12e rapport annuel

du groupe de travail «Article 29» sur la

protection des données

COMMISSION EUROPÉENNE

1830-6454

12e 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 2008

Adopté le 16 juin 2009

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

«La liberté appartient à ceux qui l'ont conquise.» André Malraux

Ce douzième rapport d'activité sur la protection des données dresse le bilan des avancées majeures réalisées au cours d'une année particulièrement riche en évènements et en défis. Il s'agit également du premier rapport que j'ai l'honneur de présenter en tant que président du groupe de travail «Article 29», succédant ainsi à mon honorable collègue et ami Peter Schaar.

Ce rapport est d'autant plus important qu'il se fait l'écho du travail remarquable accompli par les différentes délégations nationales au sein du groupe de travail «Article 29» en 2008. Il retrace en effet la synergie particulièrement efficace qui a permis l'adoption d'avis décisifs pour la protection des libertés individuelles.

Saisi de nouvelles problématiques complexes liées à l'extraordinaire développement des systèmes d'informations, notre groupe a su forger une doctrine, qui lui est propre, en opérant la synthèse des concepts que partagent les différentes autorités nationales de protection des données. Il a pu dépasser certaines divergences d'interprétation pour se concentrer sur la construction commune d'un socle de valeurs et de principes fondamentaux qui lui paraissent mériter une protection adaptée.

Quatre problématiques stratégiques ont plus particulièrement retenu notre attention au cours de l'exercice 2008.

La protection des données à caractère personnel de l'enfant constitue l'un des thèmes centraux de notre programme de travail. Cette préoccupation résulte principalement du développement des réseaux sociaux sur internet et des nouveaux comportements qu'ils induisent. La situation spécifique de l'enfant, sa vulnérabilité et sa condition d'être en devenir, exigeaient que notre groupe concentre ses efforts sur ces questions et dégage des solutions appropriées.

C'est désormais chose faite depuis l'adoption de l'avis WT147 de février 2008. Notre groupe a en effet présenté une synthèse structurée des préoccupations relatives à la protection des données à caractère personnel des enfants en s'attachant à définir les principes fondamentaux qui leur sont applicables et en précisant leur mise en œuvre pratique dans le contexte scolaire. Pour autant, le sujet n'est pas épuisé et d'autres développements suivront nécessairement. Dans l'immédiat, les progrès d'ores et déjà réalisés par notre groupe constituent un acquis commun essentiel pour nos travaux futurs.

Les moteurs de recherche constituent ensuite un autre thème de travail capital. Dans la société de l'information qui est la nôtre, les fournisseurs de moteurs de recherche sur internet font désormais partie du quotidien des internautes et jouent, à ce titre, un rôle d'intermédiaire déterminant dans le libre accès à l'information.
Toutefois, les volumes considérables de données d'utilisateurs qu'ils collectent, traitent et stockent chaque jour ont un impact non négligeable sur la protection des données à caractère personnel des usagers. Dès lors, une réflexion commune ainsi qu'un cadrage précis de ces pratiques s'imposaient.

Notre groupe est ainsi parvenu, dans son avis commun WT 158 d'avril 2008, à définir des règles instaurant un équilibre entre les intérêts légitimes en présence. Cet avis a été l'occasion de bâtir un cadre d'actions en direction des fournisseurs de moteurs de recherche dont les obligations sont désormais clairement définies. Il a également permis de rappeler les droits des utilisateurs en termes de droit d'accès ou de rectification.

L'avis ainsi adopté constitue un progrès déterminant pour le respect de la vie privée des usagers. Ceci est d'autant plus significatif que des fournisseurs de moteurs de recherche tels que Google ont d'ores et déjà mis en œuvre les préconisations qu'il contient.

Notre groupe a également poursuivi ses travaux s'agissant des transferts internationaux de données à caractère personnel à partir de l'Union européenne et à destination de filiales domiciliées dans le monde entier. Il s'est chargé d'optimiser la lisibilité des outils existants en proposant un cadre pour les règles d'entreprise contraignantes (BCR) destiné à faciliter leur application par les multinationales.

En matière d'information des passagers, enfin, dans le cadre du transfert des données des dossiers passagers aux autorités américaines (PNR), nous nous sommes également investis dans la conception de modèles de notes d'information adaptées aux réalités du secteur du transport aérien. L'objectif ainsi poursuivi était d'actualiser les dispositifs existants et de faciliter la tâche des agences de voyages, des compagnies aériennes ou de toutes les organisations fournissant des prestations de services de voyages aux passagers effectuant des vols à destination et au départ des État-Unis.

Ces différents axes de travail et les réponses qui ont été dégagées sont autant d'illustrations de notre engagement résolu au service de la protection des données à caractère personnel. La tendance actuelle à l'immixtion dans la vie privée des citoyens européens constitue une menace bien réelle qui exige des réponses claires et stables et la définition de limites intangibles.

Alex Türk

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/2008_fr.htm

1.1. TRANSFERT DE DONNÉES VERS LES PAYS TIERS

1.1.1. Dossiers Passagers (PNR)

Avis 2/2007 (WP 151) concernant l'information des passagers au sujet du transfert de données des dossiers passagers (Passenger Name Record – PNR) aux autorités américaines, Adopté le 15 février 2007 et révisé et mis à jour le 24 juin 2008

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 (WP97). L'accord de juillet 2007 constitue le cadre juridique existant pour le transfert des informations PNR aux autorités américaines. Les agences de voyages, les compagnies aériennes et les autres organisations conservent l'obligation de fournir des informations aux passagers concernant le traitement de leurs données à caractère personnel. Cet avis a donc pour but de donner des conseils et orientations quant aux questions suivantes: qui doit fournir quelle information? Comment? Et quand? Il convient de donner des informations aux passagers quand ces derniers décident d'acheter un billet d'avion et quand ils reçoivent confirmation de ce billet. 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. Les notes d'information courte et très courte donnent des informations sommaires aux passagers quant aux transferts de leurs données aux autorités américaines. Ces notes précisent également comment obtenir plus d'informations. La note plus longue prend la forme de questions fréquemment posées et contient plus de détails en ce qui concerne le traitement des données. Cette note fournit d'abord des informations au sujet des données relatives aux personnes transportées en général, avant de se concentrer sur les données concernant les passagers aériens (les PNR). Elle comprend également des liens vers l'accord actuel ainsi que vers d'autres documents pertinents.

1.1.2. Agence mondiale antidopage (AMA)

Avis 3/2008 (WP 156) sur le projet de norme internationale de protection de la vie privée du code mondial antidopage

La direction générale de l'éducation et de la culture (DG EAC) de la Commission européenne a sollicité l'avis du groupe de travail «Article 29» sur le projet de norme internationale de protection de la vie privée, élaboré par l'Agence mondiale antidopage (AMA). Le projet de norme doit être lu en parallèle avec le code mondial antidopage de l'AMA, et en particulier avec son article 14. Le code exige que les athlètes communiquent régulièrement certaines données aux organisations antidopage. Ces informations sont ensuite regroupées avec d'autres renseignements (y compris des données sensibles) dans la base ADAMS, située au Canada. Des données relatives à leur personnel d'encadrement et à d'autres catégories de personnes sont également traitées au titre des obligations prévues dans le code. Le WP29 a signalé les dispositions du code soulevant des questions de compatibilité avec les normes européennes de protection des données. En ce qui concerne les normes internationales d'AMA, le groupe de travail «Article 29» a abordé plusieurs questions traitant de la qualité du traitement des données appropriées, du consentement des sujets de données, des informations leur étant fournies, de la transmission de données personnelles à des tiers, des engagements de sécurité et droits des sujets de données.

