu d'émission et date d'expiration de la carte d'identité et la signature sur son site Internet. Pour les raisons évoquées plus haut, au point 2, et après décision réglementaire de la Commissaire, les médias ont retiré les données personnelles excessives du site Internet.

4. Lors d'une autre inspection, la Commissaire à l'information a mis en évidence une violation de la loi sur la protection des données consistant en la publication de la photographie figurant sur un passeport dans la version papier d'un journal, rendant ainsi publiques les données personnelles suivantes du titulaire du passeport: photo, nom, nationalité, lieu et date de naissance, sexe, date d'émission et d'expiration du passeport, numéro de passeport, numéro d'identification (EMŠO), autorité émettrice et signature. Le responsable du traitement des données ne disposait pas d'une base légale autorisant le traitement de ces données, à savoir la publication de données personnelles (ni disposition légale, ni consentement personnel de la personne concernée), et il ne s'agissait pas d'un cas de prévalence du droit du public à l'information, qui aurait pu permettre la publication de toutes les données personnelles en question. De la même façon, et comme dans les affaires précitées, les données personnelles publiées n'étaient donc pas proportionnées à l'objectif de la publication.

5. Un quotidien a publié une plainte pénale déposée par la police contre une personne privée. La Commissaire a estimé qu'il s'agissait là d'un traitement illicite étant donné que les données personnelles suivantes avaient été publiées : nom, lieu et date de naissance, adresse, nationalité et numéro d'identification personnel (EMŠO). La Commissaire à l'information a ainsi mis en évidence une violation de la loi relative à la protection des données personnelles en raison de la publication des données personnelles précitées et ce sans base légale appropriée ni consentement de la personne concernée.

En 2007, la Commissaire à l'information a rendu **plusieurs décisions qui ont été largement relayées dans les médias nationaux** :

1. La Commissaire à l'information a lancé une procédure d'inspection contre toutes les pharmacies et les compagnies d'assurance slovènes proposant des assurances volontaires de soins de santé, et ce en raison de la polémique publique autour du différend opposant différentes pharmacies et la société d'assurance de soins de santé Vzajemna. Dans sa décision, la Commissaire a interprété sous quelle forme les données personnelles en rapport avec l'assurance volontaire de soins de santé pouvaient être transférées, car le transfert de données personnelles faisait également l'objet d'un désaccord entre pharmacies et compagnies d'assurance. Comme l'a établi la procédure d'inspection, les données personnelles suivantes des personnes assurées sont échangées entre les compagnies d'assurance et les pharmacies : numéro de la police d'assurance soins de santé, numéro de la carte d'assurance soins de santé, date de naissance, sexe, nom ou numéro de code et quantité et date du médicament ou du matériel médical délivré.
La législation existante autorise les compagnies d'assurance de soins de santé à se procurer des

données personnelles. La Commissaire a souligné, en particulier, que les compagnies d'assurance (ainsi que tous les autres responsables de fichiers de données, y compris, dans ce cas, les pharmacies) devaient traiter ces données conformément à l'objectif de la collecte de données (dans ce cas-ci, les données personnelles ne pouvaient être utilisées que pour les régimes d'équilibrage et le règlement de pertes, et, avec les pharmacies, uniquement pour le transfert de données aux compagnies d'assurance, pour le contrôle de l'exactitude des règlements effectués ou pour d'autres objectifs éventuels définis par une autre loi). En ce qui concerne en particulier les compagnies d'assurance, ces données ne peuvent être intégrées à d'autres fichiers en rapport avec d'autres transactions d'assurance.

Une obligation légale de transfert des données personnelles existe en vertu du paragraphe 1 de l'article 22 de la loi sur la protection des données. Les contrôleurs (pharmacies) sont donc tenus de transmettre ces données. Ils n'ont pas le droit discrétionnaire d'en décider autrement. Les pharmacies et les compagnies d'assurance ne doivent pas utiliser des indemnisations de transmission pouvant s'avérer inadéquates (trop faibles) au détriment de l'intérêt public de la République de Slovénie et des assurés. En particulier, elles ne sont pas autorisées à négliger leur devoir de protection des données à caractère personnel, par exemple en transférant ces données sous un format électronique non sécurisé ; elles ne sont pas autorisées – car c'est contraire à la loi – à déplacer la charge pour obtenir le remboursement des médicaments payés et pour obtenir la transmission des données personnelles des assurés (en leur demandant de fournir eux-mêmes les reçus aux compagnies d'assurance). La loi stipule clairement que les données ne peuvent être transférées que des pharmacies aux compagnies d'assurance.

Les coûts controversés de ce service que les pharmacies offrent aux compagnies d'assurance pourraient bien être à l'origine d'autres actions en justice, mais comme la loi stipule clairement qui a l'obligation de transférer les données, ces transferts actuels ne peuvent s'arrêter pendant le règlement du litige. Comme les données transférées incluent des données personnelles sensibles (sur l'état de santé des personnes), la Commissaire à l'information a estimé que les données devaient être transférées sous forme d'un code de signature électronique afin de les rendre parfaitement illisibles et non identifiables.

Une des personnes tenues de s'exécuter a interjeté appel contre la décision de la Commissaire. Le tribunal a ordonné, dans une action administrative, l'annulation de la décision de la Commissaire.

2. La Commissaire à l'information a reçu plusieurs plaintes émanant de personnes ayant reçu des formulaires de déclaration fiscale sous pli non fermé et préremplis ou des formulaires mal scellés, de sorte que tout le monde pouvait lire les informations fiscales y figurant. La Commissaire a lancé une procédure d'inspection contre l'administration fiscale de la République de Slovénie et contre le ou les responsables y travaillant afin d'établir si les mesures de protection des données personnelles avaient été suffisamment respectées pendant l'envoi des formulaires de déclaration préremplis. Il a également lancé une action pour violation de la loi contre le responsable contractuel de la protection des données.

L'administration fiscale et son responsable contractuel du traitement des données ont violé la loi en ne garantissant pas une protection adéquate des données personnelles lors de l'envoi des formulaires de déclaration fiscale, permettant ainsi à des tiers non autorisés d'examiner les données personnelles concernées et donc de les traiter. Conformément à l'article 24 et à l'article 25 de la LPD, l'administration fiscale est tenue, en sa qualité de responsable de la protection des données, d'assurer la protection des données personnelles extraites de ses fichiers, y compris lors de leur transmission à d'autres utilisateurs ou lors de l'envoi des déclarations fiscales à chaque contribuable. Cette obligation générale inclut l'obligation de veiller à ce que tout document contenant des données personnelles sensibles de contribuables (confidentialité des données fiscales) soit envoyé dans des enveloppes qui empêchent des tiers d'examiner les données sans détérioration visible de l'enveloppe et dont l'impression empêche la lecture du contenu (y compris des données fiscales) à la lumière habituelle.
L'administration fiscale de la République de Slovénie a remédié à son erreur et a donc arrêté d'envoyer

des formulaires de déclaratoni fiscale préremplis, et ce dès la réception des premières plaintes émanant de particuliers. Tous les autres envois ont été ensuite sécurisés à l'aide d'un film plastique, et scellés de façon à assurer une protection adéquate des formulaires préremplis.

En 2007, la Commissaire à l'information a **introduit deux requêtes pour examen de la constitutionnalité de lois**.

Pendant son mandat, la Commissaire à l'information a introduit deux demandes pour un examen de la constitutionnalité de certaines dispositions de quatre lois (deux en 2007). Elle a en outre contribué à la préparation de nombreux autres textes de législation nationale en ce qui concerne la protection des données personnelles.

1. En 2007, le Tribunal constitutionnel a rendu une décision[16] sur la demande d'examen de la constitutionnalité du paragraphe 1 de l'article 96, du paragraphe 2 de l'article 98, de l'article 100, des paragraphes 5 et 6 de l'article 103 et du paragraphe 1 de l'article 114 de la loi sur l'enregistrement des biens immobiliers[17] introduite par la Commissaire en décembre 2006.

Le tribunal a accédé à la demande de la Commissaire à l'information ayant trait en partie à la publicité du registre immobilier et aux personnes physiques (données relatives au propriétaire, à l'occupant, au locataire et au gérant immobilier – leur nom et leur numéro d'identification unique – EMŠO), qui faisait l'objet de la plainte principale adressée par la Commissaire à l'encontre du législateur. La publicité du registre immobilier permet en effet la publication du nom de la personne et de son numéro d'identification personnel dans le domaine immobilier. Ces données étant alors accessibles via l'Internet, les données personnelles collectées pouvaient être utilisées à d'autres fins, ce que le tribunal a estimé anticonstitutionnel. Le tribunal a confirmé sa décision selon laquelle la publication du registre immobilier entraînerait un préjudice irréparable pour les personnes concernées.
2. Examen de la constitutionnalité du point 7, paragraphe 2, article 62 et paragraphe 2, article 62d de la loi sur les soins de santé et l'assurance-santé[18] , qui réglementent le traitement et le transfert de données nécessaires à la mise en œuvre des régimes passibles de mesures compensatoires, d'une part, et de l'article 2 des règles relatives à la mise en œuvre d'une assurance santé complémentaire que les fournisseurs de services de santé sont tenus de respecter[19] , d'autre part. La Commissaire à l'information a avancé que les dispositions contestées de cette loi sont en contradiction avec l'article 38 de la constitution de la République de Slovénie en ce qui concerne la spécification requise du type de données personnelles à traiter. Les dispositions contestées stipulent une clause générale et l'obligation de transmettre toutes les données nécessaires ou toutes les données nécessaires à la mise en œuvre des régimes passibles de mesures compensatoires. La réglementation légale existante ne spécifie pas les types de données personnelles à traiter, ce qui conduit à plusieurs interprétations et, partant, à un traitement de données personnelles potentiellement disproportionné. D'où une violation du principe constitutionnel de proportionnalité selon lequel toute atteinte au droit protégé par la constitution doit être proportionnée aux objectifs qu'elle entend réaliser. De même, le fait que l'étendue des données collectées et le type de données soient définis par un règlement d'application (et non une loi) est contraire à la constitution. La définition légale qui stipule que « toutes les données nécessaires » doivent être transmises n'est pas immuable et ne définit donc pas de manière suffisamment spécifique le traitement des données personnelles comme l'exige l'article 38 de la constitution, puisque cette définition admet trop largement que le traitement des données personnelles soit régi par un règlement d'application.

3. Examen de la constitutionnalité du paragraphe 4, article 47, de l'alinéa 1, point 1, paragraphe 2 de l'article 58, du point 5, paragraphe 1, l'article 123, des points 3 et 4, article 165, du point 2, paragraphe 2, article 247, du point 3, paragraphe 1, article 334, du point 3, paragraphe 1, article 432 et du point 1, paragraphe 1, article 543 de la loi relative au marché des instruments financiers[20] qui, de l'avis de la Commissaire à l'information, sont en contradiction avec l'article 38 de la constitution de

[16] Journal officiel de la République de Slovénie, n° 65/2007.

[17] Journal officiel de la République de Slovénie, n° 47/2006.

[18] Journal officiel de la République de Slovénie, n° 72/2006 et 91/2007.

[19] Journal officiel de la République de Slovénie, n° 7/2007.

[20] Journal officiel de la République de Slovénie n° 67/2007 et 100/2007.

la République de Slovénie en raison d'une spécification insuffisante du type de données personnelles à traiter.

La loi controversée ne spécifie ni la finalité ni l'étendue des données personnelles à recueillir ou à traiter. Les dispositions controversées évoquent le traitement de données personnelles, sans spécifier le type de données soumises au traitement. La question de l'étendue des données à traiter et à collecter dépend alors d'une décision de la Securities Market Agency qui peut être arbitraire. Pour ces définitions, la réglementation légale existante renvoie au règlement d'application, ce qui est contraire à la constitution. L'étendue des données personnelles et leur type devraient être entièrement régis par la loi.

L'imprécision juridique et l'absence de spécification de la base légale définissant le traitement des données personnelles pourraient aboutir à des interprétations différentes, et dès lors à un traitement disproportionné de données personnelles. Il s'agirait alors d'une violation du principe selon lequel toute mesure diminuant la protection d'une valeur ou d'un bien doit être proportionnée à l'importance des objectifs définis par la loi. Par conséquent, l'interférence légitime avec un droit devrait être réduite au niveau le plus faible permettant la réalisation des objectifs définis ; ainsi un équilibre raisonnable sera atteint entre la valeur de ces objectifs et la gravité de l'atteinte aux droits d'une personne.

C. Questions diverses importantes

La loi relative à la protection des données personnelles décrit de manière très détaillée les conditions dans lesquelles la vidéosurveillance d'entrées de locaux d'entreprises, d'immeubles à appartements et d'espaces de travail peut être autorisée. En vertu de ces dispositions, les personnes réalisant ce type de vidéosurveillance ne doivent pas solliciter l'autorisation de l'organisme de contrôle. Ces dernières sont uniquement tenues d'aligner la mise en œuvre de la vidéosurveillance sur les dispositions légales, c'est-à-dire adopter une décision de vidéosurveillance, publier une notification appropriée, informer par écrit le personnel, obtenir l'accord des copropriétaires, consulter les syndicats, etc. Toutefois, de nombreux contrôleurs n'ont toujours pas adapté leur pratique aux dispositions légales, ce qui a conduit à de nombreux appels auprès de l'autorité de contrôle.

À plusieurs reprises, les suspicions de violation de la LPD concernaient la collecte illicite de données à caractère personnel comme la collecte de données sur la participation à divers concours de jeux d'argent, sur des contrats avec des opérateurs des télécommunications ou dans le cadre de la surveillance de membres du personnel par l'employeur. Des suspicions ont également été mises en évidence dans des domaines comme le marketing direct, la publication illicite de données personnelles (sur différents panneaux d'affichage d'immeubles résidentiels, au travail), la protection inadéquate de données personnelles et la transmission de données personnelles à des utilisateurs non autorisés. Parmi les domaines où les inspections ont révélé de graves manquements, retenons la non-existence d'une base légale pour le traitement de données (dans la loi ou sous la forme du consentement de la personne concernée), la protection inadéquate de données personnelles, le non-enregistrement du système de classement de données dans le registre, ainsi que le traitement de données personnelles sensibles.

Fin 2007, environ 10 000 contrôleurs de données à caractère personnel avaient renvoyé des informations sur les systèmes d'archivage de données à caractère personnel qu'ils géraient. (Suite aux amendements à la LPD entrés en vigueur en 2007, le nombre de contrôleurs tenus de renvoyer des informations sur ces systèmes d'archivage de données a considérablement diminué.) Le registre des systèmes d'archivage est publié sur la page Internet de la Commissaire à l'information, afin de permettre à tout un chacun de s'informer aisément sur les systèmes d'archivage gérés par les contrôleurs de données de la République slovène, de consulter les informations sur les systèmes d'archivage gérés par les différents contrôleurs, de se renseigner sur les types de données personnelles figurant dans les systèmes d'archivage, sur l'objectif du traitement, etc.

Inspections (au 1er décembre 2007, onze contrôleurs travaillaient pour le compte de la Commissaire). En 2007, la Commissaire à l'information a reçu **406** demandes et plaintes (179 du secteur public et 227 du secteur privé) en rapport avec une suspicion de violation des dispositions de la LPD, contre **231** (88 pour le secteur public et 143 pour le privé) en 2006. Il s'agit là d'une augmentation de 76%. La plupart des plaintes ont

concerné la divulgation de données personnelles à des utilisateurs non autorisés, une collecte illicite ou excessive de données personnelles, une vidéosurveillance illicite, une protection insuffisante des données personnelles, une publication illicite de données personnelles, etc. On a donc noté une augmentation significative du nombre de procédures administratives : 133 en 2007 contre 41 l'année précédente.

Le nombre de demandes d'**opinions et de clarifications écrites** reçues par la Commissaire a également augmenté de manière significative, passant de 616 en 2006 à 1144 en 2007 (et même seulement 34 en 2005). Cette évolution reflète incontestablement une prise de conscience croissante du droit au respect de la vie privée rendue possible par la mise en œuvre d'une loi moderne sur la protection des données personnelles. Nous espérons que cette prise de conscience améliorée soit aussi liée à la campagne de sensibilisation et à la transparence des travaux de la Commissaire à l'information.

Espagne

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La directive 95/46/CE du Parlement européen et du Conseil a été transposée en droit national par le biais de l'adoption de la loi organique 15/1999 du 13 décembre relative à la protection des données à caractère personnel.

1. Arrêté royal 1720/2007 du 21 décembre, portant approbation du règlement d'application de la loi organique 15/1999 relative à la protection des données à caractère personnel

L'approbation de ce règlement d'application représente un pas important dans le processus législatif concernant la protection des données en Espagne. Ce règlement vise à offrir toute la certitude juridique nécessaire dans le domaine de la protection des données, aspect tellement essentiel des droits fondamentaux, et renforce les textes précédents de l'Agence espagnole de protection des données. Il a également pour objectif de répondre aux questions les plus fréquemment posées et de résoudre les problèmes d'interprétation qui demeurent, en particulier ceux qui peuvent avoir une plus grande importance. Les commentaires et les observations des autorités actuelles des Communautés autonomes ont été pris en considération, tout comme ceux de plus de soixante entités et associations défendant les droits et les intérêts concernés par ce règlement.