1.1.3. Règles d'entreprise contraignantes (BCR)

Document de travail (WP153) établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes

Afin de faciliter l'application des règles d'entreprise contraignantes (BCR) par les groupes d'entreprises dans le cadre des transferts internationaux qu'ils effectuent de l'UE vers leurs filiales, le groupe de travail «Article 29» a élaboré un tableau dont l'objectif est:

- de préciser le contenu obligatoire des BCR tel qu'il est exposé dans deux documents distincts, à savoir le WP 74[2] et le WP 108[3],
- d'établir une distinction entre ce qui doit être inclus dans les BCR et ce qui doit être présenté aux autorités chargées de la protection des données dans le cadre d'une demande d'approbation des BCR (document WP 133[4]),
- pour chaque principe, d'indiquer des références aux documents WP 74[5] et WP 108[6] pour plus de détails, et
- de fournir des explications/commentaires sur chacun des principes.

Document de travail (WP 154) établissant un cadre pour la structure des règles d'entreprise contraignantes

Le groupe de travail a déjà établi que les transferts internationaux de données à caractère personnel à partir de l'UE effectués entre filiales d'un même groupe peuvent avoir lieu sur la base des règles d'entreprise contraignantes (BCR) et a fourni des orientations quant aux éléments indispensables de ces règles dans les documents WP74[7] et WP108[8].

Pour continuer à aider les groupes d'entreprises et à les guider dans l'élaboration de règles d'entreprise contraignantes, le groupe de travail a élaboré un document qui laisse entrevoir ce à quoi ces règles pourraient ressembler si elles intégraient tous les éléments indispensables décrits dans les documents WP 74[9] et WP 108[10].

Document de travail (WP 155) sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes

Comme expliqué dans le document de travail 74 (WP 74)[11], le groupe de travail «Article 29» estime que les règles d'entreprise contraignantes sont une solution convenant aux sociétés multinationales et autres groupes semblables, qui leur permet de remplir leurs obligations légales et de garantir un niveau adéquat de protection des informations à caractère personnel lors du transfert de données à l'extérieur de l'Union européenne. Le groupe de travail/les autorités de protection des données publient un ensemble de FAQ qui s'appuient sur leur expérience en matière de demandes d'approbation des règles d'entreprise contraignantes et de demandes d'information sur l'interprétation des documents WP 74[12] et WP 108[13]. Les FAQ ont pour but de clarifier certaines exigences particulières afin d'aider les demandeurs à obtenir l'approbation de leurs règles d'entreprise contraignantes. Ces FAQ ne sont pas exhaustives et seront mises à jour le cas échéant.

[2] Document de travail WP 74: Transferts de données personnelles vers des pays tiers: Application de l'article 26 (2) de la directive de l'UE relative à la protection des donnés aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, adopté le 3 juin 2003 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_fr.htm

[3] Document de travail WP 108 établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes, adopté le 14 avril 2005. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_fr.htm

[4] Document de travail WP 133: Recommandation 1/2007 relative au formulaire de demande d'approbation des règles d'entreprise contraignantes applicables au transfert des données à caractère personnel http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_fr.htm

[5] Voir note de bas de page 2.

[6] Voir note de bas de page 3.

[7] Voir note de bas de page 2.

[8] Voir note de bas de page 3.

[9] Voir note de bas de page 2.

[10] Voir note de bas de page 3.

[11] Voir note de bas de page 2.

[12] Voir note de bas de page 2.

[13] Voir note de bas de page 3.

1.2. COMMUNICATIONS ÉLECTRONIQUES INTERNET ET NOUVELLES TECHNOLOGIES

Avis 1/2008 (WP 148) sur les aspects de la protection des données liés aux moteurs de recherche

Les moteurs de recherche font désormais partie de la vie quotidienne des personnes utilisant l'internet et les technologies de recherche d'informations. Dans le présent avis, le groupe de travail «Article 29» reconnaît l'utilité de ces moteurs de recherche et il est conscient de leur importance et dresse une liste précise des responsabilités qui, en vertu de la directive sur la protection des données (95/46/CE), incombent aux fournisseurs de moteurs de recherche en qualité de responsables du traitement de données d'utilisateur. Du fait de leur rôle de fournisseurs de données de contenu (en l'occurrence, l'index des résultats de recherche), les moteurs de recherche sont eux aussi soumis à la législation européenne en matière de protection des données dans des cas bien particuliers, par exemple s'ils proposent un service de stockage dans une mémoire cache, ou s'ils sont spécialisés dans l'établissement de profils de personnes. Le principal objectif poursuivi dans le présent avis est de parvenir à un équilibre entre les besoins légitimes des fournisseurs de moteurs de recherche dans l'exercice de leur activité et la protection des données à caractère personnel des internautes. L'avis aborde la définition des moteurs de recherche, les types de données traitées dans le cadre des services de recherche, le cadre juridique, les finalités/raisons d'un traitement légitime, l'obligation d'informer les personnes concernées, et les droits de ces personnes.

L'une des principales conclusions de l'avis est que la directive sur la protection des données s'applique généralement au traitement des données à caractère personnel par les moteurs de recherche, même lorsque le siège de ces derniers se trouve en dehors de l'EEE, et qu'il incombe aux fournisseurs de moteurs de recherche qui se trouvent dans cette situation de clarifier leur rôle dans l'EEE ainsi que l'étendue de leurs responsabilités en vertu de la directive. Il ressort clairement que la directive sur la conservation des données (2006/24/CE) ne s'applique pas aux fournisseurs de moteurs de recherche. L'avis conclut que les données à caractère personnel ne doivent être traitées qu'à des fins légitimes. Les fournisseurs de moteurs de recherche ont l'obligation de supprimer ou de rendre les données à caractère personnel totalement anonymes dès qu'elles ne servent plus les finalités déterminées et légitimes pour lesquelles elles ont été collectées, et ils doivent à tout moment être en mesure de justifier le stockage et la durée de vie des «cookies» envoyés. Le consentement de l'utilisateur est requis pour tout projet de recoupement entre données relatives à l'utilisateur et d'enrichissement du profil de ce dernier. Les moteurs de recherche doivent respecter les demandes d'exclusion d'indexation formulées par les éditeurs de sites internet et répondre immédiatement aux demandes des utilisateurs concernant l'actualisation/le rafraîchissement des mémoires caches. Le groupe de travail rappelle que les moteurs de recherche sont tenus d'informer clairement les utilisateurs à l'avance de toutes les utilisations prévues de leurs données, et de respecter leur droit de consulter, de vérifier ou de corriger aisément ces données personnelles conformément à l'article 12 de la directive sur la protection des données (95/46/CE).

Avis 2/2008 (WP 150) sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»)

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. Le principal objectif de la 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. Le groupe de travail «Article 29» a commenté sur la proposition et a abordé certaines questions supplémentaires, au sujet, principalement, de la notification des violations de la sécurité, le concept des «données personnelles»; les concepts du «réseau de communications publiques» et des «services de communications électroniques»,

les autorités réglementaires nationales (NRAs) et les communications non sollicitées.

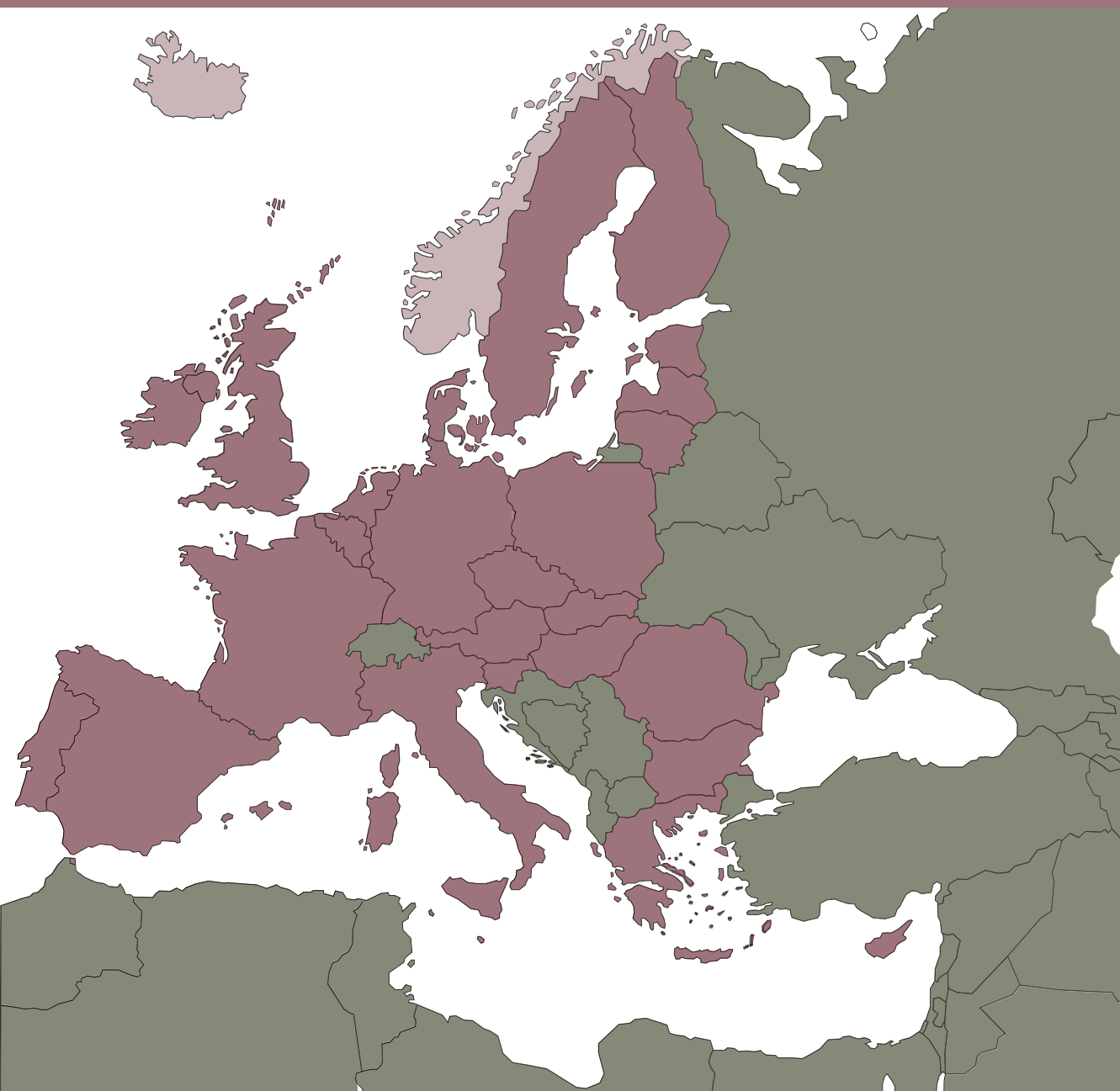
1.3. DONNÉES À CARACTÈRE PERSONNEL

Document de travail 1/2008 (WP147) sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles)

Le présent avis porte sur la protection des informations concernant les enfants. Il est essentiellement destiné aux personnes qui gèrent les données à caractère personnel des enfants. Dans les écoles, il s'agit plus particulièrement des enseignants et des autorités scolaires. Il s'adresse également aux autorités nationales de contrôle de la protection des données, qui sont chargées de surveiller le traitement de ce type de données.

Le groupe de travail «Article 29», qui a déjà adopté plusieurs avis relatifs à cette question. Ses avis sur le code de conduite «FEDMA» (avis 3/2003), sur l'utilisation des données de localisation (avis 5/2005) et sur les visas et les éléments d'identification biométrique (avis 3/2007) contiennent certains principes ou recommandations concernant la protection des données relatives aux enfants. Le présent document a pour objectif de synthétiser cette question de manière structurée, en définissant les principes fondamentaux applicables et en les illustrant par des références aux données scolaires. Le domaine des données scolaires a été sélectionné car c'est l'un des plus importants secteurs de la vie des enfants et il représente une part significative de leurs activités quotidiennes. Son importance tient également au caractère sensible de la plupart des données traitées dans les établissements scolaires.

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 loi autrichienne sur la protection des données de 2000 («Datenschutzgesetz 2000») devait être amendée en 2008. Un avant-projet à cet effet avait été distribué au début de l'année, et des observations avaient été formulées[14]. Toutefois, les élections législatives de l'automne 2008 ont mis un terme au processus législatif, qui n'a pas encore été relancé. L'avant-projet traitait notamment des questions suivantes:

- Les dispositions de l'actuelle Datenschutzgesetz 2000 eu égard aux personnes morales ou aux groupes de personnes physiques en tant que personnes concernées. L'avant-projet entendait limiter cette protection aux personnes physiques. Cette proposition a recueilli des réactions mitigées; le barreau autrichien a ainsi fait remarquer que de nombreuses entreprises avaient autant besoin du droit de consulter, de rectifier et d'effacer leurs données que les personnes physiques pour protéger leurs intérêts, et qu'aucune autre loi ne leur octroyait un tel droit.
- L'avant-projet contient des dispositions relatives à la désignation d'un responsable de la protection des données dans les (grandes) entreprises.
- Il prévoit en outre d'importants changements en matière de notification: dorénavant, toutes les notifications devront se faire en ligne à l'aide d'un nouveau système exclusivement électronique. Par ailleurs, dans l'intérêt d'accélérer la procédure, le contrôle matériel des notifications se limitera à des contrôles *ex ante*.
- Une toute nouvelle réglementation aurait dû régler la question de la **vidéosurveillance**. La commission pour la protection des données a reçu tellement de plaintes et de notifications à ce sujet qu'une réglementation plus détaillée de la vidéosurveillance (et surtout de la vidéosurveillance mise en place par des personnes ou groupements privés) semble nécessaire.

La **directive 2006/24/CE sur la conservation des données** n'avait pas été mise en œuvre en 2008. De nouveaux efforts dans ce sens ont été amorcés après la décision de la CE concernant sa base juridique.

[14] L'avant-projet lui-même, de même que tous les commentaires à son endroit, peuvent être consultés sur le site du Parlement autrichien: http://www.parlament.gv.at/PG/DE/XXIII/ME/ME_00182/pmh.shtml

B. Jurisprudence

La première affaire de «**dénonciation des dysfonctionnements**» a été tranchée à la fin de l'année 2008. La commission pour la protection des données a considéré, après de longs débats, que la filiale autrichienne d'une entreprise était responsable, via un système d'alerte éthique, des données transférées à sa société mère américaine. Son avis était motivé comme suit:

Les collaborateurs de la filiale autrichienne ont reçu de leur employeur, par l'entremise de leur contrat de travail, l'instruction de suivre un code de conduite spécifique (celui-ci étant contraignant pour l'ensemble du personnel de toutes les entreprises du groupe). Celui-ci prévoit, entre autres obligations, le devoir de signaler certaines situations contraires à l'éthique, voire illégales, dont ils auraient connaissance et fait mention, parmi les moyens de dénoncer lesdites situations, d'une ligne d'assistance téléphonique. Par conséquent, tout collaborateur ayant recours à cette ligne ne fait que suivre les instructions générales données par son employeur. Il agit donc en tant que membre du personnel de la filiale autrichienne et non en tant que personne privée. Les transferts de données effectués par des collaborateurs doivent relever de la responsabilité de l'employeur, surtout s'ils sont mandatés par celui-ci (affaire K178.274/0010-DSK/2008).