Ce règlement inclut explicitement dans son champ d'application les fichiers non automatisés et le traitement des données (sur papier), et définit des critères spécifiques pour les mesures de sécurité les concernant. Il précise aussi le cadre territorial d'application et prévoit que toutes les formes de traitement sont soumises à ses dispositions si le droit espagnol s'applique, conformément au droit public international, ou lors de l'utilisation de ressources situées sur le territoire espagnol, sauf en cas de transit uniquement.

La disposition qui prévoit l'autorisation du traitement de données nécessaire dans l'intérêt légitime poursuivi par le contrôleur des données revêt une importance particulière.

Tout aussi importante, une procédure définie dans ce règlement garantit que toute personne peut prendre connaissance de l'usage qui sera fait des données avant de consentir à leur collecte et à leur traitement. Il est important de souligner par ailleurs l'adoption de dispositions spécifiques concernant l'obtention du consentement des mineurs d'âge, qui, s'ils sont âgés de moins de 14 ans, doivent bénéficier de l'aide de leurs parents ou du tuteur légal.

Dans la quête d'une meilleure protection du droit des personnes à vérifier l'exactitude de leurs données personnelles et l'usage qui en est fait, le contrôleur des données est explicitement tenu de leur proposer un moyen simple et gratuit d'accéder à leurs données, de les rectifier, de les supprimer ou de les contester. Dans le même esprit, il est interdit d'exiger de ces personnes d'avoir recours à l'envoi de plis recommandés ou autres ou à l'utilisation de moyens de télécommunication impliquant le paiement de frais supplémentaires. Enfin, ce règlement n'est pas applicable aux personnes décédées pour éviter de placer leurs proches dans des situations pénibles, mais ceux-ci peuvent informer le contrôleur du décès et solliciter la suppression des données.

Il décrit également en détail les règles applicables aux instances de traitement des données. Autre innovation, la mise en place d'un système détaillé de traitement concernant, d'une part, la solvabilité financière et le potentiel d'emprunt et, d'autre part, les activités de recherche en matière de publicité et de marketing, qui met en application des dispositions spécifiques de la loi organique 15/1999.

Ce règlement traite par ailleurs des transferts internationaux de données et instaure les règles concernant un régime systématique qui offre au directeur de l'Agence espagnole de protection des données la possibilité de déclarer adéquat le niveau de protection des données dans un pays à défaut d'évaluation par l'Union européenne, ce qui clarifie la situation dans laquelle des garanties peuvent être apportées pour permettre au directeur d'autoriser un transfert. Sont également visées dans ce cadre les « règles d'entreprise contraignantes » et les codes internes des groupes multinationaux. Enfin, ce règlement définit les procédures que l'Agence espagnole de protection des données doit appliquer dans l'exercice de ses

fonctions et étend son mandat pour lui permettre de collaborer avec ses homologues dans les Communautés autonomes.
https ://www.agpd.es/upload/English_Resources/reglamentolopd_en.pdf

2. Loi organique 10/2007 du 8 octobre réglementant la base de données ADN de la police

Après la signature du traité de Prüm, en mai 2005, il s'est révélé nécessaire de fusionner les bases de données de la police contenant des données génétiques qui étaient valides en Espagne jusqu'alors. Cette loi organique réglemente les bases de données de la police qui contiennent des identifiants ADN obtenus lors d'enquêtes criminelles. Ces identifiants ne donneront des informations génétiques que sur l'identité des personnes et leur sexe (ADN non codant). Cette loi définit par ailleurs les garanties qui s'appliqueront au transfert de ces informations aux forces de sécurité habilitées et précisent la durée de la période pendant laquelle ces données pourront être conservées. Les données ne pourront être utilisées que par les instances dûment habilitées et dans le cadre d'enquêtes criminelles. Elles seront conservées jusqu'à prescription des crimes.

3. Loi 37/2007 du 16 novembre sur la réutilisation des informations du secteur public

Cette loi transpose la directive 2003/98/CE en droit national. Elle s'applique aux documents que le secteur public peut mettre à la disposition des citoyens et des entreprises pour leur permettre d'exploiter les possibilités que ce type d'information peut receler, dans le but de contribuer à la croissance économique et à la création d'emplois et d'améliorer la transparence du secteur public. Comme la directive, cette loi ne change rien aux droits et obligations prévus dans la loi espagnole sur la protection des données.
http ://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/19814 (en espagnol).

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

Cette directive a été transposée en droit national par la loi 32/2003 du 3 novembre sur les télécommunications, mise en application par l'arrêté royal 424/2005 du 15 avril qui réglemente les services de communication électronique, le service universel et la protection des utilisateurs.

1. Loi 25/2007 du 18 octobre sur la conservation des données dans le cadre des services de communication électronique et de réseaux publics de télécommunications

Cette loi qui transpose la directive 2006/24/CE sur la conservation des données prévoit la conservation des données relatives aux communications électroniques pour une durée de 12 mois dans l'intérêt de la sécurité publique. Les données relatives aux appels n'ayant pas abouti et aux cartes prépayées doivent également être conservées. Ces informations ne pourront être transférées aux forces de sécurité que sur ordonnance du tribunal et uniquement à des agents habilités.
http ://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/22440 (en espagnol).

2. Loi 11/2007 du 22 juin sur l'accès des citoyens aux services publics par voie électronique

Cette loi a pour objet d'intensifier le recours aux moyens électroniques dans les relations entre les services publics et les citoyens et d'améliorer l'accessibilité universelle à l'information et aux services publics et l'interopérabilité entre les services publics. Elle érige en droit pour les citoyens et en obligation pour les services publics l'accès sûr et total à ce type de moyens. Il va de soi que le traitement des données doit respecter les droits et obligations prévus dans la loi espagnole sur la protection des données, ce qui garantit notamment que les données obtenues par voie électronique doivent être destinées à l'usage précis pour lequel elles ont été adressées à une instance administrative.

Conséquence de l'adoption de cette loi, le journal officiel espagnol et les autres journaux officiels seront publiés en version électronique. De même, cette loi, qui a valeur de loi fondamentale, doit être adoptée par les Communautés autonomes (notamment dans la Communauté autonome du Pays basque par le biais du décret 232/2007 du 18 décembre).
http ://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/12352 (en espagnol).

3. Loi 56/2007 du 28 décembre sur les mesures visant à promouvoir la société de l'information

Cette loi modernise à plusieurs égards la législation sur la vente et la facturation par voie électronique afin de sécuriser les relations entre utilisateurs et consommateurs et fournisseurs de services électroniques, lesquels doivent garantir le respect de la loi espagnole sur la protection des données lors du traitement des données.

De plus, les entreprises qui fournissent des services d'une importance économique particulière doivent permettre aux personnes concernées d'exercer aisément leur droit à accéder à leurs données, à les rectifier, à les supprimer et à les contester par voie électronique.
http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/22440 (en espagnol).

B. Jurisprudence

L'analyse du degré de certitude juridique quant à l'application de la loi organique sur la protection des données à caractère personnel (LOPD) passe par l'analyse de la mesure dans laquelle les décisions de l'Agence espagnole de protection des données (AEPD) sont suivies ou non par les tribunaux. La Cour d'examen de la constitutionnalité des lois du tribunal national a prononcé 158 jugements, et la Cour suprême, 13 jugements et 2 actes de refus. Les affaires les plus importantes sont mentionnées ci-dessous :

1. Tribunal national

- Envoi massif de courriers électroniques publicitaires non sollicités (spam).
- Le jugement du 25 octobre 2007 confirme que la publication à dessein par une entreprise des données personnelles d'un citoyen sans son consentement constitue une infraction au droit à la protection des données.
- Le jugement du 14 novembre 2007 repose sur l'interprétation selon laquelle la réglementation sur la protection des données et sur l'autonomie des patients n'impose pas l'envoi de tests de diagnostic.
- Le jugement du 19 décembre 2007 analyse l'antagonisme entre deux droits fondamentaux, en l'occurrence la liberté d'affiliation syndicale et la protection des données à caractère personnel, et conclut à la prééminence du premier.
- Arrêt de la Cour suprême espagnole sur l'apostasie. La décision de l'AEPD qui reconnaît aux citoyens le droit de ne pas figurer au registre des baptêmes et d'exiger leur radiation de ce registre, a été contestée par l'Archevêque de Valence qui s'est pourvu en appel devant la Cour suprême nationale. Celle-ci a confirmé la décision de l'AEPD. Plusieurs aspects de son arrêt méritent d'être soulignés : les registres de baptême sont à considérer comme des fichiers de données personnelles au sens de la LOPD, et le refus d'en supprimer des données peut constituer une infraction au principe de la qualité des données.

2. Cour suprême

Il convient d'insister sur le fait que la Cour suprême a confirmé les décisions de l'AEPD dans 11 des 13 affaires qui lui ont été soumises dans cette matière.

Parmi ses jugements, plusieurs sont à citer à titre de référence :

- Le jugement du 16 février 2007 rejette l'appel contre le jugement du Tribunal national, qui a rejeté l'appel en annulation de l'instruction 1/1995 adoptée par l'AEPD. Dans son jugement, la Cour suprême admet que l'AEPD peut adopter des instructions pour encadrer les activités des opérateurs en matière de traitement automatisé, de façon à ce que celles-ci respectent les principes de droit, de manière obligatoire et avec effet ad extra, dans des termes similaires à ceux employés pour d'autres régulateurs par le même tribunal.
- Le jugement du 27 mars 2007 confirme l'argument de l'AEPD qui estime contraire à la LOPD la transmission par un opérateur [de télécommunication] de données sur ses clients à un tiers pour permettre à celui-ci d'évaluer leur solvabilité financière.
- Le jugement du 17 avril 2007 déclare conformes à la loi les amendes infligées par l'AEPD à un certain nombre d'entités qui ont participé au processus de sélection de candidats à une émission télévisée car certains des mandats prévus portaient sur l'état de santé des candidats, et les mesures de sécurité imposées par la réglementation sur la protection des données n'ont pas été prises.
- Le jugement du 12 décembre 2007 déclare conforme à la loi l'argument de l'AEPD qui a déclaré illégal le traitement des données sur l'état de santé d'employés demandé

par un employeur à un tiers pour étudier les causes d'absentéisme parmi les membres de son personnel.

3. Décisions de l'AEPD

En 2007, 1 624 plaintes ont été déposées par des citoyens à l'AEPD, soit une augmentation d'environ 7 %. Au total, 1 263 enquêtes ont été ouvertes par l'AEPD à la suite de plaintes ou sur l'initiative de son directeur. En 2007, l'AEPD a intenté 399 procédures d'infraction, soit 32,5 % de plus qu'en 2006. Au total, l'AEPD a infligé 19,6 millions d'euros d'amendes.

Le nombre de demandes en faveur de la protection des droits a fortement augmenté (879 au total), tout comme la proportion de celles qui ont été acceptées (54 %). Ces demandes reflètent les mêmes préoccupations que celles énoncées ci-dessus, et les droits les plus souvent accordés sont le droit de suppression (62 %) et le droit d'accès (32 %).

En 2007, le droit de suppression des données a très souvent été invoqué à cause de l'affaire spécifique de la suppression des données dans les registres de baptême de l'Église catholique : sur les 896 procédures intentées pour la protection des droits, 304 (soit 34 %) concernent ce droit spécifique.

Les autres demandes de suppression soumises par les citoyens ont essentiellement porté sur les faits suivants :

- l'inclusion abusive, par des institutions financières, de données de clients dans des fichiers d'information sur la solvabilité et le potentiel d'emprunt, et la suppression de ces données à la fin de la relation légale entre les clients et leur institution financière ;
- la suppression de données des fichiers d'opérateurs de télécommunication dans le cas d'un changement d'opérateur auquel l'abonné n'a pas consenti ;
- la suppression de données sur l'Internet (forums de discussion, YouTube) ;
- l'accès aux dossiers d'anamnèse clinique.

La répartition des amendes par secteur d'activité montre que c'est le secteur des télécommunications qui a été le plus visé (112 procédures clôturées). Viennent ensuite les institutions financières (80) et les communications marketing et les courriers électroniques non sollicités (spam) (37). Plusieurs des décisions les plus pertinentes sont présentées ci-dessous.

- **Vidéosurveillance :** l'AEPD a ouvert de son propre chef une enquête sur l'enregistrement par caméra vidéo d'images dans une rue de Madrid et leur diffusion via le site YouTube, afin de déterminer si ces faits constituaient une infraction grave à la LOPD, passible d'une amende pouvant aller jusqu'à 600 000 euros.
- **Emule :** l'AEPD a infligé une amende pour cause de diffusion de données personnelles sur l'Internet via le système de partage de fichiers Emule. C'est la première fois que l'AEPD inflige une amende pour cause d'utilisation de systèmes qui permettent le partage et le téléchargement de fichiers de textes, de vidéos, de musique ou autres qui sont enregistrés dans l'ordinateur d'autres utilisateurs. L'AEPD exige que des mesures de sécurité soient prises, comme l'installation de pare-feu, et que le dossier contenant les informations à partager soit sélectionné avec circonspection.
- **YouTube :** l'AEPD a ouvert de son propre chef une enquête sur l'enregistrement d'images d'une personne handicapée et leur diffusion via le site YouTube, au titre du droit du représentant de cette personne à la suppression de ces données, afin de déterminer si ces faits constituaient une infraction grave à la LOPD, en l'occurrence le traitement d'images en rapport avec l'état de santé d'une personne et leur diffusion.
- **Forums Internet :** l'AEPD a estimé que le droit de suppression s'appliquait aussi aux données personnelles publiées sur un forum Internet, si celles-ci ne concernent pas une célébrité et ne portent pas sur un fait susceptible d'être intéressant. La divulgation de données personnelles sur l'Internet ne tombe pas nécessairement sous le coup de la protection du droit à la liberté d'expression.

C. Questions diverses importantes

1. Transparence

Devant le Parlement

Le directeur de l'AEPD s'adresse à la chambre basse du Parlement espagnol

Dans son discours annuel, le directeur de l'AEPD a épinglé la prolifération récente de dispositifs de vidéosurveillance, non seulement sur l'initiative des pouvoirs

publics, mais aussi à l'instigation du secteur privé, en l'occurrence l'installation généralisée de caméras de surveillance à la demande de copropriétaires ainsi que dans les magasins et les réseaux de transport. Il a également évoqué des services tels que ceux proposés sur le site YouTube, qui permettent la diffusion mondiale d'images auprès de tous les internautes. Dans son discours, il a par ailleurs insisté sur la nécessité d'offrir des garanties quant aux nouveaux risques issus de services Internet, notamment les moteurs de recherche et les messageries électroniques, et a rappelé que les moteurs de recherche devaient garantir l'exercice du droit d'accès, de rectification, de suppression et de contestation.

2. Coopération avec les agences de protection des données des Communautés autonomes

L'expérience acquise et la renégociation de certains statuts des gouvernements autonomes ont suscité un débat sur l'opportunité de créer un nouveau modèle de coopération entre les APD existantes. À cette fin, cinq groupes de travail ont été constitués (« Enregistrement », « Inspection », « Analyse juridique », « Organisation, communication et modernisation » et « International »). Les mesures qui ont été évoquées visent à renforcer les bases de la garantie de l'égalité de tous les citoyens quant au droit fondamental à la protection des données à caractère personnel. Elles simplifient les obligations des gestionnaires de fichiers et améliorent l'efficacité des agences.

3. Recommandations au gouvernement

Durant l'année 2007, l'AEPD a formulé un certain nombre de recommandations, en particulier à l'intention des pouvoirs publics. Plusieurs de ces recommandations préconisent d'améliorer la réglementation pour :

- appliquer des procédures qui permettent la protection de la propriété intellectuelle d'une manière compatible avec le droit fondamental à la protection des données ;
- réglementer la publication anonyme de jugements par les instances judiciaires ;
- réglementer les systèmes internes de signalement à la disposition des travailleurs dans leur entreprise, c'est-à-dire identifier les activités qui pourraient nécessiter la mise en place de tels systèmes, garantir le droit à la confidentialité des auteurs des signalements et les droits des parties qui font l'objet de signalements.

De plus, l'AEPD a formulé une série de recommandations pratiques qui insistent sur la nécessité, pour les services publics concernés, de prendre les mesures suivantes :

- élaborer un plan d'action prévoyant des mesures spécifiques pour la protection des mineurs d'âge et de leurs données sur l'Internet ;
- renforcer les mesures de précaution pour empêcher l'échange non consenti de données personnelles sur l'Internet au travers des réseaux de partage de fichiers en P2P ;
- inciter les médias à l'autorégulation pour garantir le respect de la vie privée et la protection des données à caractère personnel et à les encourager à adopter des pratiques plus respectueuses de la réglementation sur la protection des données ;
- mettre en œuvre des initiatives visant à promouvoir le recours à des garanties de confidentialité pour les destinataires de courriers électroniques ;
- élaborer un plan d'action en faveur de l'amélioration des bonnes pratiques pour garantir le respect de la vie privée dans le Journal officiel au travers de l'adoption de mesures qui permettent de limiter les informations personnelles obtenues à l'aide de moteurs de recherche sur l'Internet, sans que l'objet du Journal officiel n'en pâtisse ;
- adopter une stratégie locale visant à adapter l'installation de caméras de surveillance du trafic en fonction de la réglementation sur la protection des données à caractère personnel.