Pour la jurisprudence sur la vidéosurveillance, voir la section «Questions diverses importantes».

C. Questions diverses importantes

Vidéosurveillance

La vidéosurveillance s'est révélée être l'un des principaux sujets de préoccupation, tant en nombre de plaintes que de notifications.

Une décision rendue dans le domaine du droit d'accès aux fichiers de vidéosurveillance qui n'a pas été exploitée pourrait être d'intérêt général.

Un citoyen a exigé de pouvoir accéder à un fichier vidéo appartenant à une société de transport public. Dans

le système de cette société, les données vidéo sont supprimées après 48 heures, à moins d'une agression ou d'actes de vandalisme. Le citoyen a été débouté par le responsable du traitement des données (société de transport).

La plainte de la personne concernée à la commission pour la protection des données a été rejetée pour les raisons suivantes: pour pouvoir lui octroyer un accès aux données en question, il aurait été nécessaire d'examiner des enregistrements qui, sinon, auraient été supprimés après 48 heures sans avoir été visionnés. Par ailleurs, l'enquête nécessaire pour déterminer si l'image du plaignant figurait parmi les données de surveillance aurait révélé des données sur toutes les autres personnes figurant dans ce fichier, données qui, sans cela, seraient restées secrètes et auraient été effacées après 48 heures.

Compte tenu du fait qu'en Autriche, les fichiers de vidéosurveillance ne peuvent être exploités que si un événement prévu par la législation a effectivement eu lieu (p. ex. un acte de vandalisme), il a été décidé qu'aucun accès à des fichiers non exploités ne serait accordé si les données du fichier étaient appelées à être supprimées après un délai de conservation très court (p. ex. 48 heures) et s'il y avait une forte probabilité pour que d'autres personnes soient visibles dans le fichier, de sorte que permettre la consultation de celui-ci violerait les droits à la protection des données de nombreuses autres personnes (affaire K121.385/0007-DSK).

Deux cas de notification avaient trait à la vidéosurveillance dans les écoles. La commission pour la protection des données n'a pas autorisé la vidéosurveillance pour maintenir l'ordre à l'intérieur des bâtiments scolaires (ceci relevant de la mission pédagogique du personnel enseignant) mais a permis l'utilisation de caméras vidéo dans certains espaces extérieurs, de manière à protéger les biens, et notamment à prévenir les vols de bicyclettes (affaires K600.054-001/0002-DVR/2008 et K600.055-001/0002-DVR/2008).

Évaluation de la solvabilité
Les plaintes à l'encontre des agences de notation restent en tête des préoccupations de la commission pour la protection des données.

Assurance santé privée
La commission autrichienne pour la protection des données a lancé un audit sur le secteur de l'assurance santé privée en 2008. Les recommandations requises seront bientôt adoptées.

Belgique

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

Aucun développement significatif ne nous paraît devoir ici être mentionné.

B. Jurisprudence

Aucune décision particulièrement importante rendue par les cours et tribunaux ne nous parait devoir ici être mentionnée à l'exception de la position exprimée par le Conseil d'État selon laquelle: en application de l'article 7 § 3 de la *Loi Vie privée* (Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)[15], tout projet d'arrêté royal portant sur un traitement de données relatives à la santé doit être délibéré en Conseil des ministres et soumis à l'avis de la Commission de la protection de la vie privée (ci-après la Commission ou la CPVP) (Comité sectoriel de la sécurité sociale et de la santé - Avis 09/2008 du 27 février 2008).

C. Questions diverses importantes[16]

Traitement de données sensibles

Données relatives à la santé - Plateforme e-health (Comité sectoriel de la sécurité sociale et de la santé - Avis 14/2008)

Il a été créé au sein de la Banque – carrefour de la sécurité sociale, une nouvelle institution publique dotée de la personnalité juridique dénommée «Plateforme e-health». Cette plateforme a pour but premier d'offrir une infrastructure et des services de base pour l'échange sécurisé de données relatives à la santé entre les différents acteurs du secteur de la santé, et à servir d'organisation intermédiaire chargée de la collecte et du codage de données destinées à la recherche historique, statistique et scientifique. Le numéro de Registre national (identifiant unique) et le numéro d'identification de la sécurité sociale (dérivé du premier) serviront d'identifiants au sein de cette plateforme. Celle-ci conservera par ailleurs un répertoire des références reprenant, pour les patients qui y consentent, chez quels acteurs de la santé quels types de données à caractère personnel les concernant sont reprises. Ce répertoire sert à canaliser les demandes de données vers l'endroit où ces dernières sont disponibles et à assurer un contrôle préventif effectif.

La Commission a estimé qu'une telle plateforme décentralisée qui se limite à véhiculer des données à caractère personnel mais n'en conserve aucune (à l'exception néanmoins de celles qui sont contenues dans le répertoire de références) va dans le sens d'un respect satisfaisant de la vie privée des patients et répond aux recommandations du groupe 29 *(Document de travail 131 sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques).*

Quant à l'utilisation du numéro de registre national comme identifiant au sein de la plateforme, la Commission a rappelé sa jurisprudence générale qui tend à promouvoir l'usage d'identifiants sectoriels. Elle ne s'est toutefois pas opposée à son utilisation en l'espèce. Nous aborderons plus loin d'autres questions liées à l'utilisation du numéro de registre national, lequel, s'il n'est pas formellement considéré comme une donnée sensible, n'en requiert pas moins des garanties lors de son utilisation (article 8 § 7 de la directive 95/46/CE).

Données relatives à des personnes condamnées (Avis 28/2008)

Le ministre de la justice recevant de plus en plus de questions portant sur des personnes condamnées dans le cadre de l'exercice du contrôle parlementaire et par la presse, il a interrogé la Commission de la protection de la vie privée sur la délicate question du rapport entre la protection de la vie privée et le droit à l'information. Le droit à l'information implique pour tout parlementaire le droit de poser des questions écrites ou orales au ministre. Conformément au règlement du Parlement, les questions concernant un cas personnel sont en principe irrecevables. De l'avis de la Commission, le ministre pourrait donc invoquer ces dispositions pour refuser de répondre à une question sur des données relatives

[15] «Le Roi détermine, par arrêté délibéré en conseil des ministres et après avis de la Commission de la protection de la vie privée, des conditions particulières auxquelles doit satisfaire le traitement de données à caractère personnel».

[16] Tous les avis, recommandations, autorisations et autres documents cités dans la présente contribution sont disponibles sur le site de la Commission de la protection de la vie privée à l'adresse: http://www.privacycommission.be

à une personne condamnée au pénal mais il pourrait également choisir d'invoquer le droit constitutionnel à l'information pour répondre à l'auteur de la question. Conformément à la *Loi Vie privée*, une interdiction de principe interdit le traitement des données judiciaires mais une exception est prévue pour les traitements qui se font sous la surveillance d'une autorité publique si ce traitement s'avère *nécessaire* pour l'exercice de ses tâches. De l'avis de la Commission, cette exception s'applique au traitement de données judiciaires par le ministre. L'évaluation du caractère nécessaire de ce traitement sera fonction des circonstances et la Commission indique ne pouvoir se prononcer de manière générale sur ce point. L'interdiction de traitement des données judiciaires ne s'applique pas non plus aux traitements de données à caractère personnel destinées à des finalités exclusivement journalistiques lorsque ce traitement concerne des données rendues notoirement publiques par la personne concernée ou en étroite corrélation avec le caractère public de celle-ci ou du fait dans lequel cette dernière est impliquée. Ici aussi la Commission conclut que tout dépendra des circonstances et elle se limite à formuler quelques lignes directrices. Elle fait également référence à la disposition constitutionnelle qui stipule qu'un jugement est prononcé en audience publique. Pour autant qu'elle ait été présente au prononcé, la presse a pu en prendre connaissance. À cet égard, la Commission estime que c'est à la magistrature qu'il revient d'abord de communiquer la teneur d'un jugement, et ce, par le biais du magistrat de presse. Enfin, la Commission précise que lorsqu'un cas personnel fait référence à une question d'ordre plutôt légistique, stratégique ou structurel, le ministre peut communiquer des données pour permettre une meilleure compréhension du problème. Il lui reviendra cependant toujours de déterminer au cas par cas si une question dépasse ou non le cadre individuel. Lorsque ce n'est pas le cas, la Commission est d'avis qu'une certaine réserve est de rigueur.

Traitement de données sensibles et mise en œuvre d'une politique antidiscrimination (Avis 05/2008)

En exécution de sa politique en matière d'égalité des chances et de diversité, l'Office flamand de l'emploi et de la formation professionnelle voulait se faire une idée de la présence tant des personnes d'origine allochtone que des personnes soufrant d'un handicap dans son fichier du personnel. À quelles conditions un monitoring de ces catégories de personnes pouvait-il être mis en place conformément à la loi belge de protection de la vie privée? La Commission a conclu que les données relatives à la diversité étaient suffisamment transparentes et proportionnelles et qu'elles étaient traitées sur une base volontaire. Les finalités du traitement sont légitimes, basées entre autres, sur les droits et obligations fixées dans un texte légal relatif à la participation proportionnelle sur le marché de l'emploi. La Commission a néanmoins constaté une série d'imperfections dont elle a exigé qu'elles soient corrigées au plus tard au moment de l'opérationnalisation du système de monitoring :

- les membres du personnel doivent pouvoir retirer leur consentement ou leur refus; ce changement ne peut être archivé dans le système de manière permanente;
- la période de mise en œuvre du système d'auto-enregistrement est mal choisie car elle coïncide avec la période d'évaluation du personnel, ce qui peut donner l'impression aux membres du personnel appartenant aux groupes concernés qu'ils sont mis sous pression pour communiquer leurs données;
- étant donné que la politique d'égalité des chances et de diversité n'est pas axée sur certaines nationalités spécifiques, la Commission estime que le fait de demander d'emblée la nationalité du (des) grand(s)-parent(s) du membre du personnel est excessif;
- aucun monitoring des membres du personnel sur la base de leur nationalité ne peut être mis en place si ces personnes ne se sont pas volontairement fait enregistrer en tant que telles pour les finalités de monitoring de ce projet.

La Commission souligne enfin que les données traitées sont des données sensibles. Elle recommande de faire contrôler l'ensemble du projet par un conseiller en sécurité de l'information notamment chargé des missions d'un préposé à la protection des données (détaché à la protection des données au sens de la directive).

Traitement de données sensibles et étude antidiscrimination

À l'occasion d'une recommandation (02/2008) adressée à une société publique de logement désireuse de mener une étude sociologique sur les (candidats) locataires, la Commission a indiqué que les données «lieu de naissance» et «nationalité» ne lui apparaissaient pas

d'évidence comme des données sensibles. Leur collecte n'en doit pas moins demeurer pertinente. L'auteur de l'étude invoquait à cet égard un objectif de *mixité sociale et de lutte contre les discriminations dans le secteur du logement*. En réponse à cet argument, la Commission a relevé que conformément à la législation en matière de lutte contre les discriminations, la distinction fondée sur un des motifs admis de discrimination ne constitue pas une discrimination lorsqu'elle est objectivement justifiée par un but légitime et que les moyens de réaliser ce but sont appropriés et nécessaires. Aussi, la détermination précise de la ou des finalités et des critères d'attribution revêt-elle toute son importance dès lors que des données potentiellement sensibles ou discriminatoires seraient traitées. La Commission a recommandé que les textes applicables à l'auteur de la demande prévoient une meilleure détermination des finalités (lutte contre la discrimination) et des données traitées. Invoquer de manière générale l'obligation non-discrimination ne peuvent constituer un fondement suffisant.

Dans le même avis, la Commission précise que l'examen de la compatibilité d'un traitement ultérieur par un responsable de traitement relevant du secteur public doit s'appuyer sur des dispositions légales et réglementaires qui décrivent suffisamment le traitement ultérieur et le type de données qui peuvent être traitées, leur origine et les finalités du traitement. L'adoption d'une disposition décrétale ou réglementaire *ad hoc* pourrait ainsi permettre de considérer qu'un tel traitement ultérieur n'est pas incompatible avec traitement initial. À défaut, l'ensemble des conditions fixées en cette matière par l'arrêté royal d'exécution (13 février 2001) de la *Loi Vie privée* sont d'application.

En 2008, la Commission a par ailleurs pris plusieurs initiatives au regard des traitements de données intervenant dans le contexte de la recherche. Certaines d'entre-elles sont décrites ci-dessous.

Recherche historique, statistique et scientifique
Vade-mecum du chercheur
En 2008, la Commission a par exemple édité un *Vade-mecum* du chercheur. Dans cette publication, elle informe le secteur de la recherche des règles et des procédures à suivre lors de la collecte et l'analyse de données à caractère personnel à l'occasion d'une recherche. La Commission distingue 4 étapes pour lesquelles elle identifie un certain de nombre de questions et formule des recommandations: avant le début de la recherche (principes régissant l'utilisation de données secondaires, la collecte de données sensibles), lors de la collecte de données (information lors du premier contact, le refus de participer et la suppression des données d'identification des personnes qui optent pour ce refus, la collecte proprement dite et les droits d'accès, de rectification et de suppression), pendant l'analyse et la publication (anonymisation la plus poussée et la plus rapide possible, la sensibilisation des collaborateurs, les publications) et après la recherche. Enfin, le *Vade-mecum* intègre également un Code de conduite (voir ci-dessous) que les destinataires de données du Registre national s'engagent à respecter lors de l'exécution de leur mission de recherche scientifique.

Code de conduite pour les chercheurs recourant au Registre national (Avis 27/2008)
Les procédures strictes en matière de protection de la vie privée mises en place par la Commission ces dernières années inquiétaient les chercheurs. La lourdeur des conditions d'accès au registre national leur faisait craindre de ne plus pouvoir faire de la recherche scientifique responsable. La Commission a pris cette crainte à cœur et a mené une réflexion tant interne qu'avec le secteur de la recherche scientifique sur cette problématique.
Dans le cadre de la réalisation d'une recherche scientifique basée sur un échantillon de la population et poursuivant une finalité d'intérêt général, toute institution de droit belge est en droit d'obtenir la communication de données d'identification du Registre national après autorisation du Comité sectoriel compétent. L'enquête écrite constitue la règle, l'enquête orale (en présence donc de la personne) l'exception. Si le chercheur ne peut ou ne souhaite pas travailler au moyen d'un questionnaire écrit, il doit en faire la demande et motiver son choix auprès du Comité sectoriel du Registre national. S'il s'agit de questionnaires écrits destinés à une enquête unique, le Registre national se charge lui-même de l'envoi des questionnaires accompagnés d'une lettre d'introduction et des documents fournis par l'institution de recherche. Les envois ultérieurs peuvent également se faire en suivant la même procédure. Dans ce cas, le Registre national ne transmet à l'organisme de recherche que les informations nécessaires pour lui permettre d'effectuer

une analyse des refus de répondre et ceci sous forme codée exclusivement. S'il s'agit d'enquêtes orales dans le cadre desquelles des données d'identification s'avèrent nécessaires, le Registre national transmet les données pertinentes à l'organisme de recherche à condition que celui-ci s'engage à respecter ce qui suit:

- la personne concernée ne peut être sollicitée plus qu'elle ne le souhaite;
- l'institution de recherche doit adopter un comportement correct et professionnel;
- les données d'identification doivent faire l'objet d'une protection particulière, éventuellement par le biais d'un recours à un tiers de confiance;
- les rapports et publications réalisés sur la base des données de recherche obtenues à l'aide de données du Registre national ne peuvent contenir que des données anonymes.