4. Plus d'informations, plus de sensibilisation, plus de questions

L'information est essentielle pour sensibiliser les citoyens à la protection des données à caractère personnel. Dans ce contexte, l'AEPD a intensifié sa coopération avec les médias et a affecté davantage de moyens humains et matériels à la communication dans le but de répondre à la demande croissante d'informations et de multiplier ses campagnes d'information. L'amélioration de la sensibilisation des citoyens s'est traduite par une augmentation de 30 % des demandes adressées au Service d'information des citoyens l'année dernière (47 741 demandes au total).

5. Mise en application

L'amélioration de la sensibilisation à la réglementation sur la protection des données a donné lieu à l'augmentation

du nombre de plaintes pour cause d'infraction présumée à la législation. Le législateur a conféré à l'AEPD des pouvoirs qui lui permettent d'agir en toute indépendance, d'ouvrir des enquêtes sur des infractions présumées et d'infliger des amendes le cas échéant dans le but de garantir l'application de la réglementation en vigueur. La majorité des enquêtes concernent le secteur des télécommunications et les institutions financières. Les faits en rapport avec la vidéosurveillance viennent en troisième place, après une augmentation de plus de 400 %.

5.1 Renforcement des mesures préventives

a. Plan d'action en faveur de la protection des données des mineurs d'âge sur l'Internet

Le règlement de développement de la loi organique sur la protection des données définit les principes fondamentaux du traitement des données personnelles des mineurs d'âge. Toutefois, l'adoption d'un cadre réglementaire ne suffit pas. L'installation de logiciels de contrôle de contenus, l'aide aux parents et aux opérateurs et le renforcement de la sécurité sur l'Internet passent par une action résolue des pouvoirs publics, qui s'articule autour de différentes initiatives en faveur de la protection des mineurs d'âge.

b. Rapport sur les moteurs de recherche

En 2007, l'Agence espagnole de protection des données a publié un rapport reprenant ses principales observations concernant l'adaptation des pratiques des moteurs de recherche en matière de collecte, d'enregistrement et d'utilisation de données personnelles à la réglementation nationale sur la protection des données. Ce rapport, disponible en ligne sur le site de l'AEPD, inclut les principales conclusions de l'analyse des implications que ces pratiques peuvent avoir pour le respect de la vie privée des utilisateurs des moteurs de recherche et des autres services proposés par ces opérateurs.

Conclusions :

- les moteurs de recherche doivent limiter la durée de stockage des données afin de réduire à un minimum les risques de manquement au respect de la vie privée des utilisateurs ;
- les informations fournies aux utilisateurs sont complexes et ne leur sont guère utiles ;
- les citoyens ont le droit de supprimer et de contester les données les concernant qui sont générées par une recherche.

Ce rapport est accessible via ce lien :
https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/declaracion_aepd_buscadores_en.pdf

c. Inspection sectorielle en Colombie

L'AEPD a réalisé une inspection dans des entreprises qui procèdent à des transferts internationaux de données personnelles dans le cadre de la fourniture de services à des centres de télémarketing ou de service à la clientèle. Parmi ses préoccupations majeures, l'accroissement des demandes d'autorisation qu'elle a reçues ces dernières années concernant les transferts internationaux de données, les pays de destination et les finalités de ces demandes.

Le rapport et ses conclusions sont accessibles via ce lien:
https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/report_Inter_data_transfers_colombia_en.pdf

6. Activités de l'Espagne dans le cadre du Réseau ibéro-américain de protection des données

L'année 2007 a été particulièrement riche pour le Réseau ibéro-américain de protection des données, créé en 2003 à l'initiative de l'AEPD dans le but de promouvoir la réglementation de la protection des données dans les pays membres. La cinquième réunion ibéro-américaine s'est tenue en 2007 à Lisbonne, au Portugal. Un séminaire a également été organisé en 2007 à Carthagène des Indes, en Colombie, dans le but de créer un forum de débat et d'échange d'informations. Des orientations ont été définies pour promouvoir des initiatives à mettre en œuvre dans le but de parvenir à un niveau adéquat de protection des données dans les pays ibéro-américains et, par là, de lever les obstacles entravant la libre circulation des données personnelles entre ces pays. Dans le cadre de son engagement dans ce réseau, l'AEPD a accueilli en ses locaux des représentants du Chili, du Mexique et d'Uruguay. Les représentants uruguayens se sont vu prodiguer des conseils au sujet de leur loi sur la protection des données.

Suède

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La directive 95/46/CE a été transposée en droit national par le biais de l'adoption de la loi (1998:204) sur les données à caractère personnel (PDA, *Personal Data Act*), entrée en vigueur en octobre 1998. La PDA est complétée par l'ordonnance (1998:1191) relative aux données à caractère personnel, entrée en vigueur le même jour. Comme la directive, cette loi s'applique au traitement automatisé et au traitement manuel des données. Même si la PDA s'applique en principe au traitement des données à caractère personnel dans tous les secteurs de la société, plusieurs lois et ordonnances traitent du traitement des données dans certains secteurs d'activité, soit en lieu et place de la PDA, soit en complément de celle-ci. La directive européenne a été prise en compte également lors de l'élaboration de ces lois et ordonnances spécifiques.

Des éditions précédentes du Rapport du Groupe de travail « Article 29 » décrivent le « modèle d'utilisation abusive » instauré par l'entrée en vigueur d'un amendement de la PDA le 1er janvier 2007. Cet amendement vise – dans le cadre de la directive – à simplifier la réglementation applicable au traitement courant des données à caractère personnel. Il concerne les formes de traitement qui ne peuvent en principe accroître les risques d'infraction au respect de la vie privée. Il peut être dérogé à la réglementation sur le traitement de données « sensibles » (notification, information et protection) et à l'obligation d'obtenir un consentement le cas échéant si les données visées ne sont et ne seront pas incluses dans un ensemble de données personnelles fortement structuré dans le but de faciliter la recherche ou la compilation de données. Le contrôleur de données n'est donc plus dans l'obligation de respecter la réglementation sur le traitement des données si le traitement n'est pas structuré et porte par exemple sur un courrier électronique ou sur du texte continu dans un site Internet. Dans ces cas s'applique le « modèle d'utilisation abusive », qui prévoit que le traitement n'est autorisé que s'il ne manque pas au respect de la vie privée. Une infraction à ce modèle entraîne l'application de la réglementation sur la responsabilité civile et est passible d'amendes dans certains cas.

Des problèmes d'interprétation se posent à propos de ce qu'il convient de considérer comme du traitement structuré et du traitement non structuré. Mais nous pensons que cet amendement est une adaptation à la réalité.

La directive 2002/58/CE a été transposée en droit national par la loi (2003:389) relative aux communications électroniques (ECA, *Electronic Communications Act*), entrée en vigueur en juillet 2003. Le chapitre 6 de l'ECA définit les règles applicables à la protection des données dans le domaine des communications électroniques. C'est à l'Agence nationale des postes et télécommunications qu'il incombe de veiller au respect des dispositions de l'ECA concernant la protection des données. L'article 13 de la directive européenne sur les courriers électroniques non sollicités est transposé en droit national par des amendements à la loi (1995:450) relative aux pratiques de marketing.

Ces amendements sont entrés en vigueur le 1er avril 2004. L'Agence de protection des consommateurs est chargée de veiller au respect de la loi relative aux pratiques de marketing. Le gouvernement a décidé en avril 2004 de créer une commission pour la protection de la vie privée (*Integritetsskyddskommittén*). Ses membres, des experts et des élus du Riksdag (le Parlement suédois) ont été chargés de réaliser une étude et d'analyser la législation suédoise concernant le respect de la vie privée. Il leur a également été demandé par la suite de déterminer s'il y avait lieu de prévoir des textes généraux pour protéger la vie privée en plus de la législation existante. Au printemps 2007, la commission a présenté un rapport détaillé rendant compte de ses travaux d'étude et d'analyse, qui constituaient la première partie de sa mission. Les membres y décrivent de manière relativement détaillée l'évolution de la législation dans différents secteurs de la société, la nature des informations sur lesquels le gouvernement et le Parlement ont dû se baser pour prendre leurs décisions et le compromis trouvé pour concilier la protection de la vie privée et d'autres intérêts. Le principe de la proportionnalité a fait l'objet d'une analyse particulière.

Les membres de la commission critiquent à plusieurs égards l'adoption d'une approche systématique et méthodique et expliquent en quoi ces imperfections se traduisent par un niveau de protection inférieur au niveau requis.

Ils répondent d'emblée par la négative à la question de savoir si la réglementation de la protection de la vie privée peut être considérée comme satisfaisante. Ils ont présenté la deuxième et dernière partie de leur rapport en janvier 2008. Ils y livrent une analyse de la façon dont la protection de la vie privée doit être réglementée par la constitution, et ils identifient d'autres mesures à prendre.

En mai 2006, le ministère de la justice a confié à une commission d'enquête la mission de passer en revue la législation nationale en vigueur pour proposer les amendements requis par l'adoption de la directive européenne concernant la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ; cette commission d'enquête a présenté son rapport en novembre 2007.

Le Conseil de l'inspection des données est représenté au sein de la commission, et des prestataires de services ont été consultés. Le ministère de la justice a soumis le rapport pour étude. Le Conseil de l'inspection des données étudie actuellement les propositions qui y sont faites. Le gouvernement soumettra un projet de loi au Parlement d'ici la fin de l'année. Il est peu probable que la directive soit transposée et mise en œuvre avant 2009.

Les propositions d'amendement de la réglementation sur les soins de santé et sur les dossiers des patients sont décrites dans l'édition précédente du rapport annuel. La commission d'enquête a proposé l'adoption d'une toute nouvelle loi, en l'occurrence la loi sur les données des patients, qui prévoit la réglementation unifiée des données personnelles dans les services de santé et de soins médicaux. Un représentant du Conseil de l'inspection des données a participé aux travaux d'élaboration de cette nouvelle proposition de loi. Cette proposition a été soumise pour consultation et est actuellement à l'étude au gouvernement.

En principe, cette nouvelle loi devrait entrer en vigueur le 1er juillet 2008. La commission d'enquête a présenté son dernier rapport, en l'occurrence sur les produits pharmaceutiques et sur les données des patients, durant l'été 2007.

En novembre 2007, le ministère de la justice a présenté un rapport proposant d'adopter une nouvelle loi sur le traitement des données personnelles par la police dans le cadre de la lutte contre la criminalité. Cette nouvelle loi devrait remplacer la loi de 1992 sur les données de la police. Elle règlemente à de rares exceptions près toutes les formes de traitement de données auxquelles se livre la police dans le cadre de la lutte contre la criminalité. Elle s'appliquera au Conseil national de la police, aux autorités de la police et au Bureau suédois de lutte contre la criminalité économique. Le traitement des données au sein du service national de sécurité intérieure fera l'objet d'une réglementation spécifique. La nouvelle loi offre des possibilités pour améliorer la coopération entre les services chargés de la lutte contre la criminalité, car elle instaure de nouvelles dispositions en matière de divulgation des données. Le rapport a été soumis pour consultation, et les propositions sont actuellement à l'étude au Conseil de l'inspection des données. En principe, ces propositions devraient entrer en vigueur le 1er janvier 2009.

B. Jurisprudence

La neuvième édition du rapport annuel a évoqué une affaire de données biométriques en milieu scolaire et la décision du Conseil 2004 de l'inspection des données concernant la collecte et le traitement des empreintes digitales des élèves en guise de contrôle d'accès à la cantine scolaire. Cette décision stipule qu'indépendamment de l'obtention du consentement des personnes visées, ce mode de contrôle n'est ni adéquat, ni pertinent et qu'il pourrait être réalisé d'une manière plus respectueuse de la vie privée. Cet argument a été retenu dans des affaires similaires. Les décisions du Conseil de l'inspection des données ont fait l'objet d'un pourvoi en appel auprès du Tribunal administratif du Comté, qui les a confirmées. Ces décisions ont ensuite été portées en appel devant la Cour administrative d'appel de Stockholm, qui a déclaré que ce mode de collecte et de traitement des données était conforme aux principes qualitatifs de la protection des données et était légitime sans consentement.

Le Conseil de l'inspection des données a interjeté appel devant la Cour administrative suprême. Trois affaires de ce type sont pendantes devant cette instance.

En juin 2007, la Cour administrative d'appel de Stockholm a rendu son jugement dans l'affaire du Bureau national de lutte contre le piratage, déjà évoquée dans de précédentes éditions du rapport annuel. L'enjeu de cette affaire est de déterminer

si les numéros IP (Internet Protocol) sont à considérer ou non comme des données à caractère personnel. Le Bureau de lutte contre le piratage, une association coopérative économique, a collecté des fragments d'information, en particulier des numéros IP, dans le cadre du partage sur l'Internet de matériel protégé par des droits d'auteur. Le Conseil de l'inspection des données a estimé dans sa décision que les numéros IP étaient à considérer comme des données à caractère personnel et que le traitement auquel le Bureau de lutte contre le piratage avait soumis ces données tombait sous le coup de la loi relative aux données à caractère personnel (PDA), car il concernait des infractions au sens du chapitre 21 de cette loi.

Seuls les pouvoirs publics sont autorisés à traiter des données à caractère personnel concernant des infractions criminelles à moins d'une exemption accordée par le Conseil de l'inspection des données. Dans sa décision de juin 2005, le Conseil a ordonné au Bureau de lutte contre le piratage de mettre un terme à cette forme de traitement. Le Bureau de lutte contre le piratage a avancé l'argument que les numéros IP ne pouvaient être considérés comme des données à caractère personnel, dans la mesure où il n'avait pas accès aux données identifiant les abonnés qui utilisent telle ou telle adresse IP. Il s'est pourvu en appel de la décision. Le tribunal administratif du Comté et la Cour administrative d'appel ont confirmé la décision du Conseil de l'inspection des données.

Après la décision rendue par le Conseil de l'inspection des données en 2005, le Bureau de lutte contre le piratage a demandé l'autorisation de se soustraire à l'application du chapitre 21 de la PDA dans le cadre du traitement des numéros IP pour pouvoir signaler les infractions des abonnés aux droits de propriété intellectuelle à la police et aux prestataires de services sur l'Internet. Le Conseil de l'inspection des données a accordé son autorisation une première, puis une seconde fois. Le Bureau de lutte contre le piratage est autorisé à traiter des données personnelles relatives à des infractions jusqu'à la fin de l'année 2008.

C. Questions diverses importantes

Documents imprimés

Tous les documents imprimés du Conseil de l'inspection des données peuvent être téléchargés gratuitement sur son site web. *Magazin DIrekt* est un périodique proposant des reportages, des actualités et des commentaires en rapport avec les centres d'intérêt du Conseil de l'inspection des données. Quatre numéros ont été publiés en 2007. Le nombre d'abonnés à la version papier a sensiblement augmenté durant l'année 2007.

Le Conseil de l'inspection des données a été chargé par le gouvernement de contribuer à la mise en place de services publics en ligne sûrs et efficaces. Dans le cadre de cette mission, nous avons rédigé à l'intention des municipalités un manuel d'orientation sur les services publics en ligne et les données à caractère personnel. Ce manuel a été distribué dans toutes les municipalités du pays. Conformément aux orientations, nous allons continuer à observer les phénomènes nouveaux. Dans le cadre de ce travail, nous avons publié des rapports sur « L'omniprésence de l'informatique : une vision qui risque de devenir réalité », sur « Le système de traitement informatique des visas : la plus grande base de données biométriques du monde » et sur « Le traité de Prüm, qui donne aux forces de police de l'UE le droit de consulter les fichiers de prélèvements ADN, d'empreintes digitales et d'immatriculation des véhicules de leurs homologues ».Nous avons chargé un centre de recherche d'étudier l'attitude des jeunes à l'égard de l'Internet et de rendre compte de ses travaux dans un rapport intitulé « Les jeunes et le respect de la vie privée ». Nous avons également publié un portrait de notre autorité, en suédois et en anglais, intitulé *What on Earth does the Data Inspection Board do?* (Rôle du Conseil de l'inspection des données). Dans cette publication, nous présentons nos activités en donnant la parole à dix membres du personnel, qui expliquent en quoi consiste leur travail et parlent d'eux-mêmes. Enfin, nous avons publié une liste de contrôle sur les clés électroniques dans les sociétés de logement et les copropriétés.

Concernant l'autorégulation, le Conseil de l'inspection des données a rendu son avis sur un nouveau système, l'ID06, dans le secteur de la construction. Ce système a deux objectifs : rendre le travail clandestin plus difficile et contrôler – pour des raisons de sécurité – les présences sur les lieux de travail. Le Conseil de l'inspection des données a estimé que le système était conforme à la loi sur les données à caractère personnel, mais a insisté sur la nécessité d'informer clairement les personnes concernées. Les données à caractère personnel qui sont collectées peuvent être conservées pendant maximum deux ans, car les services fiscaux peuvent en avoir besoin pour des contrôles.

Royaume-Uni

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

La directive 95/46/CE a été transposée en droit national par la loi de 1998 sur la protection des données qui est entrée en vigueur le 1er mars 2000.

La directive 2002/58/CE a été transposée en droit national par la réglementation concernant la vie privée et les communications électroniques qui est entrée en vigueur le 11 décembre 2003.

La période de transition est arrivée à son terme le 23 octobre 2007, ce qui implique que les fichiers manuels constitués avant 1998 sont désormais soumis à la loi.

B. Jurisprudence

La Cour d'appel a rejeté le pourvoi en appel de David Paul Johnson dans l'affaire Johnson c. The Medical Defence Union (décision civile n° 262 de la Cour d'appel d'Angleterre et du Pays de Galles, 2007). Selon deux des trois juges appelés à statuer, la loi sur la protection des données ne s'étend pas à la sélection d'informations personnelles par un être humain, même si ces informations sont par la suite enregistrées dans un système automatisé. Il reste à déterminer si leur interprétation fera jurisprudence.

C. Questions diverses importantes

En novembre, l'administration fiscale et douanière (Her Majesty's Revenue and Customs, HMRC) a admis avoir perdu deux disques informatiques contenant l'ensemble des dossiers d'allocations familiales, soit les données personnelles de 25 millions de personnes. Cet incident a mis en lumière l'importance de la protection des données et les limites du pouvoir du Commissaire à empêcher ou sanctionner ces infractions. En décembre, le Commissaire a appelé le gouvernement à lui conférer davantage de pouvoirs pour lui permettre d'auditer les contrôleurs de données sans leur consentement et de leur infliger des sanctions en cas d'infractions délibérées et répétées aux principes de protection des données. Il a par ailleurs proposé d'instaurer la progressivité des droits de notification, ce qui aurait pour effet d'accroître sensiblement les moyens à la disposition du Commissaire. Le gouvernement devrait procéder à des consultations sur ces propositions de modification en 2008.

En 2007, les services du Commissaire à l'information (Information Commissioner's Office – ICO) ont procédé à une consultation à propos de la stratégie de protection des données. Cette stratégie prévoit notamment de concentrer les moyens de l'ICO sur les cas où il existe un risque réel de préjudice individuel. Le Commissaire entend rendre la tâche plus facile à la grande majorité des contrôleurs de données honnêtes tout en mobilisant ses pouvoirs contraignants envers la minorité de contrôleurs qui menacent réellement les droits des individus. Cette stratégie sera lancée en mars 2008.

En octobre, le Premier ministre Gordon Brown a confié à Richard Thomas, Commissaire à l'information, et au Dr Mark Walport, directeur du Wellcome Trust, la mission de réaliser une étude indépendante sur le partage d'informations et de formuler dans leur rapport des recommandations de modification de la loi et de réorientation de l'action publique dans ce domaine.

En janvier 2007, le Commissaire a marqué la première édition de la Journée européenne de la protection des données en attirant l'attention sur le risque d'usurpation d'identité. L'ICO a rendu publics les résultats d'une enquête qui montre que la majorité des Britanniques ont déjà été victimes d'une usurpation d'identité ou qu'ils s'y exposent. Il a réalisé un petit film d'information (« The man in the mirror ») pour sensibiliser l'opinion à ce risque et a publié un petit guide pour aider les citoyens à protéger leurs données personnelles (*Personal Information Toolkit*).

En mars, l'ICO a découvert que onze banques et institutions financières enfreignaient la loi sur la protection des données à caractère personnel, lorsque les médias ont fait état de la mise au rebut de données bancaires confidentielles dans des sacs en plastique et des poubelles ordinaires. Les directeurs des établissements concernés ont pris par écrit l'engagement d'améliorer leurs procédures de sécurité.

En août, l'ICO a publié un dossier sur la définition de la notion de « données personnelles », compte tenu de l'avis du Groupe de travail « Article 29 ».

En octobre, l'ICO a publié le code de déontologie en matière d'échange d'informations. Ce code aidera les organisations à élaborer leurs propres protocoles d'échange de données à caractère personnels. L'ICO a également entamé un processus de consultation à propos de la version révisée du code de déontologie concernant les systèmes de télévision en circuit fermé qui a été publiée en janvier 2008.

En novembre 2007, le Commissaire a enjoint les forces de police de supprimer les anciennes condamnations mineures du fichier national de la police. Le Tribunal des informations étudiera ce dossier en avril 2008.

Le 11 décembre, le Commissaire a accueilli la conférence « Surveillance Society : turning debate into action » (Société de la surveillance : traduire les débats en action), à Bridgewater Hall, à Manchester. Le manuel d'évaluation de l'impact sur la vie privée rédigé par l'ICO et les recherches y afférentes ont été rendus publics lors de cet événement. Ce manuel d'évaluation d'impact sur la vie privée est le premier qui ait été élaboré par une autorité européenne de protection des données. L'ICO remercie ceux qui contribué au projet, notamment la DPA finlandaise.

En 2007, le Commissaire s'est exprimé devant sept commissions parlementaires spéciales au sujet de dix affaires (soit une augmentation sensible par rapport à 2006).

- Commission sur l'Union européenne de la Chambre des Lords, sous-commission F (affaires intérieures), dans les enquêtes sur le système d'information Schengen de deuxième génération, sur les dossiers passagers et sur le traité de Prüm.
- Commission sur la Constitution de la Chambre des Lords, dans l'enquête sur l'impact de la surveillance et de la collecte des données sur la vie privée des citoyens et leur relation avec l'État.
- Commission de la santé de la Chambre des Communes, dans l'enquête sur le dossier médical électronique.
- Commission des affaires intérieures de la Chambre des Communes, dans l'enquête sur la société de surveillance et les dossiers concernant la justice et les affaires intérieures soumis à l'échelle de l'Union européenne.
- Commission de la culture, des médias et des sports de la Chambre des Communes, à propos du rôle du régulateur de la presse britannique (Press Complaints Commission).
- Commission en charge de la loi sur la justice pénale et l'immigration, chapitre 55 de la DPA (les actes illicites d'accès aux données ou de traitement ou de vente de données).
- Commission de la justice, à propos de la protection des données à caractère personnel.

En 2007, le Commissaire a répondu à 47 consultations (soit une augmentation très sensible par rapport à 2006).

Chapitre 3
Union européenne et activités communautaires

3.1. COMMISSION EUROPÉENNE

Communication de la Commission au Parlement européen et au Conseil – Suivi du Programme de travail pour une meilleure mise en application de la directive sur la protection des données, Bruxelles, le 7.3.2007[21]

Le premier rapport de la Commission sur la mise en œuvre de cette directive[22] conclut qu'il n'est pas nécessaire d'amender la législation, mais qu'il reste du chemin à parcourir et que la mise en œuvre de la directive peut être sensiblement améliorée. Ce rapport inclut un *programme de travail pour une meilleure mise en application de la directive sur la protection des données*.

La communication adoptée le 7 mars 2007 examine le travail réalisé dans le cadre de ce programme, évalue la situation actuelle et esquisse les perspectives futures en tant que préalable au succès dans une série de domaines d'action, à la lumière de l'article 8 de la Charte européenne des droits fondamentaux, qui reconnaît un droit autonome à la protection des données à caractère personnel.

Les principales conclusions de cette communication sont les suivantes : la Commission n'envisage pas dans l'immédiat de soumettre une proposition législative visant à modifier la directive et invite instamment les États membres à veiller à la bonne mise en œuvre de la législation nationale adoptée en application de la directive. Les activités énumérées dans le programme de travail seront poursuivies, et l'association de tous les acteurs constitue une bonne base pour améliorer la mise en œuvre des principes de la directive. Afin de tirer pleinement parti de cette mission, les autorités de contrôle doivent également s'efforcer d'adapter leurs pratiques nationales afin de les aligner sur la ligne commune arrêtée au sein du Groupe de travail.

Communication de la Commission au Parlement européen et au Conseil – Promouvoir la protection des données par les technologies renforçant la protection de la vie privée, Bruxelles, le 2.5.2007[23]

Cette communication sur la promotion de la protection des données par les technologies renforçant la protection de la vie privée vise à identifier les avantages de ces technologies, à définir les objectifs de la Commission dans le but de promouvoir ces technologies et à décrire clairement les mesures qu'il convient de prendre à l'appui du développement de ces technologies et de leur utilisation par les contrôleurs de données et les consommateurs.

La Commission estime qu'il convient de développer les technologies renforçant la protection de la vie privée et de les utiliser plus largement, notamment dans le cadre du traitement de données à caractère personnel par l'intermédiaire de réseaux de TIC. Elle considère qu'un usage plus large de ces technologies améliorerait la protection de la vie privée et aiderait à observer les règles relatives à la protection des données. L'usage de ces technologies serait complémentaire au cadre juridique et aux mécanismes de contrôle existants.

Proposition de ***directive du 13 novembre 2007***[24] ***modifiant la directive 2002/22/CE du Parlement européen et du Conseil*** *concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération en matière de protection des consommateurs*.

Le 13 novembre 2007, la Commission a adopté une proposition de directive modifiant, entre autres, la 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.

[21] Communication de la Commission au Parlement européen et au Conseil – Suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, Bruxelles (JO C 138 du 22.6.2007, p. 17 ; URL : http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_fr.htm#follow_up).

[22] Rapport de la Commission – Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE), COM(2003) 265 final, 15.5.2003 (JO C 76 du 25.3.2004, p. 18).

[23] Communication de la Commission au Parlement européen et au Conseil – Promouvoir la protection des données par les technologies renforçant la protection de la vie privée (JO C 181 du 3.8.2007, p. 22 ; URL : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0228:FR:NOT)

[24] COM(2007) 698 final, JO C 55 du 28.2.2008, p. 4 (URL :

L'objectif premier de cette proposition est d'améliorer la protection des données à caractère personnel et de la vie privée des individus dans le secteur des communications électroniques, notamment en renforçant les dispositions liées à la sécurité et les mécanismes coercitifs.

Première édition de la Journée européenne de la protection des données, le 28 janvier 2007[25]

La Commission salue et soutient l'initiative du Conseil de l'Europe qui a fait du 28 janvier, date de la signature de la Convention 108 concernant le traitement des données à caractère personnel, la « Journée européenne de la protection des données ».

Des événements ont été organisés dans les États membres pour sensibiliser les citoyens à leurs droits en matière de protection des données à caractère personnel.

Conférence sur le thème de la sécurité publique, de la vie privée et de la technologie, Bruxelles, le 20 novembre 2007[26]

Le 20 novembre 2007, la Commission européenne a organisé une conférence sur le thème de la sécurité publique, de la vie privée et de la technologie. La technologie permet le transfert des données, améliore le contrôle d'accès aux données et facilite la recherche de données pertinentes, tout en conciliant les impératifs en matière de sécurité et la nécessité de protéger la vie privée. Cette conférence a réuni des représentants du secteur public et du secteur privé.

Elle a permis de débattre d'activités relevant de domaines différents, notamment le développement de nouvelles technologies, en particulier celles qui renforcent la protection de la vie privée, d'ouvrir un dialogue entre le secteur public et le secteur privé à propos de la recherche et du développement en matière de sécurité et d'étudier la contribution des nouvelles technologies à l'amélioration de la sécurité.

Protection des données à caractère personnel en vertu du traité de Lisbonne

Une version adaptée de la Charte des droits fondamentaux de l'Union européenne a été promulguée à **Strasbourg le 12 décembre 2007**[27]. Les chefs d'État et de gouvernement des 27 États membres ont signé le traité de Lisbonne[28] le 13 décembre 2007, à Lisbonne. Ces deux conventions contiennent des dispositions importantes pour la protection des données à caractère personnel.

L'article 8 de la Charte des droits fondamentaux dispose que toute personne a droit à la protection des données à caractère personnel la concernant.

L'article 16 (nouveau) du traité sur le fonctionnement de l'Union européenne jette les bases légales de l'adoption de textes législatifs relatifs à la protection des individus et à la libre circulation des données à caractère personnel, en l'occurrence l'application de la procédure législative ordinaire (procédure de codécision). Ces dispositions s'appliquent au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union ; elles s'appliquent aussi à la libre circulation de ces données. Cette nouvelle formulation vise en particulier la coopération policière et judiciaire en matière criminelle à l'échelle nationale et européenne, car la nature spécifique de ces activités peut nécessiter l'adoption de règles spécifiques[29].

L'article 39 (nouveau) du traité de l'Union européenne jette les bases légales spécifiques de la protection des données à caractère personnel dans le cadre de la politique étrangère et de sécurité commune (PESC) et des règles relatives à la libre circulation de ces données.

[25] Déclaration du vice-président Frattini, au nom de la Commission européenne, à l'occasion de la Journée de la protection des données (28 janvier) (URL : http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/102&format=HTML&aged=1&language=FR&guiLanguage=en). Résolution du Groupe de travail « Article 29 » à l'occasion de la première édition de la Journée européenne de la protection des données (URL : http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm).

[26] Pour plus d'informations concernant la conférence sur la sécurité publique, la vie privée et la technologie, voir la page web à l'adresse : http://ec.europa.eu/justice_home/news/events/events_2007_en.htm).

[27] JO C 303 du 14.12.2007, p. 1.

[28] JO C 306 du 17.12.2007, p. 1.

[29] Déclarations 20 et 21.

Cela s'applique au traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 2 « Dispositions spécifiques concernant la politique étrangère et de sécurité commune ». Ces dispositions traduisent la volonté des États membres de laisser sous contrôle intergouvernemental les grands enjeux de la diplomatie et de la défense et constituent une exception à la base juridique unique, en vertu du principe de primauté du droit communautaire[30].

Accord PNR 2007[31]

Un accord a été signé à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007 entre l'Union européenne et les États-Unis d'Amérique à propos du traitement et du transfert de données des dossiers passagers (données PNR, Passenger Name Record) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS, *Department of Homeland Security*). Cet accord ne vise pas à amender le droit des États-Unis, de l'Union européenne ou de ses États membres, ni à y déroger, mais à prévenir et à combattre efficacement la criminalité transnationale et le terrorisme pour protéger les sociétés démocratiques et les valeurs communes des parties.

*Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record – *PNR) à des fins répressives [COM(2007) 654 final]*[32]

La proposition de la Commission concernant la décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record – PNR) à des fins répressives qui a été adoptée le 6 novembre 2007 autorise les compagnies aériennes à mettre à la disposition des autorités compétentes des États membres les données PNR des passagers des vols internationaux dans le but de prévenir et de combattre le terrorisme et la criminalité organisée. Elle règlemente également le traitement et la conservation de ces données par ces autorités et l'échange de ces données entre elles.

SWIFT

Le département du Trésor des États-Unis a élaboré le programme de surveillance du financement du terrorisme (Terrorist Finance Tracking Program – TFTP) après les attaques terroristes du 11 septembre 2001 pour identifier, suivre et arrêter ceux qui apportent un soutien financier aux activités terroristes. Dans le cadre de ce programme, le département du Trésor a adressé des injonctions administratives à la Société de télécommunications interbancaires mondiales (Society for Worldwide Interbank Financial Telecommunication – SWIFT). Ces injonctions imposent au centre d'exploitation de la SWIFT aux États-Unis de transférer au département du Trésor une partie limitée des données financières personnelles enregistrées sur son serveur aux États-Unis ; le département du Trésor pourra les utiliser pour empêcher des entités ou des individus suspects de commettre des actes terroristes.

Lorsque ces faits ont été rendus publics en 2006, l'Autorité belge de protection des données a émis un avis estimant que les activités de traitement menées par la SWIFT concernant l'exécution de paiements interbancaires enfreignaient la loi belge sur la protection des données, qui transpose en droit national la directive 95/46/CE sur la protection des données à caractère personnel. Le Groupe de travail « Article 29 » a lui aussi considéré, dans un avis rendu en novembre 2006[33], que la SWIFT et les institutions financières recourant à ses services avaient enfreint les règles communautaires sur la protection des données arrêtées dans la directive 95/46/CE, notamment en transférant des données à caractère personnel aux États-Unis sans prévoir de protection adéquate ni informer les personnes concernées de l'usage de leurs données personnelles. Durant l'année 2007, le Groupe

[30] Article 40 du TUE amendé par le traité de Lisbonne.

[31] Décision 2007/551/CFSP/JHA du Conseil du 23 juillet 2007 (JO L 204 du 4.8.2007, p. 16) relative à la signature d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (JO L 204 du 4.8.2007, p.18 ; URL : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:0017:FR:PDF).

[32] Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record – PNR) à des fins répressives [COM(2007) 654 final] (JO C 55/4 ; URL : http://europa.eu.int/eur-lex/lex/JOHtml.do?uri=OJ%3AC%3A2008%3A055%3ASOM%3AEN%3AHTML).

[33] Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT) (WP 128) (URL : http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_fr.htm).

de travail « Article 29 » a suivi l'évolution de ce dossier et les progrès accomplis par les différentes parties pour appliquer les recommandations formulées dans son avis du 22 novembre 2006. Il a rencontré à plusieurs reprises des représentants de la SWIFT et d'associations sectorielles pour faire le point sur les mesures et initiatives à prendre en vue de respecter les principes de protection des données.

En marge de l'action du Groupe de travail « Article 29 » et des autorités nationales de protection des données, la Commission et la présidence du Conseil se sont attelées à traiter le dossier d'infraction au droit communautaire sur la protection des données de la SWIFT et des institutions financières et à résoudre les différents problèmes y afférents.

La Commission a toujours soutenu que pour résoudre ces différents problèmes, il fallait avant tout que la SWIFT et les institutions financières respectent la directive sur la protection des données, en l'occurrence que la SWIFT prenne les mesures nécessaires pour se conformer à la loi belge sur la protection des données, c'est-à-dire informer l'APD belge de ses activités de traitement et prévenir les clients des banques et autres institutions financières que la façon dont les données SWIFT sont traitées implique leur transfert sur le serveur de la SWIFT aux États-Unis, où les autorités peuvent y accéder dans le cadre de la lutte contre le terrorisme. Il faut aussi que la SWIFT veille à ce que les transferts de données SWIFT sur son serveur miroir aux États-Unis à des fins commerciales soient effectués dans le respect de la directive sur la protection des données. C'est à cet effet que la SWIFT a adhéré au Safe Harbor américain en juin 2007.