Réutilisation de données administratives à des fins de recherche – tiers de confiance (Avis 20/2008)

A l'occasion d'une demande d'avis portant sur la réutilisation de données issues de bases de données administratives d'universités dans le but de suivre la mobilité intersectorielle et internationale des chercheurs ainsi que l'influence d'un doctorat sur le marché du travail, la Commission a demandé la mise en place d'un *tiers de confiance* chargé du couplage des données. Cette exigence vise à garantir une étanchéité certaine entre d'une part l'entité au sein de laquelle les données administratives sont rassemblées et couplées et d'autre part, l'institution de recherche qui ne recevra que des données anonymisées destinées à l'étude scientifique et statistique. Dans l'intervalle, la cellule interne chargée du couplage devra répondre aux exigences suivantes:

- un contrôle externe du processus de couplage interne doit être organisé;
- la gestion de la cellule interne doit être assurée par un organe dans lequel sont représentées les différentes catégories de personnes dont les données sont traitées;
- la cellule de couplage doit, conformément à la loi vie privée et son arrêté royal d'exécution, être considérée comme un responsable de traitement autonome (et non comme un sous-traitant des différents fournisseurs de données); elle endosse une responsabilité propre de ce fait;
- la cellule de couplage doit anonymiser les données pour que la cellule de recherche ne puisse pas, elle-même, établir de lien entre les informations obtenues et une personne physique identifiée ou identifiable.

Dans le dossier relatif à la plateforme e-health déjà mentionné, la Commission avait, dans le même sens, également indiqué que le rôle d'e-health comme organisation intermédiaire correspondait à ses vœux de faire assurer le codage en vue de la recherche historique, statistique ou scientifique par un tiers indépendant et neutre. La Commission insiste sur la nécessité que cette organisation intermédiaire n'effectue aucune recherche elle-même.

Secteur privé – activités commerciales et financières

SWIFT

Par une décision du 8 décembre 2008, la Commission a mis un terme à la procédure de recommandation initiée à l'encontre de la société SWIFT (voir également les rapports annuels 2007 et 2006). Plusieurs éléments qui ont caractérisé le déroulement des procédures et plusieurs éléments de la décision rendue par la Commission méritent d'être soulignés:

SWIFT a collaboré loyalement et sans réserve à l'établissement des faits, permettant à la Commission d'accéder à toutes les informations et tous les documents utile. La Commission a dès lors pu déterminer avec précision les responsables respectifs de différentes opérations bien identifiées (l'indétermination qui régnait jusqu'ici était principalement due à la complexité et à la méconnaissance du système). Les banques, la communauté financière, SWIFT, chacun a désormais des obligations précises à exécuter - en qualité de responsable de traitement - pour garantir la protection des données personnelles qui accompagnent l'exécution de transactions financières.

SWIFT a accepté de reconnaître et d'assumer des responsabilités bien circonscrites. Elle les a déclarées d'initiative au registre public tenu par la Commission, se conformant ainsi aux obligations légales qui imposent la transparence en matière de traitement de données personnelles.

La Commission a par ailleurs constaté qu'en réponse aux accusations dont elle a fait l'objet, SWIFT a adopté une série de mesures destinées à mieux prévenir certains

risques et à améliorer la protection des données personnelles qu'elle traite: nouvelle architecture du réseau international et implantation d'un centre de traitement en Suisse pour gérer les messages intra-européens (qui ne seront plus transférés aux USA); désignation à temps plein d'un «Privacy Officer» au sein de la société, doté de compétences et de missions déterminées; formalisation de procédures d'encadrement, d'orientation et de suivi des demandes adressées par les personnes dont les données sont traitées; instauration d'un groupe de travail permanent «data protection», chargé d'évaluer et d'adapter les mesures de protection existantes; développement d'une politique d'information accessible,…

Marketing direct

En juin 2008, la Commission a pris l'initiative de publier une note juridique sur la problématique du marketing direct. Pour une meilleure protection de la vie privée dans le cadre des traitements à des fins de marketing direct, la Commission met en exergue les points suivants:

- il est indispensable de faire une meilleure distinction entre le marketing direct sur une base (pré)contractuelle - marketing direct utilisé dans le cadre d'une gestion normale de la clientèle - et les autres formes de marketing direct à propos desquelles la Commission reçoit de nombreuses plaintes;
- l'intérêt légitime du responsable de traitement [article 5 f) de la LVP – article 7 f) de la directive 95/46/CE - dont les conditions d'invocation sont précisées] – ne doit être considéré que comme un fondement résiduaire après les articles 5 a) et 5 b) de la LVP [articles 7 a) et b) de la directive 95/46/CE];
- le consentement est posé comme une condition dans le cadre du courtage d'adresses et du profilage à des fins de marketing direct, pour les traitements qui ne sont pas a priori légitimés par un contact direct avec la personne concernée;
- la notion de (non-)respect du principe de loyauté a été expliquée à l'aide d'exemples concrets;
- la notion «utilisation incompatible» a été précisée de même que l'exigence d'un délai de conservation;
- sur la base du principe de loyauté, la Commission préconise l'obligation de déclaration proactive au niveau de la source d'une action de marketing direct lorsqu'il n'y a pas de contact direct avec la personne concernée (par exemple en cas de commerce de données). La Commission invite à la prudence en cas d'utilisation de clauses d'information standard et insiste sur le fait que ces informations doivent être les plus claires et compréhensibles possible.

Cette note fait actuellement l'objet d'une concertation avec le secteur et pourrait, en fonction des remarques reçues dans le cadre de celle-ci, être amendée à l'avenir.

Listes négatives

Comme les années précédentes, la question des listes noires a été au cœur des préoccupations de la Commission belge. L'avis 34/2008 concernant une proposition de loi relative à l'encadrement des listes négatives fait la synthèse du point de vue constant de la Commission au fil de 9 avis depuis 1998:

- les listes négatives constituent des ingérences dans la vie privée contraires à l'article 8 de la Convention européenne des droits de l'homme;
- seul le législateur dispose de la compétence «d'autoriser» de telles listes; la Commission invite dès lors le législateur à encadrer les listes négatives non réglementées existantes;
- les éléments essentiels d'éventuelles listes négatives doivent être fixés par la loi. Il s'agit surtout de la définition de la finalité, des conditions d'enregistrement, des situations et des conditions dans lesquelles le responsable de traitement peut valablement légitimer son traitement en vertu de l'article 5 f) de la LVP [article 7 f) de la directive 95/46/CE], de la nature des données, du délai de conservation et de la diffusion et de l'accès aux données;
- les finalités des listes négatives doivent être clairement formulées; les finalités «lutte contre la fraude» ou «protection de la sécurité» ne sont pas suffisamment précises;
- une obligation de déclaration des listes négatives pour lutter contre la discrimination;
- un système d'autorisation unique et de déclaration de conformité reposant sur une base légale comme c'est déjà largement le cas en France;
- l'introduction d'une garantie de réciprocité au niveau de l'échange des données à caractère personnel avec les autres pays de l'Union européenne qui appliquent des régimes plus stricts, notamment les listes négatives multisectorielles ou les listes sectorielles «zero tolérance».