Enfin, la Commission et la présidence du Conseil ont débattu avec des représentants du département du Trésor d'une série d'« observations » en vertu desquelles ce département s'engage unilatéralement à traiter les données à caractère personnel en provenance de l'UE dans le respect des principes communautaires de protection des données. Le Parlement (la commission LIBE) et le Conseil (le COREPER) ont été tenus informés de ces débats de même que le Groupe de travail « Article 29 ». Le 28 juin 2008, le département du Trésor a informé la présidence du Conseil et la Commission de ses observations concernant le traitement, l'utilisation et la communication de données obtenues en vertu du programme de surveillance du financement du terrorisme (Terrorist Financing Tracking Program – TFTP)[34].

3.2. COUR DE JUSTICE EUROPÉENNE

Arrêt du 8 novembre 2007 du Tribunal de première instance – The Bavarian Lager contre la Commission des Communautés européennes (Affaire T-194/04)[35]

La troisième chambre du Tribunal de première instance des Communautés européennes a annulé la décision de la Commission du 18 mars 2004 rejetant une demande introduite afin d'obtenir l'accès au procès-verbal d'une réunion. Le Tribunal de première instance estime, d'une part, que la Commission des Communautés européennes ne peut avancer les arguments de la protection de la vie privée et de l'intégrité de l'individu pour refuser une demande d'accès à des données personnelles contenues dans un document émanant de ses services que si cette divulgation est susceptible de porter concrètement et effectivement atteinte au respect de la vie privée et à l'intégrité de l'individu et, d'autre part, que le demandeur n'est pas dans l'obligation de prouver le caractère nécessaire de la divulgation. La Commission a interjeté appel.

3.3. CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Introduction

Conformément aux dispositions du règlement (CE) n° 45/2001[36], les principales activités du contrôleur

[34] JO C 166 du 20.7.2007, p. 17.

[35] JO C 315 du 22.12.2007, p. 33.

[36] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 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 L 8 du 12.1.2001, p. 1).

européen de la protection des données (CEPD) sont les suivantes :

- contrôler le traitement des données à caractère personnel par les administrations de l'UE, en veillant à ce qu'il ne soit pas porté atteinte aux droits et aux libertés des personnes dont les données sont traitées (supervision) ;
- émettre des avis sur les propositions de nouvelles législations européennes ayant une incidence sur la protection des données (consultation) ;
- coopérer avec d'autres autorités compétentes en matière de protection des données afin de garantir un niveau élevé et cohérent de protection des données dans toute l'Europe (coopération).

En 2007, des progrès importants ont été accomplis dans le domaine de la supervision. L'accent mis sur l'évaluation des résultats a encouragé la plupart des institutions et organes communautaires à prendre des mesures pour se conformer aux exigences en matière de protection des données. Les mesures prises sont assez satisfaisantes, mais il convient de poursuivre les efforts afin de se conformer pleinement à ces exigences.

Dans le domaine de la consultation, l'accent a été mis en particulier sur la nécessité de se doter d'un cadre cohérent et efficace pour la protection des données, tant dans le premier que dans le troisième pilier. Les résultats obtenus n'ont cependant pas toujours été satisfaisants. Les domaines d'action bénéficiant des activités consultatives du CEPD sont de plus en plus nombreux.

Le traité de Lisbonne est un repère important de l'histoire de l'UE, mais il devrait également être considéré comme un défi. Les garanties fondamentales qui y occupent une place privilégiée doivent être mises en œuvre dans la pratique. Ceci vaut lorsque les institutions et instances concernées traitent des données à caractère personnel, mais aussi lorsqu'elles élaborent des règles et des politiques susceptibles d'avoir une incidence sur les droits et sur les libertés des citoyens européens.

Supervision

Le travail de supervision, mené par le contrôleur adjoint, consiste à fournir des avis et à assister les délégués à la protection des données (DPD, *Data Protection Officers*) en soumettant les traitements à risque à des contrôles préalables, à mener des enquêtes, à traiter les réclamations, etc. Il consiste également à rédiger des documents de référence et d'information et à superviser l'unité centrale d'Eurodac.

En 2007, **le contrôle préalable** a continué d'être l'une des principales activités du CEPD dans le cadre de sa mission de supervision. L'échéance pour la réception des notifications en vue d'un contrôle préalable du CEPD – cas examinés *a posteriori* – a été fixée au printemps 2007 afin d'encourager les institutions et les organes communautaires à redoubler leurs efforts en vue de respecter pleinement leur obligation de notification.

Dans l'ensemble, le bilan relatif aux contrôles préalables réalisés par le CEPD en 2007 montre une augmentation importante du nombre de notifications adressées par beaucoup de délégués à la protection des données en raison de **l'échéance fixée au « printemps 2007 »**, notamment au cours du premier semestre de l'année. Toutefois, il reste encore beaucoup à faire pour le délai de réponse des institutions et des agences communautaires aux demandes d'informations complémentaires du CEPD.

En 2008, les efforts porteront donc essentiellement sur les points suivants :

- les institutions devraient finaliser leur processus de notification a posteriori, et les agences devraient réaliser un pas en avant important dans ce sens en 2008 ;
- il sera systématiquement donné suite aux recommandations du CEPD à travers les informations fournies par le responsable du traitement, et des inspections sur le terrain y seront associées.

En 2007, le CEPD a reçu 65 **réclamations**. Les cas déclarés recevables portaient notamment sur la collecte de données excessives concernant les visiteurs, l'accès aux données, le transfert et la copie de courriels, la demande d'informations de cartes de crédit, le traitement de données sensibles, le droit de rectification et l'obligation de fournir des informations.

Un certain nombre d'**enquêtes** ont été réalisées dans différents domaines au cours de l'année 2007. Deux de ces enquêtes ont requis une attention particulière de la part du CEPD, à savoir l'audit de sécurité de l'Office européen de lutte antifraude (OLAF) et le rôle de la Banque centrale européenne (BCE) dans l'affaire SWIFT[37].

Le CEPD a également continué à fournir des conseils sur les **mesures administratives** que les institutions et les organes communautaires envisagent de prendre en ce qui concerne le traitement des données à caractère personnel. Plusieurs questions importantes ont été soulevées, notamment la détermination de périodes de conservation pour certaines catégories de fichiers, les documents d'orientation sur l'internet, les procédures d'enquête pour fraude et corruption, l'échange d'informations, les dispositions d'application concernant la protection des données et l'applicabilité du droit national en matière de protection des données.

Le CEPD a continué de travailler à l'élaboration de **lignes directrices dans le domaine de la vidéosurveillance** afin de fournir aux institutions et organes communautaires des conseils pratiques sur le respect des règles en matière de protection des données lors de l'utilisation de systèmes de vidéosurveillance.

Au cours de l'année 2007, les travaux sur le contrôle commun d'**Eurodac** se sont poursuivis conjointement avec les autorités nationales compétentes en matière de protection des données. Après le lancement d'un audit de sécurité approfondi en septembre 2006, un rapport final sur cet audit a été présenté en novembre 2007. La principale conclusion en est que les mesures de sécurité initialement mises en œuvre en ce qui concerne Eurodac et leur maintien au cours des quatre premières années d'activité ont jusqu'à ce jour fourni un niveau correct de protection. Certaines parties de ces systèmes ainsi que la sécurité organisationnelle présentent néanmoins des faiblesses qu'il conviendra de corriger.

Consultation

En 2007, les activités du CEPD se sont exercées dans un contexte caractérisé par différents développements ayant pour point commun le fait qu'ils ont tous contribué à l'émergence d'une « **société de surveillance** ». Parmi ces faits nouveaux, citons les nouveaux moyens offerts aux autorités répressives pour la collecte et le traitement d'informations à caractère personnel, l'utilisation accrue de la biométrie et de l'identification par radiofréquence (RFID), ainsi que l'importance de plus en plus grande des flux de données mondiaux.

En 2007, le CEPD a rendu **12 avis** sur des propositions de législations européennes. Dans le domaine de la liberté, de la sécurité et de la justice, une préoccupation majeure a été l'adoption de nouvelles propositions visant à faciliter le stockage et l'échange d'informations entre autorités répressives, sans une évaluation en bonne et due forme de l'efficacité des instruments juridiques existants. Cette question a revêtu une importance particulière en ce qui concerne la transposition du traité de Prüm au niveau de l'UE et en ce qui concerne le système européen pour les dossiers passagers.

La question de l'absence d'un cadre juridique complet pour la protection des données a également joué un rôle déterminant dans les avis rendus par le CEPD en ce qui concerne le troisième pilier.

Un troisième enjeu réside dans le fait que l'UE impose aux États membres de créer des autorités nationales pour certaines tâches, mais leur laisse le choix de décider des conditions de leur fonctionnement. Cela empêche les États membres d'échanger des informations et porte atteinte à la sécurité juridique des personnes dont les données sont transférées entre les autorités de différents États membres.

L'échange d'informations avec des pays tiers à des fins répressives est une question distincte que le CEPD a traitée dans d'autres avis.

Dans un contexte plus général, le CEPD a rendu deux avis à propos de communications importantes de la

[37] Société de télécommunications interbancaires mondiales (*Society for Worldwide Interbank Financial Telecommunication*).

Commission sur le **futur cadre pour la protection des données**. Dans l'avis qu'il a rendu sur la mise en œuvre de la directive sur la protection des données[38], le CEPD a recensé diverses perspectives d'un contexte en mutation, l'une étant l'interaction avec la technologie. Les nouvelles évolutions technologiques ont une incidence évidente sur la nécessité d'un véritable cadre juridique pour la protection des données. **L'identification par radiofréquence**, qui est un aspect important de ces évolutions technologiques, a fait l'objet d'un autre avis du CEPD.

L'**inventaire 2008** (le second inventaire annuel) a été publié sur le site web du CEPD en décembre 2007. Il s'inscrit, dans les grandes lignes, dans le prolongement de l'inventaire 2007. L'annexe de l'inventaire montre que l'étendue des activités du CEPD atteint maintenant un grand nombre de domaines.

Dans son avis sur la communication relative à la mise en œuvre de la directive sur la protection des données, le CEPD a recensé cinq **perspectives pour les modifications futures**. Elles constitueront les points du programme pour ses activités futures. Il s'agit de :

- l'interaction avec la technologie;
- l'impact du traité de Lisbonne;
- le respect de la législation;
- le respect de la vie privée à l'échelle mondiale et les compétences;
- la mise en œuvre complète de la directive.

Coopération

Le principal forum de coopération entre les autorités compétentes en matière de protection des données en Europe est le **Groupe de travail « Article 29 »**. Le CEPD participe aux activités du groupe, qui joue un rôle important dans l'application uniforme des principes généraux de la directive 95/46/CE et dans leur interprétation.

Le CEPD salue les avis du Groupe de travail, auxquels il a activement contribué et dans lesquels les avis qu'il a lui-même rendus ont été pris en compte. À titre d'exemples de bonnes synergies entre les avis du Groupe de travail et ceux rendus par le CEPD en 2007, on peut citer les instructions consulaires communes adressées aux représentations diplomatiques et consulaires en rapport avec l'introduction d'éléments biométriques d'identification, ainsi que les transferts aux États-Unis de données sur les passagers des compagnies aériennes et l'utilisation de dossiers passagers à des fins répressives.

Le CEPD et le Groupe de travail ont également analysé en étroite collaboration deux grands systèmes relevant du premier pilier, à savoir le système de coopération en matière de protection des consommateurs et le système d'information du marché intérieur.

L'un des volets les plus importants de cette collaboration concerne le système Eurodac : à ce niveau, la responsabilité du contrôle de la protection des données est partagée entre les autorités nationales compétentes en matière de protection des données et le CEPD. En juillet 2007, le Groupe de coordination du contrôle d'Eurodac, composé des autorités nationales compétentes en matière de protection des données et du CEPD, a publié un rapport sur sa première inspection coordonnée d'**Eurodac**. Selon ce groupe, rien n'indique qu'il y ait eu usage abusif du système Eurodac. Certains aspects doivent néanmoins être améliorés, notamment l'information des personnes concernées.

Le CEPD s'efforce de garantir un niveau élevé et cohérent de protection des données dans le cadre des travaux des autorités de contrôle communes de Schengen, d'Europol, d'Eurojust et du système d'information douanier. En 2007, le CEPD a porté son attention sur deux points importants : la proposition de décision-cadre de la Commission relative à la protection des données dans le troisième pilier et l'échange d'informations en matière répressive conformément au principe de disponibilité.

Le CEPD a également participé aux **conférences européenne et internationale** sur la protection des données et la vie privée. La conférence internationale, qui a eu lieu à Montréal en septembre 2007, portait sur les nombreuses questions que traitent les commissaires

[38] Avis du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données (JO C 255 du 27.10.2007, p. 1).

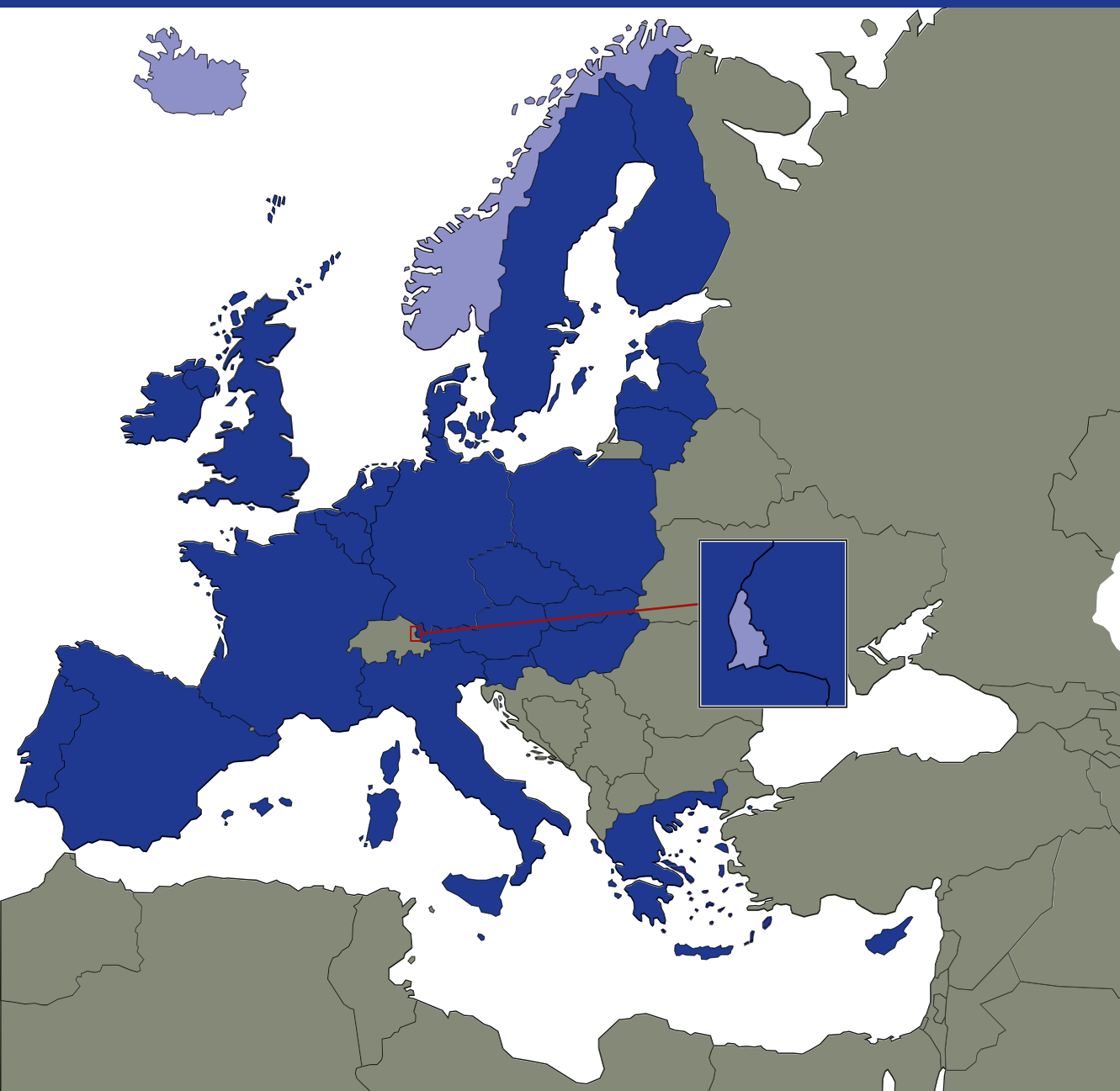
à la protection des données et de la vie privée, telles que la sécurité publique, la mondialisation, le droit et la technologie, l'« informatique omniprésente » et le « corps humain comme donnée ». Le CEPD a présidé une session réservée aux commissaires sur l'initiative de Londres et a contribué à un atelier sur la mondialisation.

Communication

Un des principaux objectifs poursuivis par le CEPD dans le cadre de ses activités de communication au cours de ses premières années d'existence consistait en l'amélioration de sa **visibilité** au niveau européen. Trois ans après le début de ses activités, les efforts consentis en matière de communication commencent à porter leurs fruits. Aussi, le contrôleur figurait-il parmi les 50 nominés au prix de l'Européen de l'année 2007 du magazine *European Voice*.

En tant que l'un des principaux architectes de l'**initiative de Londres**, conçue pour rendre plus efficaces la communication sur la protection des données et la protection des données elle-même, le CEPD a contribué activement, en février 2007, au travail de suivi dans l'atelier sur la communication organisé par la Commission nationale de l'informatique et des libertés (CNIL), l'autorité française compétente en matière de protection des données. Cet atelier a débouché notamment sur la création d'un réseau d'agents de communication auquel les autorités compétentes en matière de protection des données feront appel pour l'échange de bonnes pratiques et la réalisation de projets précis.

Chapitre 4
Principaux développements dans les pays de l'EEE



Islande

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

En 2007, plusieurs textes législatifs ont été adoptés dans le cadre de la transposition de la directive 95/46/CE (mais pas de la directive 2002/58/CE) concernant la protection des données. Les textes les plus importants sont repris ci-après.

1. Loi n° 36/2007 portant modification de la loi n° 66/1985 relatives aux Archives nationales. Selon la loi n° 36/2007, tous les documents relatifs à la sécurité nationale de l'Islande entre 1945 et 1991 seront conservés dans une section spéciale des Archives nationales. Cette loi a été adoptée après une large consultation concernant des écoutes téléphoniques réalisées durant la Guerre froide. Parmi les personnalités mises sur écoute téléphonique s'en trouvaient notamment certaines qui étaient influentes au sein des mouvements syndicaux et du Parti socialiste. La loi a été adoptée pour rendre publics les documents relatifs à ces événements, par exemple des ordonnances de tribunaux, et les documents concernant la sécurité nationale durant ces années en général. L'objectif était qu'ils puissent être consultés par le public et par les personnes visées, c'est-à-dire celles citées dans ces documents. Toutefois, les données personnelles à caractère sensible concernant des personnes autres que celles ayant demandé à consulter des documents seront effacées des copies des documents. Mais elles seront toutefois rendues publiques si les personnes auxquelles elles se rapportent consentent à leur divulgation.

2. Loi n° 40/2007 sur les services de santé. Selon l'article 20 de cette loi, c'est à l'Hôpital national qu'il revient de gérer, entre autres, une banque du sang. Toutefois, cette banque du sang ne fait pas l'objet de dispositions complémentaires, par exemple concernant la protection des données à caractère personnel. Les dispositions de la loi antérieure sur les services de santé (la loi n° 97/1990) étaient en revanche plus précises et stipulaient entre autres que l'Autorité de la protection des données avait pour mission de contrôler le traitement des données personnelles au sein des banques du sang. Dans un avis, l'APD a critiqué l'absence de telles dispositions dans le projet de loi qui a par la suite été adopté sous le numéro 40/2007. Aucune modification n'a été apportée au projet de loi pour donner suite à cette critique.

3. Loi n° 41/2007 sur la Direction nationale de la santé. Cette loi contient des dispositions concernant le traitement des données à caractère personnel, dont les plus importantes portent sur les registres de la Direction nationale de la santé. En vertu de l'article 8 de la loi, le consentement préalable des patients n'est pas requis pour inscrire leurs données dans ces registres, en l'occurrence les registres des naissances, des affections cardiovasculaires, des maladies nerveuses, des cancers, des accidents, des hospitalisations, des correspondances entre établissements de soins et des correspondances entre professionnels de la santé indépendants.

Le Directeur national de la santé, qui dirige la Direction nationale de la santé, est responsable de ces registres, qui ne sont toutefois pas tous conservés dans les locaux de la Direction. Ainsi, c'est à la Société cancérologique islandaise qu'est confié le registre des cancers. Dans ces registres, les éléments d'identification doivent être cryptés. Le traitement des données à caractère personnel doit être effectué dans le respect de la loi n° 77/2000 relative à la protection des données, et les mesures de sécurité concernant ces données doivent satisfaire aux exigences de l'APD. Tout usage de données à des fins de recherche scientifique doit être autorisé par l'APD.

Par ailleurs, en vertu de la loi n° 93/1994 concernant les produits pharmaceutiques (voir la loi 89/2003), la Direction nationale de la santé tient à jour une base de données sur les produits pharmaceutiques, où sont enregistrées les données de toutes les prescriptions médicales des trois dernières années (ce point est également mentionné dans la section consacrée à l'Islande dans les éditions de 2002 et de 2003 du rapport annuel). Les éléments d'identification sont cryptés, mais il est possible de les décrypter. Un projet de loi qui prévoit l'allongement de la période de conservation à 30 ans est actuellement à l'étude au Parlement. L'APD y est fortement opposée et l'a indiqué dans l'avis rendu concernant ce projet de loi.

4. Loi n° 163/2007 sur l'Office national de statistique. Les articles 5 à 8 stipulent que l'Office national de statistique

procède à la collecte de données, dont des données à caractère personnel, aux fins d'études statistiques. L'article 9 de la même loi autorise l'Office national de statistique à relier ses registres et ceux de tiers au moyen de numéros d'identification individuels ou autres codes d'identification.

Cette loi contient d'autres dispositions concernant la protection des données à caractère personnel. Ainsi, les membres du personnel de l'Office national de statistique sont tenus au secret professionnel (article 11), les données confidentielles doivent être supprimées après usage sauf s'il est prévu de les réutiliser aux fins d'études statistiques, auquel cas les éléments d'identification doivent être masqués ou supprimés (article 12). La loi impose à l'Office national de statistique d'adopter un règlement pour la sécurité et la conservation des données confidentielles, qui définit les procédures concernant la conservation et la destruction des documents sur papier et précise dans quelles conditions et à quel moment les données enregistrées sur support informatique seront supprimées et les éléments d'identification qui y figurent seront masqués ou cryptés (article 12 également).

L'article 13 prévoit que l'Office national de statistique peut autoriser des tiers à consulter des données à caractère personnel dans le cadre de recherches pour autant que ceux-ci s'engagent à lui retourner les données ou à supprimer les éléments d'identification à l'issue de leur projet de recherche. Dans l'avis rendu sur le projet de loi qui a été adopté sous le numéro 163/2007, l'APD a recommandé d'ajouter que la conservation de données par des tiers doit toujours s'assortir d'un délai et que les chercheurs qui prévoient de conserver les données au-delà de ce délai doivent en demander l'autorisation à l'Office national de statistique. Sa recommandation a été suivie.

Toutefois, le Parlement n'a pas suivi l'APD dans sa recommandation d'ajouter une disposition sur le cryptage des données lors du lien établi entre des registres conformément à l'article 9, comme mentionné plus haut.

B. Jurisprudence

Le 6 décembre 2007, la Cour suprême d'Islande a rendu un jugement à propos de la décision prise par l'APD le 27 février 2006. Elle a été saisie par un médecin qui, selon la décision de l'APD, avait consulté le dossier médical d'une personne sans son autorisation pour procéder à l'évaluation de son état de santé pour le compte d'une compagnie d'assurances. Selon la décision de l'APD, la consultation du dossier médical n'avait pas fait l'objet d'un consentement de la part de la personne visée et était, par voie de conséquence, illégale. Le tribunal d'arrondissement de Reykjavik a confirmé cette décision dans le jugement qu'il a rendu le 21 décembre 2006 (dont il fait état dans la section sur l'Islande dans l'édition de 2006 du rapport annuel).

Toutefois, la Cour suprême a infirmé la décision de l'APD. Elle a invoqué le fait que la personne concernée avait remis à son avocat une autorisation écrite par laquelle elle consentait à la consultation de son dossier médical ; l'avocat avait remis au médecin une copie de cette autorisation. Par ces motifs, la Cour a considéré que le médecin a agi de bonne foi lorsqu'il a consulté le dossier médical de cette personne. En d'autres termes, la Cour a estimé que le médecin avait toute raison de croire que la personne concernée avait consenti à ce qu'il consultât son dossier médical, même en l'absence d'autorisation écrite établie à son nom.

C. Questions diverses importantes

Les dossiers les plus importants que l'APD a traités en 2007 sont repris ci-dessous.

Le 19 février 2007, l'APD s'est prononcé sur la légalité de la consultation des dossiers électroniques des patients et sur les mesures de sécurité à ce propos à l'Hôpital national. Cet hôpital a autorisé certains membres de son personnel, notamment tous les médecins, à consulter les dossiers électroniques de tous les patients, à l'exception de certaines catégories de données, notamment celles concernant des troubles psychologiques, qui sont conservées dans une unité spéciale. Selon la direction de l'hôpital, un accès étendu s'imposait pour ces membres du personnel étant donné qu'ils s'occupent de patients dans tous les services de l'hôpital et prodiguent des

conseils sur les traitements dans tous les services. L'APD n'a pas remis cet argument en cause, mais a imposé de strictes mesures de sécurité, dont l'obligation pour les personnes qui consultent un dossier médical d'en indiquer la raison (en cochant une case, par exemple), l'enregistrement de toutes les consultations dans un fichier-journal et le contrôle régulier de ce fichier-journal.

Le 26 juin 2007, l'APD a décidé que la Direction nationale de la santé ne pouvait pas permettre à des chercheurs de consulter des données sensibles, notamment sur les avortements. Des chercheurs avaient demandé à consulter des données relatives à des femmes qui avaient participé à un projet en matière de contraception. Selon les informations fournies à ces femmes, les données recueillies les concernant seraient détruites à l'issue du projet. Toutefois, bien après le terme de ce projet, il était question de recueillir des données supplémentaires sur ces femmes sans leur demander leur consentement. L'APD a considéré que cette opération enfreignait la loi n° 77/2000 sur la protection des données et en est arrivée à la conclusion évoquée ci-dessus. Les chercheurs ont ensuite détruit toutes les données à caractère personnel qui avaient été recueillies dans le cadre du projet précédent.

Le 6 octobre 2007, l'APD s'est prononcée sur la collecte de données réalisée par une usine d'aluminium dans la ville de Hafnarfjördur dans le cadre d'un sondage d'opinion à propos de l'agrandissement de ses installations. Ce sondage a été réalisé par téléphone auprès des habitants de la ville. Les résultats de ce sondage ont été enregistrés dans une base de données électronique sans que les personnes interrogées n'en soient informées. L'APD en est arrivée à la conclusion que cela constituait une infraction à la loi relative à la protection des données.

Le 26 novembre 2007, l'APD s'est prononcée sur l'utilisation des empreintes digitales à la cantine d'une école primaire. Les empreintes digitales étaient utilisées pour limiter l'accès de la cantine aux élèves en droit d'y recevoir les repas de l'école. Ce sont des modèles de comparaison d'empreintes d'élèves qui étaient utilisés à cet effet. Ces modèles ne pouvaient pas être utilisés pour reproduire les empreintes digitales. Les parents d'élèves ont consenti à ce traitement, mais ils pouvaient aussi opter pour la carte de cantine nominative. L'APD en est arrivée à la conclusion que ce traitement ne constituait pas une infraction à la loi relative à la protection des données.

Le 26 novembre 2007, l'APD s'est prononcée sur l'opportunité d'accorder l'autorisation de relier des données génétiques issues de différents projets de recherche menés par la société de génie génétique deCode. Les données visées concernaient 85 000 personnes, qui avaient pris part à 66 projets. Ces personnes avaient consenti à la conservation de leurs données pour un usage dans le cadre d'un projet précis, mais également dans le cadre d'autres projets sous réserve de l'autorisation de l'APD et de la Commission nationale de bioéthique. Dans ce contexte, deCode n'envisageait pas de demander aux personnes concernées de donner leur consentement à ce que les données soient reliées. L'opération consistait à sélectionner parmi les personnes ayant participé à un projet celles ayant un génotype fréquent parmi les personnes ayant participé à un autre projet et à inclure leurs données dans cet autre projet. Les éléments d'identification seraient cryptés, mais il serait possible de les décrypter. L'APD a considéré que cette forme de traitement était trop vaste pour y appliquer le consentement des personnes à ce que leurs données soient utilisées dans d'autres projets de recherche. De plus, l'APD a estimé qu'elle n'était pas en droit d'autoriser cette forme de traitement. Elle a donc décidé de ne pas donner suite à la demande d'autorisation.

Le 10 décembre 2007, l'APD s'est prononcée sur la légalité des deux banques de données biologiques de la Société cancérologique islandaise et sur les mesures de sécurité les concernant. En vertu de la loi n° 110/2000 relative aux banques de données biologiques, les échantillons biologiques doivent être séparés des éléments d'identification et conservés à part. Mais l'une des banques de la société ne respecte pas cette disposition. L'APD a ordonné une mise en conformité avant le 1er septembre 2008. Cette banque de données biologiques est utilisée à des fins thérapeutiques. Un projet de loi récent précise que dans ce cas, il n'est pas nécessaire de conserver séparément les échantillons et les éléments d'identification.

Liechtenstein

A. Mise en œuvre des directives 95/46/CE et 2002/58/CE et autres développements législatifs

L'une des missions du Contrôleur de la protection des données (Datenschutzbeauftragten, en abrégé DSB) est de rendre des avis sur des projets de loi et règlements clés majeurs touchant à la protection des données et de vérifier leur conformité avec les dispositions de la directive 95/46/CE. En 2007, le DSB a ainsi rendu un avis sur plus de 20 projets de loi. En voici quelques exemples :

En ce qui concerne les prises de position dans le cadre des consultations concernant l'amendement de la loi relative à la reconnaissance des diplômes de l'enseignement supérieur et des qualifications professionnelles, de la loi sur les médecins, de la loi sur les vétérinaires, de la loi relative aux avocats, aux administrateurs judiciaires et aux ingénieurs conseil en propriété industrielle (Gesetz betreffend die Anerkennung von Hochschuldiplomen und beruflichen Befähigungsnachweisen, des Ärztegesetzes, des Gesetzes über das Veterinärwesen, des Gesetzes über die Rechtsanwälte, die Treuhänder und die Patentanwälte) ainsi que de la loi relative aux ingénieurs du bâtiment et aux architectes (Gesetz für die im Bauwesen tätigen Ingenieure und Architekten), c'est surtout l'instauration du système d'information sur le marché intérieur (IMI) qui intéresse de près la protection des données à caractère personnel. L'avis a souligné l'importance d'une réglementation unique pour les différentes catégories professionnelles concernées. En substance, le DBS a suggéré de se rapprocher le plus possible, dans les différents textes de loi, du texte de l'article 56 alinéa 2 de la directive sur les qualifications professionnelles et de l'avis substantiel du Groupe de travail « Article 29 » sur la protection des données pour les aspects juridiques soulevés par l'IMI (WP 140). À la fin de l'année de référence 2007, tous les amendements liés à l'IMI n'avaient pas encore été adoptés.

Une loi sur la réutilisation des informations du secteur public (Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen, dite Informationsweiterverwendungsgesetz, en abrégé IWG) assurera la transposition dans le droit national de la directive 2003/98/CE concernant la réutilisation des informations du secteur public. Dans son avis, le DSB a fait référence à l'avis 7/2003 du Groupe de travail « Article 29 » sur la réutilisation des informations du secteur public et la protection des données à caractère personnel daté du 12 décembre 2003 (WP 83). Par ailleurs, dans le même temps, il a été suggéré d'amender l'article 17 alinéa 2 point f et l'article 3 alinéa 1 point c de la loi sur la protection des données à caractère personnel (Datenschutzgesetz, en abrégé DSG). Contrairement à un certain nombre d'autres lois nationales relatives à la protection des données en Europe, la législation du Liechtenstein stipule que les données à caractère personnel ne peuvent être traitées que si la personne concernée en a autorisé l'accès. Le DSB aspire ici toutefois à une application plus large et a donc proposé d'amender la loi relative à la protection des données en expliquant qu'il suffit que les données personnelles soient publiquement accessibles (par exemple via l'annuaire téléphonique). Une telle vision autoriserait une pratique plus large qui, à la lumière de la nouvelle IWG, serait sage et souhaitable. Le droit d'opposition aux termes de l'article 16 alinéa 3 de la DSG demeure ici inchangé.

Un amendement à la loi relative aux pratiques commerciales déloyales (Gesetz über den unlauteren Wettbewerb, en abrégé UWG) était en cours d'examen en 2007, l'amendement devant permettre la transposition des dispositions de la directive 2005/29/CE relative aux pratiques commerciales déloyales, qui vise en particulier à faciliter les échanges transfrontaliers. Conformément à ces nouvelles dispositions qui doivent être introduites au Liechtenstein, non seulement les sollicitations importunes par télécopieur et courriel, mais aussi les sollicitations téléphoniques seront considérées comme des pratiques commerciales agressives, voire déloyales en cas de sollicitations persistantes. D'où une évaluation différente de ce type de sollicitation non désirée par rapport à celle prévue par la loi relative aux communications électroniques (Kommunikationsgesetz) en fonction du canal utilisé. Conformément à cette dernière, toute publicité qui serait envoyée par télécopieur ou par courrier électronique sans que le destinataire n'en ait fait la demande est en principe interdite dès le premier envoi[39].

[39] Article 50 de la loi relative aux communications électroniques (*Kommunikationsgesetz*, en abrégé KomG).