Vie privée et droit de propriété
En 2008, la Commission a régulièrement été consultée quant à l'application de la *Loi Vie privée* dans le domaine de la copropriété forcée d'immeubles bâtis. Ces questions émanaient tantôt des syndics d'immeubles (qu'ils soient professionnels ou non) tantôt des copropriétaires eux-mêmes. Dans un avis 22/2008, la Commission a estimé que l'association des copropriétaires doit être considérée comme le responsable des différents traitements réalisés par le syndic, son mandataire, dans le cadre ou à l'occasion de la gestion de la copropriété. L'avis conclut également à la légalité de certains traitements spécifiques tels la communication par le syndic aux copropriétaires des noms et adresses d'autres copropriétaires ainsi que la communication à l'ensemble des copropriétaires du compte (répartition des dépenses et charges) de chaque copropriétaire individuel. Enfin, la Commission de la protection de la vie privée a encouragé l'adoption d'éventuels codes de conduite professionnels ou sectoriels.

Questions d'identification
La Belgique a, de longue date, opté pour un identifiant unique, le numéro de registre national, dont l'accès et l'utilisation son strictement réglementés. Un comité (le comité sectoriel du Registre national) pour partie composé de membres de la Commission est chargé d'autoriser cet accès et son utilisation moyennant le respect de garanties strictes.

Gestion des utilisateurs et des accès (Recommandation 01/2008)
En 2008, le Comité du registre national a reçu plusieurs demandes d'autorisation d'utilisation du numéro de registre national à des fins de gestion des accès des utilisateurs. S'agissant d'une problématique générale, le dossier a été évoqué auprès de la Commission. Celle-ci a émis une recommandation générale qui contient plusieurs règles pratiques en matière de gestion de ces accès dans le secteur public:

- il est souhaitable de développer un système basé sur le principe des cercles de confiance;
- il faut prévoir un enregistrement de qualité lequel implique le contrôle de l'identité de l'utilisateur qui se connecte, de ses caractéristiques et de ses mandats à l'appui de sources authentiques validées (lesquelles offrent des garanties quant à l'exactitude des données);
- l'authentification électronique de l'identité doit se faire, de préférence, au moyen de la carte d'identité électronique;
- la gestion des accès inclut l'enregistrement et la vérification des autorisations.

Modalité d'accès au registre national
Une loi de 2008 confie aux établissements bancaires et compagnies d'assurance la mission de rechercher les titulaires de comptes et coffres dormants ainsi que les titulaires de contrats d'assurance dormants. Afin de rechercher et de contacter ces titulaires, la consultation de registres tels que le Registre national est autorisée. Dans un avis 31/2008, la Commission a fait part de sa satisfaction au sujet de la configuration prévue pour les accès aux registres dans la mesure où ceux-ci ne sont pas directement mis à disposition des banques. Un *point central est chargé de rassembler les requêtes d'accès motivées* des banques et compagnies d'assurance et d'adresser ensuite une réponse à celles-ci. Ce type de configuration (accès au Registre national pour un secteur déterminé via un point central assurant un contrôle des accès sur le secteur) rend possible une prévention contre tout accès illégitime aux données des registres concernés et contre tout détournement de finalité de la part des établissements bancaires et d'assurances.

Utilisation de la carte d'identité électronique (Recommandation Comité sectoriel du Registre national 02/2008)
Le Comité du Registre national a été amené à répondre à une série de questions relatives à l'utilisation de la carte d'identité électronique (eID). Si la Commission relève que l'eID représente l'instrument d'identification idéal, elle rappelle les conditions légales dans lesquelles sa présentation peut être exigée. Ces conditions de présentation excluent l'utilisation obligatoire de l'eID en tant que carte de bibliothèque. Le citoyen reste par contre libre de choisir d'utiliser sa carte eID comme carte de bibliothèque mais cette modalité ne peut lui être imposée. Aucun avantage dont ne pourrait bénéficier le titulaire d'une carte de bibliothèque distincte ne peut être lié à l'utilisation de l'eID en tant que carte de bibliothèque.

Secteur public
Fichier central des véhicules
Depuis 2006, la Commission a émis plusieurs avis (négatifs) relatifs à la création d'une source authentique de données

relatives aux véhicules. Dans un avis 23/2008, elle rappelle que son responsable de traitement doit être clairement identifié et qu'un stockage centralisé et une journalisation soumis à un contrôle fédéral externe semble être l'option qui offre le plus de garanties en matière de protection des données à caractère personnel. La Commission a également rappelé que le Comité sectoriel pour l'Autorité fédérale[17] doit accorder une autorisation pour les flux de données électroniques au départ de l'institution fédérale (DIV - Direction véhicules) qui abritera cette base de données. À cet égard, la Commission ne s'est pas montrée partisane de la création d'un nouveau comité sectoriel «Mobilité et transport» mais a plutôt conseillé de viser la plus grande cohérence possible avec les comités sectoriels existants.

Dans l'intervalle, à défaut de base légale suffisante, la communication de données à caractère personnel en provenance du fichier central des véhicules doit être autorisée et pour satisfaire à la *Loi Vie privée*, les conditions de cette communication doivent être stipulées dans les marchés publics et les conventions de concessions conclues avec les concessionnaires.

Intégrateur fédéral de services (Avis 41/2008)
Dans le courant de l'année 2008, la Commission a également émis un avis sur un avant-projet de loi relatif à l'institution et à l'organisation d'un *intégrateur de services fédéral*. L'évaluation de cette initiative pour laquelle la Commission avait déjà plaidé par le passé fut positive, compte tenu notamment de l'option prise d'un intégrateur de *services*, moins menaçante en termes de protection des données qu'une intégration de données. La Commission n'en a pas moins rappelé l'importance des concepts de source et données authentiques, du principe de la collecte unique et de la nécessaire transparence à l'égard du citoyen (possibilité de vérifier qui a consulté des données le concernant).

Décret flamand relatif à l'échange électronique de données administratives (Avis 01/2008)
Etant donné que ce décret visait avant tout à combler une lacune qui avait d'importantes répercussions sur la protection de la vie privée, et plus précisément l'absence d'un contrôle approfondi de l'échange électronique de données entre des services dépendant des institutions *fédérées*, l'initiative a été accueillie favorablement par la Commission. Cette dernière n'en a pas moins regretté que ce contrôle n'ait pas été confié à un comité sectoriel institué ou à instituer au sein de la Commission mais à une commission flamande autonome, extérieure à la Commission et dont l'indépendance ne lui paraissait de surcroît pas garantie. À cet égard, elle a souligné que cette option compliquerait l'échange de données entre les autorités des différents niveaux de pouvoir et qu'elle induisait un risque de jurisprudence divergente. Le décret finalement adopté a tenu compte de manière non négligeable des remarques de la Commission. Afin de garantir son indépendance, la commission flamande a été instituée par le Parlement flamand et un lien étroit a été organisé avec la Commission dont 3 membres font désormais également partie de cette nouvelle commission fédérée.

Nouvelles technologies

Rétention des données (Avis 24/2008)
En 2008, la Commission a rendu un avis visant à transposer en droit belge la directive européenne 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. Cette directive poursuit l'objectif d'harmoniser les obligations imposées aux fournisseurs en matière de conservation de certaines données et à garantir que ces données soient disponibles à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne. Pour diverses raisons, la Commission a émis un avis défavorable, dont principalement, l'absence de la mention des éléments essentiels en matière de conservation des données (type de données conservées, délai de conservation, mode de conservation, justification de la conservation, type de faits criminels dont la répression justifie l'utilisation des données conservées, finalités etc.).

Information au public

C'est également en 2008 que la Commission a développé plusieurs pages de son site en anglais informant notamment le citoyen de ses activités internationales en ce domaine dans cette langue ainsi qu'en français et néerlandais.

[17] Ce comité sectoriel est compétent pour autoriser toute communication électronique de données au départ d'une autorité fédérale.