Par contre, cette loi ne mentionne pas la publicité non désirée par téléphone. La nouvelle UWG n'interdirait pas d'emblée les sollicitations téléphoniques, mais n'entraînerait des conséquences sur le plan du droit (pénal) que s'il s'agit de sollicitations persistantes au sens de la loi relative aux pratiques commerciales déloyales. En conséquence, on assisterait, au Liechtenstein, à une distinction – en termes juridiques – entre les publicités non sollicitées par téléphone et les sollicitations par télécopieur ou par courrier électronique. Dans son avis concernant le projet de révision de l'UWG, le DSB a affirmé qu'il était dans l'intérêt des consommateurs de faire remarquer cette divergence et de promouvoir un traitement juridique égal de tous les canaux utilisés, ceci afin de protéger efficacement les consommateurs.

L'amendement de la loi relative à la police (*Polizeigesetz*), entrée en vigueur en 2007, a lui aussi revêtu une importance juridique toute particulière en matière de protection des données. Dans le cadre des compétences policières en matière d'enquête, quelques nouvelles bases juridiques ont été établies : la collecte et le traitement de données biométriques sont désormais autorisés dans des cas bien précis, et l'enregistrement de sons et d'images lors de manifestations publiques ou dans des lieux publics est maintenant possible sous certaines conditions.

L'autorisation de principe de la vidéosurveillance par la police nationale représente, au Liechtenstein, la seule et unique réglementation autorisant la vidéosurveillance dans des lieux publics. Elle revêt donc pour cette raison une importance considérable en termes de protection des données. Par la suite, plusieurs réglementations en matière d'entraide administrative (internationale) ont vu le jour, et le système d'information électronique bénéficie désormais d'une base légale. Du point de vue de la protection des données, ce système d'information n'est pas sans poser de problème, étant donné qu'il doit permettre d'interconnecter plusieurs bases de données.

Un droit indirect de demande d'information a donc été introduit tout récemment. En cas d'intervention des services de sécurité de l'État ou lors d'une enquête préventive dans le cadre d'une affaire criminelle, la personne concernée peut ainsi demander, non pas personnellement, mais par le biais du Contrôleur de la protection des données, si des données le concernant sont en cours de traitement. Fin 2007, personne n'avait fait usage de ce droit indirect à l'information.

Dans ce contexte, retenons également l'amendement à la loi sur l'octroi et la perte de la nationalité (*Gesetz über den Erwerb und Verlust des Landesbürgerrechts*) ainsi que la création d'une base juridique pour le registre central des personnes de l'administration nationale du (*Zentrale Personenverwaltung der liechtensteinischen Landesverwaltung*, en abrégé ZPV). Il s'agit là d'un projet de loi qui, en raison de la problématique juridique liée à la protection des données, est d'actualité déjà depuis de nombreuses années déjà mais qui n'a toutefois pas encore pu être adoptée en 2007[40].

Enfin, la loi, modifiée, relative aux banques (*Bankengesetz*) a introduit des obligations liées à la protection des données, dans le cadre de la coopération des autorités ou vis-à-vis de la clientèle, avec, en particulier, l'obligation générale d'information envers les clients des banques. Il convient de préciser que cette obligation d'information s'applique non seulement à la clientèle existante mais aussi, conformément aux directives 2004/39/CE et 2006/73/CE, aux clients potentiels.

À cet égard, il convient également de mentionner le règlement 1781/2006 de l'UE (relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds) qui n'était toujours pas entré en vigueur au Liechtenstein en 2007. Étant toutefois déjà applicable en 2007 au sein de l'UE, ce règlement produit d'ores et déjà certains effets au Liechtenstein, à savoir dans les mouvements de fonds transfrontaliers entre une banque du Liechtenstein et une banque de l'UE. Les banques du Liechtenstein ont donc été contraintes d'informer leurs clients, au cours de l'année de référence, des effets dudit règlement bien que celui-ci ne soit pas encore transposé dans le droit national.

B. Jurisprudence

La Cour d'État du Liechtenstein a rendu, en sa qualité de Cour constitutionnelle, un arrêt historique en matière

[40] Voir 9e Rapport annuel du Groupe de travail « Article 29 » sur la protection des données, page 128.

d'entraide administrative (internationale) et de secret bancaire[41]. L'arrêt a estimé que le secret bancaire était matière constitutionnelle même s'il n'était ancré qu'au niveau des lois. L'objectif est de protéger les aspects financiers des sphères secrètes et privées d'une entité dans les limites prévues par la loi. Cette protection est accordée par l'intermédiaire du droit à la liberté personnelle inscrit à l'article 32 de la Constitution du Liechtenstein.

Le secret bancaire n'est donc pas enfreint lorsque les autorités de contrôle compétentes respectent, dans le cadre d'une demande d'entraide internationale, les principes de la spécialité et de la confidentialité, ainsi que le *Prinzip der langen Hand* (accord donné par les autorités de contrôle à d'autres organes) et le principe de proportionnalité inscrits explicitement à l'article 38 de la loi relative aux banques. L'entraide administrative et l'entraide judiciaire ne sont donc pas toujours faciles à distinguer. La procédure d'entraide administrative ne peut donc pas contourner l'entraide judiciaire lorsque l'entraide administrative respecte ces principes. Étant donné qu'il faut apporter, en plus de la suspicion initiale, des éléments supplémentaires attestant d'une suspicion suffisamment bien fondée de conduite pénalement répréhensible, les enquêtes préalables à l'aveuglette (*Fishing expeditions*), c'est-à-dire la réalisation d'une procédure administrative visant en réalité à rechercher des preuves, ne sont ni possibles ni autorisées.

C. Questions diverses importantes

En ce qui concerne l'accès des autorités américaines aux données relatives aux transactions internationales (*Affaire Swift*), les banques ont accédé à la demande du DSB et modifié leurs conditions générales de vente. Il convient toutefois de souligner qu'en cas de règlement par des canaux internationaux, les données relatives aux ordres traversent les frontières. Dans ce cas, les données ne sont donc plus protégées par la législation du Liechtenstein, et il ne peut plus être garanti que les personnes bénéficient d'un niveau de protection des données correspondant à celui qui existe au Liechtenstein. Enfin, il convient de ne pas perdre de vue que des législations étrangères et des décisions réglementaires obligent les banques et les gestionnaires de systèmes concernés à transmettre ces données à des tiers.

En outre, un projet visant à mettre en place un service de *Integriertes Case Management* a fait l'objet d'une consultation[42]. Selon le DSB, il convenait en effet de bien y ancrer les déclarations relatives à la protection des données et les accords de confidentialité et de non-divulgation.

Le souhait accru des autorités à pouvoir recourir à la vidéosurveillance a donné lieu à des débats quelques peu controversés. Une affaire de vidéosurveillance dans un lieu public effectuée par une autorité a été soumise à l'autorité de protection des données pour avis. Fin 2007, aucun avis n'avait encore été rendu.

Mentionnons aussi une légère progression des demandes de renseignements[43] ainsi qu'une augmentation du nombre de visites enregistrées sur la page d'accueil du site Internet du DSB[44]. Ce désir accru d'information reflète la prise de conscience grandissante du public en matière de protection des données. Outre des thèmes d'actualité, le site Internet propose des manuels relatifs à l'interprétation et à l'application de la loi relative à la protection des données, les *Richtlinien*. Deux publications sont disponibles depuis 2007 : « Richtlinien zur Videoüberwachung durch Behörden » (sur la vidéosurveillance par les autorités publiques) et « Richtlinien über den Umgang mit unerwünschter Werbung, insbesondere mit Spam » (traitement des publicités non sollicitées, et en particulier les spams).

[41] Arrêt de la Cour constitutionnelle du 6 février 2006, StGH 2005/50, mais publié en 2007 *in* Liechtensteinische Juristenzeitung, 2007, LES 4/07, Page 396ff.

[42] *L'Integrierte Case Management* vise à faciliter la réinsertion professionnelle d'un employé victime d'une incapacité de travail de plus de 6 semaines. Conformément à une nouvelle disposition, l'employeur devra écrire un courrier à la caisse d'assurance maladie au plus tard après 6 semaines d'absence de son employé afin de demander l'intervention d'un *Case Manager*. Cette personne prendra alors directement contact avec l'employé pour lui demander s'il peut lui apporter son aide en vue de faciliter son retour dans l'entreprise. L'employé est libre d'accepter ou de refuser cette aide.

[43] Au cours de l'année de référence 2007, 338 demandes de renseignement ont été enregistrées et traitées.

[44] Au cours de l'année de référence 2007, le nombre d'accès au site Internet de la SDS a atteint 54 679.

Norvège

A. Mise en œuvre de la directive 95/46/CE Changements significatifs apportés à la législation relative au respect de la vie privée ou à la protection des données

Aucun changement significatif à signaler.

Changements significatifs apportés à d'autres lois en rapport avec le respect de la vie privée et la protection des données

Amendements à la loi relative à l'exécution des peines et au code civil et pénal général : instauration de l'obligation d'informer, dispositions concernant la bonne conduite antérieure et notification à la victime, etc.

Ces amendements étendent l'obligation d'informer la victime ou ses proches survivants ; désormais, s'appliquent aussi aux congés pénitentiaires avant libération et aux peines effectuées en dehors du milieu carcéral. Cette obligation porte notamment sur la durée de la peine ainsi que sur les conditions d'exécution de la peine si elles affectent directement la victime ou ses proches survivants. Parmi ces conditions, citons entre autres le lieu de résidence, l'interdiction faite au condamné d'entrer en contact avec certaines personnes et le changement de domicile du condamné.

Selon le Bureau des données, les amendements proposés à l'issue d'un processus normal de consultation reflètent uniquement le point de vue des victimes et leurs implications pour les condamnés doivent être analysées de manière plus approfondie. Par ailleurs, le Bureau a exigé de limiter à un minimum les informations fournies et a estimé que rien ne justifiait que la victime eût toujours connaissance de l'adresse du condamné, y compris durant sa mise en liberté surveillée. Il devrait suffire à la victime de savoir que le condamné n'est plus incarcéré. Le Bureau des données a également rappelé que les services correctionnels nationaux étaient dans l'obligation d'informer le condamné de son devoir d'informer.

Un règlement plus strict a également été adopté concernant l'utilisation des moyens électroniques de communication en milieu carcéral. Le Bureau des données a déclaré s'interroger sur la nécessité d'adopter un règlement plus strict. Il estime que dans la société technologique actuelle, les communications électroniques doivent être assimilées aux services postaux et téléphoniques classiques, si le budget des services correctionnels le permet.

Amendements à la loi sur la publication des listes d'impôts directs

Le durcissement de la réglementation sur la publication des listes d'impôts directs, intervenu en 2004, limitait entre autres à trois semaines à compter de leur publication le délai pendant lequel ces listes pouvaient être consultées par des particuliers. Ces listes étaient ensuite enregistrées en ligne sur le site web des autorités fiscales et fournies sur papier aux bureaux de perception. En 2007, un amendement a redonné aux médias accès à l'intégralité des listes d'impôts directs sur CD-ROM. Pour justifier cet amendement, le gouvernement a notamment invoqué sa volonté d'alimenter le débat critique sur le régime fiscal.

Le Bureau des données estime que ces amendements ne sont pas heureux. Depuis plusieurs années, il est préoccupé par la question de la publication des listes d'impôts directs. Il considère qu'il s'agit d'un manquement aux principes fondamentaux de la protection des données, car les informations que les citoyens norvégiens sont obligés de soumettre sont utilisées à des fins de divertissement, sont consultées pour des recherches et peuvent être vendues sous forme de texto ou sous une autre forme semblable. Que ces listes d'impôts directs soient publiées avant le terme du délai de recours contre l'assiette de l'impôt est également discutable.

Nouvelle loi sur la séduction malintentionnée d'enfants

En vertu d'une nouvelle loi, séduire et manipuler un enfant dans l'intention de commettre des abus sexuels sur lui est une infraction pénale. Le Bureau des données a admis qu'il était louable pour les responsables politiques de chercher des moyens de prévenir les abus sexuels sur les enfants, mais a déclaré qu'en sa qualité de gardien de la protection des données à caractère personnel, il s'intéressait à la question de savoir quelles seront les mesures d'application de cette loi, en l'oc-

currence quelles méthodes d'enquête la police pourra utiliser dans ce cadre.

B. Jurisprudence

Aucun cas à signaler.

C. Questions diverses importantes

Inspection de l'administration pénitentiaire
Le Bureau des données a sévèrement critiqué le ministère de la justice et de la police après le contrôle du traitement des données personnelles sensibles au sein de l'administration pénitentiaire. Les infractions graves à la loi que ce contrôle a révélées montrent que les manquements au respect de la vie privée concernent plus de 30 000 anciens détenus et leurs proches.

Pendant plusieurs années, le Bureau des données a reçu des plaintes de personnes incarcérées en Norvège au sujet du traitement de leurs données personnelles par l'administration pénitentiaire. La plupart de ces plaintes dénoncent le fait que les informations concernant les détenus et leurs proches ne sont pas protégées comme il se doit.

À l'issue du contrôle, le Bureau des données a conclu à l'existence d'un registre personnel parallèle et ouvert à la prison d'Ila (« détenus par numéro »). Ce registre contient des données personnelles très sensibles. De plus, les données personnelles sont enregistrées dans le système de gestion sans fondement juridique. Les droits fondamentaux des personnes enregistrées garantis par la loi sur la protection des données, en ce qui concerne le droit d'accès, de rectification et de suppression, ne sont pas respectés.

Vols massifs de données chez des opérateurs de télécommunications – Plainte officielle
Les sites web de plusieurs opérateurs de télécommunications ont été piratés pour rassembler des données à caractère personnel durant une période allant approximativement du 28 juillet au 7 août 2007. Cette collecte de données personnelles a débuté par la génération automatisée d'une liste de numéros d'identification personnels susceptibles d'être conservés dans un programme de données. Cette liste a ensuite été comparée avec un site officiel pour en supprimer les numéros non utilisés. Les numéros restants ont été utilisés pour rechercher le nom et les coordonnées de personnes sur les sites web des opérateurs de télécommunications. Rares sont les personnes affectées qui étaient en relation avec ces opérateurs ; elles ont été nombreuses à être surprises et mécontentes d'apprendre que cela leur était arrivé.

Le Bureau des données considère que les infractions les plus graves résident dans le défaut de conserver les données sous bonne protection et de fournir des informations complémentaires et dans le fait que plusieurs opérateurs n'ont pas pris la peine de prévenir les personnes affectées par l'incident. Le fait de n'avoir pas prévenu les personnes affectées illustre le peu de cas qui est fait du droit individuel au respect de la vie privée.

Le Bureau des données a décidé de porter plainte pour infraction aux dispositions de la loi relatives à la protection des données à caractère personnel concernant la conservation sous protection des données et concernant l'obligation d'informer le Bureau des données. Plusieurs des personnes enregistrées ont également porté plainte. Le ministère public a commencé par rejeter ces plaintes, mais a décidé depuis lors de les reconsidérer.

Nouvelle loi sur la liberté d'information
La nouvelle loi sur la liberté d'information a été adoptée et devrait entrer en vigueur le 1er juillet 2008. Les règlements y afférents, qui ont fait l'objet d'un processus de consultation, imposent à un certain nombre d'instances et d'entités publiques de mettre leurs dossiers électroniques en ligne. Ils précisent également que les documents doivent être rendus publics autant que faire se peut. Cette publication massive de données personnelles inquiète le Bureau des données. La collecte de nombreuses données personnelles peut permettre de dresser un profil précis des personnes. Ce qui peut être utile à des fins de marketing, mais aussi à des fins d'usurpation d'identité. Les individus qui ont l'intention d'usurper une identité sont en mesure d'obtenir un aperçu exhaustif des actes et des préférences de leur cible.

Le Bureau des données a constaté un certain nombre de cas dans lesquels des municipalités ont mis en ligne des données à caractère personnel qui n'auraient pas dû y être accessibles. Certains de ces documents contenaient des dates de naissance ou des numéros d'identification ou encore des réponses à des offres d'emploi assorties de diplômes et de références, alors que d'autres portaient sur des personnes en difficulté qui avaient demandé de l'aide à la municipalité. Ce genre d'erreurs peut avoir des conséquences désastreuses pour les personnes concernées. Les ministères et les municipalités qui constatent que des informations confidentielles à caractère personnel sont publiées invoquent souvent l'erreur humaine. Le Bureau des données estime que des « incidents » répétés révèlent une défaillance de système au sein de l'organisation.

Vie professionnelle, accès aux courriers électroniques des membres du personnel — Plaintes

En 2005, le Bureau des données a porté plainte contre deux entreprises pour cause d'infraction aux dispositions de la loi relative à la protection des données concernant l'obligation d'informer dans le cadre de l'accès aux courriers électroniques du personnel. Le ministère public a classé ses deux plaintes sans suite en 2006. Le Bureau des données a fait appel de ces deux décisions, mais le procureur général les a maintenues toutes les deux. Il a toutefois ordonné au ministère public d'ouvrir une enquête pour déterminer si des membres du personnel de l'une des deux entreprises avaient caché des informations au Bureau des données. Ce dossier a également été classé sans suite en 2007.

En 2006, le Bureau des données a porté plainte contre un éditeur pour cause d'infraction à la loi sur la protection des données. En cause, le gérant d'une maison d'édition qui copiait automatiquement les courriers électroniques entrants des membres de son personnel à leur insu au moyen d'un « compte de surveillance » pour les envoyer à la direction du siège en Suède. La messagerie électronique des membres du personnel était protégée par un nom d'utilisateur et un mot de passe personnel, mais le gérant pouvait accéder à leur boîte de réception au moyen de son « compte de surveillance ». Les membres du personnel n'avaient pas connaissance du téléchargement et de la consultation des courriers électroniques qui leur étaient destinés, ni de l'objet de l'opération ou de la divulgation d'informations.
La maison d'édition et son gérant ont été condamnés en 2007 pour avoir manqué à leur obligation d'informer et ont accepté l'amende qui leur a été infligée.

Cartes de péage — AutoPASS

Au printemps 2007, le Bureau des données a appris que les passages au péage étaient systématiquement photographiés. Or, cette procédure ne correspond pas aux spécifications officielles concernant le système AutoPASS, pas plus qu'elle ne cadre avec les informations que la Direction du réseau routier avait transmises auparavant au Bureau des données à ce sujet. Le Bureau des données a donc demandé à la Direction du réseau routier de confirmer ou d'infirmer le fait que les passages au péage étaient tous photographiés dans toutes les gares de péage de Norvège. Il a déduit de la réponse qu'il a reçue de la Direction du réseau routier que les véhicules sont tous photographiés lors de leur passage au péage. Toutefois, les photos des véhicules ne sont enregistrées dans le système qu'en cas de passage non conforme au péage ou lors de contrôles aléatoires. Autre circonstance atténuante, la mémoire interne des appareils de prise de vue est limitée, et les photos qui ne sont pas enregistrées dans le système sont relativement rapidement remplacées par d'autres. Le Bureau des données a estimé regrettable que ni l'opinion, ni ses services n'aient été informés de cette procédure à un stade plus précoce. Il compte sur un perfectionnement du système.

Les 100 derniers passages dans une gare de péage sont enregistrés dans la carte AutoPASS

Au début de l'année de référence, le Bureau des données a révélé que les cent derniers passages des utilisateurs de la carte AutoPASS dans une gare de péage étaient enregistrés dans la puce de leur carte. Par ailleurs, d'autres points de passage étaient également enregistrés. Que ces informations personnelles soient enregistrées dans des puces lisibles à distance, sans la moindre protection de la confidentialité, a également interpellé le Bureau des données. L'infraction la plus grave réside toutefois dans le fait que les utilisateurs de la carte AutoPASS,

qui sont au nombre d'un million environ, n'ont pas été dûment informés de la capacité de la puce de leur carte à enregistrer le lieu et l'heure de leurs cent derniers passages dans une gare de péage.

Nouvelle loi sur la recherche médicale

Un projet de loi concernant la recherche médicale a été soumis au Storting (Parlement) durant l'été 2007. Le Bureau des données y a épinglé plusieurs points obscurs, en rapport notamment avec ses compétences dans le cadre de la loi. Le principe fondamental de ce projet de loi est que pour utiliser des données personnelles dans des recherches médicales, il est impératif d'obtenir le consentement des personnes auxquelles ces données se rapportent.

Toutefois, le projet de loi prévoit tellement de cas où il serait possible de passer outre ce consentement qu'il est à craindre que l'obligation fondamentale de l'obtention du consentement n'en soit plus une dans les faits.

Ce projet de loi instaure également un nouveau concept juridique, en l'occurrence celui de « consentement général ». Ce concept va au-delà de la notion convenue jusqu'ici et revient en quelque sorte à signer un contrat sans avoir le droit de prendre connaissance de ses clauses. Le Bureau des données déplore l'emploi du terme « consentement » pour désigner ce concept dans le projet de loi relatif à la recherche médicale, car il estime qu'il risque de compromettre le droit fondamental de l'individu à être informé et à disposer de soi et de saper la confiance pourtant essentielle entre le patient et son médecin. Le Bureau des données a demandé au Storting d'étudier les effets positifs et négatifs du texte de manière plus approfondie avant de l'adopter.

Chapitre 5
Membres et observateurs du Groupe de travail «Article 29» relatif à la protection des données

MEMBRES DU GROUPE DE TRAVAIL « ARTICLE 29 » RELATIF À LA PROTECTION DES DONNÉES EN 2007

Autriche	**Belgique**
M^me^ Waltraut Kotschy Commission autrichienne de la protection des données (Datenschutzkommission) Ballhausplatz 1 – AT – 1014 Wien Tél : +43 1 531 15 / 2525 Fax : +43 1 531 15 / 2690 E-mail : dsk@dsk.gv.at Site web : http ://www.dsk.gv.at/	Mr Willem Debeuckelaere (Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer)Rue Haute, 139 – BE – 1000 Bruxelles Tél : +32(0)2/213.85.40 Fax : +32(0)2/213.85.65 E-mail : commission@privacycommission.be Site web : http ://www.privacycommission.be/
Bulgarie	**Chypre**
M. Krassimir Dimitrov Commission de protection des données à caractère personnel (Комисия за защита на личните данни) 1 Dondukov – BG – 1000 Sofia Tél : +359 2 940 2046 ; +359 2 915 3501 Fax : +359 2 940 3640 E-mail : kzld@government.bg Site web : http ://www.cdpd.bg	M^me^ Goulla Frangou Commissaire à la protection des données à caractère personnel (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 40, Themistokli Dervi str. Natassa Court, 3rd floor – CY – 1066 Nicosia (P.O. Box 23378 – CY – 1682 Nicosia) Tél : +357 22 818 456 Fax : +357 22 304 565 E-mail : commissioner@dataprotection.gov.cy Site web : http ://www.dataprotection.gov.cy
République tchèque	**Danemark**
M. Igor Nemec Bureau de la protection des données à caractère personnel (Úřad pro ochranu osobních údajů) Pplk. Sochora 27 – CZ – 170 00 Praha 7 Tél : +420 234 665 111 Fax : +420 234 665 501 E-mail : posta@uoou.cz Site web : http ://www.uoou.cz/	M^me^ Janni Christoffersen Agence danoise de protection des données (Datatilsynet) Borgergade 28, 5th floor – DK – 1300 Koebenhavn K Tél : +45 3319 3200 Fax : +45 3319 3218 E-mail : dt@datatilsynet.dk Site web : http ://www.datatilsynet.dk

Estonie	**Finlande**
M. Urmas Kukk Bureau estonien de la protection des données (Andmekaitse Inspektsioon) Väike – Ameerika 19 – EE – 10129 Tallinn Tél : +372 6274 135 Fax : +372 6274 137 E-mail : info@dp.gov.ee Site web : http ://www.dp.gov.ee	M. Reijo Aarnio Médiateur chargé de la protection des données (Tietosuojavaltuutetun toimisto) Albertinkatu 25 A, 3rd floor – FI – 00181 Helsinki (P.O. Box 315) Tél : +358 10 36 166700 Fax : +358 10 36 166735 E-mail : tietosuoja@om.fi Site web : http ://www.tietosuoja.fi
France	**Allemagne**
M. Alex Türk Président de la Commission Nationale de l'Informatique et des Libertés – CNIL Rue Vivienne, 8 -CS 30223 FR – 75083 Paris Cedex 02 Tél : +33 1 53 73 22 22 Fax : +33 1 53 73 22 00 M. Georges de La Loyère Commission Nationale de l'Informatique et des Libertés – CNIL Rue Vivienne, 8 -CS 30223 FR – 75083 Paris Cedex 02 Tél : +33 1 53 73 22 22 Fax : +33 1 53 73 22 00 E-mail : laloyere@cnil.fr Site web : http ://www.cnil.fr	M. Peter Schaar **Chairman** Le Commissaire fédéral à la protection des données et du droit à l'information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) Husarenstraße 30 – DE -53117 Bonn Tél : +49 (0)1888 7799-0 Fax : +49 (0)1888 7799-550 E-mail : postsTélle@bfdi.bund.de Site web : http ://www.bfdi.bund.de M. Alexander Dix (représentant des états allemands / Bundesländer) Le Commissaire à la protection des données et à la liberté d'information de Berlin (Berliner Beauftragter für Datenschutz und Informationsfreiheit) An der Urania 4-10 – DE – 10787 Berlin Tél : +49 30 13 889 0 Fax : +49 30 215 50 50 E-mail : mailbox@datenschutz-berlin.de Website : http ://www.datenschutz-berlin.de
Grèce	**Hongrie**
M. Nikolaos Frangakis Autorité hellénique pour la protection des données à caractère personnel (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1-3, avenue Kifisias, CP 115 23 Ampelokipi – GR – Athènes Tél : +30 210 6475600 Fax : +30 210 6475628 E-mail : contact@dpa.gr Site web : http ://www.dpa.gr	M. Attila Peterfalvi Commissaire parlamentaire à la protection des données (Adatvédelmi Biztos) Nador u. 22 – HU – 1051 Budapest Tél : +36 1 475 7186 Fax : +36 1 269 3541 E-mail : adatved@obh.hu Site web : http ://abiweb.obh.hu/abi/

Irlande	**Italie**
M. Billy Hawkes Commissaire à la protection des données (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlington, IE -Co.Laois Tél : +353 57 868 4800 Fax :+353 57 868 4757 E-mail : info@dataprotection.ie Site web : http ://www.dataprotection.ie	M. Francesco Pizzetti Autorité italienne de protection des données (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 – IT – 00186 Roma Tél : +39 06.69677.1 Fax : +39 06.69677.785 E-mail : garante@garanteprivacy.it, f.pizzetti@garante-privacy.it Site web : http ://www.garanteprivacy.it
Lettonie	**Lituanie**
M^me^ Signe Plumina Inspection nationale des données (Datu valsts inspekcija) Kr. Barona 5-4, Riga, LV – 1050 Tél : +371 6722 31 31 Fax : +371 6722 35 56 E-mail : signe.plumina@dvi.gov.lv, info@dvi.gov.lv Site web : http ://www.dvi.gov.lv	M. Algirdas Kunčinas Inspection de protection des données (Valstybinė duomenų apsaugos inspekcija) Žygimantų str. 11-6a – LT-01102 Vilnius Tél : +370 5 279 14 45 Fax : + 370 5 261 94 94 E-mail : ada@ada.lt Site web : http ://www.ada.lt
Luxembourg	**Malte**
M. Gérard Lommel Commission nationale pour la Protection des Données – CNPD 41, avenue de la Gare – LU – 1611 Luxembourg Tél : +352 26 10 60 -1 Fax : +352 26 10 60 – 29 E-mail : info@cnpd.lu Site web : http ://www.cnpd.lu	M. Paul Mifsud Cremona Commissaire à la protection des données 2, Airways House High Street – MT – SLM 1549 Sliema Tél : +356 2328 7100 Fax : +356 23287198 E-mail : commissioner.dataprotection@gov.mt Site web : http ://www.dataprotection.gov.mt
Pays-Bas	**Pologne**
M. Jacob Kohnstamm Autorité néerlandaise de protection des données (College Bescherming Persoonsgegevens – CBP) Juliana van Stolberglaan 4-10, P.O Box 93374 2509 AJ Den Haag Tél : +31 70 8888500 Fax : +31 70 8888501 E-mail : info@cbpweb.nl Site web : http :// www.cbpweb.nl http ://www.mijnprivacy.nl	M. Michał Serzycki Inspector général pour la protection des données à caractère personnel (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 – PL – 00193 Warsaw Tél : +48 22 860 70 86 Fax : +48 22 860 70 90 E-mail : Sekretariat@giodo.gov.pl Site web : http ://www.giodo.gov.pl

Portugal	**Roumanie**
M. Luís Novais Lingnau da Silveira Commission nationale de protection des données (Comissão Nacional de Protecção de Dados – CNPD) Rua de São Bento, 148, 3º PT – 1 200-821 Lisboa Tél : +351 21 392 84 00 Fax : +351 21 397 68 32 E-mail : geral@cnpd.pt Site web : http ://www.cnpd.pt	M[me] Georgeta Basarabescu Autorité natinale de contrôle du traitement des données à caractère personnel (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Olari Street no. 32, Sector 2, RO – Bucharest Tél : +40 21 252 5599 Fax : +40 21 252 5757 E-mail : georgeta.basarabescu@dataprotection.ro international@dataprotection.ro Site web : http ://www.dataprotection.ro
Slovaquie	**Slovenie**
M. Gyula Veszelei le Bureau de protection des données à caractère personnel de la République Slovaque (Úrad na ochranu osobných údajov Slovenskej republiky) Odborárske námestie 3 – SK – 81760 Bratislava 15 Tél : +421 2 5023 9418 Fax : +421 2 5023 9441 E-mail : statny.dozor@pdp.gov.sk Site web : http ://www.dataprotection.gov.sk	M[me] Natasa Pirc Musar Commissaire à l'information (Informacijski pooblaščenec) Vosnjakova 1, SI – 1000 Ljubljana Tél : +386 1 230 97 30 Fax : +386 1 230 97 78 E-mail : gp.ip@ip-rs.si Site web : http ://www.ip-rs.si
Espagne	**Suède**
M. Artemi Rallo Lombarte Agence espagnole de protection des données (Agencia Española de Protección de Datos) C/ Jorge Juan, 6 ES – 28001 Madrid Tél : +34 91 399 6219/20 Fax : + 34 91 445 56 99 E-mail : director@agpd.es Site web : http ://www.agpd.es	M. Göran Gräslund Inspection des données (Datainspektionen) Fleminggatan, 14 (Box 8114) – SE – 104 20 Stockholm Tél : +46 8 657 61 57 Fax : +46 8 652 86 52 E-mail : datainspektionen@datainspektionen.se, goran.graslund@datainspektionen.se Site web : http ://www.datainspektionen.se
Royaume-Uni	**Contrôleur européen de protection des données**
M. Richard Thomas Bureau du commissaire à l'information Wycliffe House Water LaneWilmslow, SK9 5AF GB Tél : +44 1625 545700 Fax : +44 1625 524510 E-mail : Veuillez compléter le formulaire sur notre site internet Site web : http ://www.ico.gov.uk	M. Peter Hustinx Contrôleur Européen de la Protection des Données (CEPD) Postal address : 60, rue Wiertz, BE – 1047 Brussels Office : rue Montoyer, 63, BE – 1047 Brussels Tél : +32 2 283 1900 Fax : +32 2 283 1950 E-mail : edps@edps.europa.eu Site web : http ://www.edps.europa.eu

OBSERVATEURS DU GROUPE DE TRAVAIL « ARTICLE 29 » RELATIF À LA PROTECTION DES DONNÉES EN 2007

Icelande	**Norvège**
M^me^ Sigrun Johannesdottir Autorité de protection des données (Persónuvernd) Raudararstigur 10 – IS – 105 Reykjavik Tél : +354 510 9600 Fax : +354 510 9606 E-mail : postur@personuvernd.is Site web : http ://www.personuvernd.is	M. Georg Apenes Bureau de protection des données (Datatilsynet) P.O.Box 8177 Dep – NO – 0034 Oslo Tél : +47 22 396900 Fax : +47 22 422350 E-mail : postkasse@datatilsynet.no Site web : http ://www.datatilsynet.no
Liechtenstein	**République de Croatie**
M. Philipp Mittelberger Autorité de protection des données (Datenschutzbeauftragter Stabsstelle für Datenschutz – SDS) Kirchstrasse 8, Postfach 684 – LI -9490 Vaduz Tél : +423 236 6090 Fax : +423 236 6099 E-mail : info@sds.llv.li Site web : http ://www.sds.llv.li	M. Franjo Lacko Directeur Mme Sanja Vuk Chef du département des affaires juridiques Agence Croate de protection des données à caractère personnel (Agencija za zaštitu osobnih podataka – AZOP) Republike Austrije 25, 10000 Zagreb Tél. +385 1 4609 000 Fax +385 1 4609 099 E-mail : azop@azop.hr or info@azop.hr Site web : http ://www.azop.hr/default.asp
ancienne République yougoslave de Macédoine	
M^me^ Marijana Marusic Direction de protection des données à caractère personnel (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tél : +389 2 3244 760 Fax : +389 2 3244 766 Site web : www.dzlp.mk , info@dzlp.gov.mk	

Secrétariat du Groupe de travail « Article 29 »
M. Alain Brun Chef d'unité Unité de protection des données Direction générale Justice, Liberté et Securité Commission européenne Bureau : LX46 01/182 – BE – 1049 Brussels Tél : +32 2 296 53 81 Fax : +32 2 299 8094 E-mail : Alain.Brun@ec.europa.eu Site web : http ://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

NE-AC-09-001-FR-C
DOI 10.2758/52795

COMMISSION
EUROPEENNE

Le Groupe de travail a été créé en vertu de l'article 29 de la directive 95/46/CE. C'est l'organe consultatif de l'UE indépendant sur la Protection des données à caractère personnel. Ses tâches sont stipulées dans l'article 30 de la directive 95/46/CE et peuvent se résumer comme suit :

- Donner un avis d'expert des États membres à la Commission concernant les questions relatives à la protection des données.
- Promouvoir l'application uniforme des principes généraux de la directive dans tous les États membres au travers d'une coopération entre les autorités chargées du contrôle de la protection des données.
- Conseiller la Commission sur les mesures communautaires affectant les droits et les libertés des personnes physiques à l'égard du traitement des données à caractère personnel.
- Faire des recommandations au public dans son ensemble et en particulier aux institutions communautaires sur des questions relatives à la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté européenne.

ISBN 978-92-79-10364-3