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 données à caractère personnel et à la libre circulation de ces données a été acquise dès décembre 2006 par l'adoption de la loi sur la protection des données à caractère personnel (LPDP). 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 n° 41 de 2007.

En 2008, la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 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, a été transposée en droit national au moyen de l'ordonnance n° 40 du 7 janvier 2008 émise par le ministère de l'intérieur et par le président de l'Agence publique pour les technologies de l'information et les communications et promulguée dans le Journal officiel n° 9 du 29 janvier 2008. Cette ordonnance définissait les catégories de données, la procédure relative à leur conservation et les mesures à prendre par les entreprises fournissant les services et/ou réseaux de communications électroniques accessibles au public, aux fins de la sécurité nationale et de la détection des crimes.

B. Jurisprudence

En 2008, les cas spécifiques de violation de la directive 95/46/CE et de la loi sur la protection des données à caractère personnel portaient sur le traitement de données personnelles allant au-delà des objectifs définis par la loi, et notamment de traitement ultérieur incompatible. Dans ces cas, il est établi que les responsables du traitement des données personnelles doivent obtenir une copie de la carte d'identité de la personne concernée pour fournir un certain type de service. C'est de cela qu'il était question dans diverses plaintes à l'encontre d'entreprises fournissant des services et/ou réseaux de communications électroniques accessibles au public en vertu de la loi sur les communications électroniques examinées par la commission pour la protection des données à caractère personnel.

Peuvent être considérés comme cas avérés de traitement de données personnelles non autorisé, les cas portant sur l'utilisation de données personnelles d'assurés dans le cadre d'un changement de compagnie d'assurance-retraite. Dans ces cas, les personnes concernées indiquent clairement ne pas avoir soumis de demande de changement et ne pas l'avoir signée devant notaire à des fins de certification des signatures. Selon la procédure en vigueur pour le transfert du dossier d'un assuré d'une compagnie à l'autre, toute compagnie d'assurance-retraite conclut un contrat avec une personne physique ou morale enregistrée comme courtier en assurances auprès de la commission de contrôle financière. En cas de demande de changement, l'assuré doit signer la demande, et sa signature doit être certifiée devant notaire. La demande est soumise à la compagnie que souhaite rejoindre l'assuré, où seules les conditions préalables sont vérifiées. Les activités de la commission pour la protection des données personnelles visent à renforcer le contrôle exercé par les compagnies d'assurance-retraite sur leurs courtiers, en leur qualité de responsables du traitement des données.

En 2008, la commission pour la protection des données personnelles a pris des mesures, de sa propre initiative, concernant l'organisation d'événements promotionnels (quizz, jeux et études de marché sur certains produits) et le traitement des données personnelles des participants lors de ceux-ci. Il a été établi que la réception d'un prix était associée à la fourniture de données personnelles complémentaires, tout comme la participation à ces événements exigeait que des informations à caractère personnel soient communiquées. La commission pour la protection des données personnelles avait publié des instructions contraignantes à l'intention des responsables du traitement des données afin qu'à l'avenir, ceux-ci observent le principe de proportionnalité des

données personnelles traitées et anonymisent les données collectées.

La commission pour la protection des données a émis des avis quant à la fourniture d'un accès au registre national de la population à toutes les parties pouvant justifier d'un intérêt légal ad hoc, personnes physiques et autorités publiques confondues, dans le but de mener à bien les opérations prévues par la loi. Des opinions ont également été rendues concernant les définitions de «responsable du traitement des données personnelles» et «agents du traitement des données personnelles».

La commission a répondu à de nombreuses requêtes émanant de personnes physiques quant aux droits que leur octroie la LPDP et aux obligations des responsables du traitement des données personnelles. Ces requêtes lui ont été adressées sous la forme de courriers électroniques, de lettres ou en personne. Beaucoup de ces questions portent sur la manière dont les droits des personnes physiques sont protégés lors du traitement de leurs données personnelles et sur la possibilité d'y accéder.

Les avis et les questions-réponses spécifiques de la commission en relation avec l'application de la loi sont publiés dans son bulletin, disponible sur son site internet officiel: www.cpdp.bg

En 2008, dans le cadre d'un projet de jumelage financé par le programme PHARE, et conjointement avec les experts de l'Agence espagnole pour la protection des données, une inspection planifiée a été effectuée dans le secteur bancaire. Celle-ci a permis d'établir que les clients des banques sont informés des données (avec mention du responsable du traitement des données et de ses représentants), sont familiarisés avec les objectifs du traitement des données personnelles et sont tenus au courant du fait que leurs données seront transférées à des tiers. Toutefois, les clients ne sont pas toujours au fait des destinataires ou des catégories de destinataires susceptibles de recevoir leurs données. Il y a également eu des cas dans lesquels les clients n'ont pas su si la fourniture des données était obligatoire ou facultative, ni les conséquences résultant d'un refus du responsable du traitement des données.

C. Questions diverses importantes

Concernant l'enregistrement des dossiers conservés par les responsables du traitement des données personnelles, effectué par la commission pour la protection des données, ainsi que la soumission habituelle des documents d'enregistrement sur papier, un système appelé eRALD a été introduit pour la première fois au début de l'année 2008. Destiné à l'enregistrement électronique des responsables du traitement des données personnelles, eRALD est une application basée sur le web qui permet à tous les responsables de saisir leurs propres données et d'amorcer le processus d'enregistrement ou d'apporter des modifications aux informations saisies. Ils reçoivent alors leur nom d'utilisateur et un mot de passe système, après quoi la procédure qu'ils ont lancée est entièrement sous leur contrôle. Ils assument alors la pleine responsabilité de l'exactitude de leurs données et de la mise à jour de celles-ci. L'accès aux données saisies est bloqué jusqu'à ce que l'enregistrement soit terminé.

La mise en œuvre d'un système d'enregistrement électronique est l'une des plus belles réussites de la commission, car celui-ci permet de considérablement simplifier et faciliter le processus et de largement écourter les délais d'enregistrement. Par ailleurs, ce système offre une plus grande stabilité et une sécurité juridique accrue.

Tout au long de l'année, la commission pour la protection des données personnelles a participé activement aux travaux du groupe *ad hoc* «protection des données personnelles», créé dans le cadre du groupe de travail conjoint du Conseil des ministres, dans le but de prendre les mesures nécessaires en vue de garantir la pleine mise en œuvre de l'acquis Schengen. Lors des réunions de travail organisées dans le cadre de cette initiative, la commission pour la protection des données personnelles débat des expériences des nouveaux pays Schengen, échange des expériences, et se familiarise avec les programmes de formation, les contrôles effectués sur la base de données SIS centrale, les recherches portant sur l'application de la base juridique, la coopération entre les autorités nationales de protection des données et l'influence de l'élargissement de l'espace Schengen.

Le 5 décembre 2008 à Bruxelles, lors de la réunion du groupe d'experts «évaluation Schengen» du Conseil de l'Union européenne, les experts bulgares du ministère de l'intérieur, du ministère des affaires étrangères et de la commission pour la protection des données personnelles ont présenté la synthèse des réponses apportées au questionnaire «évaluation Schengen». Cette présentation a amorcé la première phase de la procédure d'adhésion de la République de Bulgarie à l'espace Schengen, grande priorité et premier défi de notre pays après son adhésion à l'Union européenne.
À la fin de l'année 2008, la Commission européenne a approuvé une fiche de projet (BG-2007/019-303.07.03.01), prévoyant l'exécution d'une composante – le projet «Twinning Light» (BG/2007/IB/JH/01/UE/TWL): «Coopération en vue de la consolidation administrative de la commission bulgare pour la protection des données personnelles et d'une amélioration de l'activité de contrôle dans le domaine des audits sectoriels».

La procédure de sélection des partenaires est désormais clôturée. Le choix de la commission s'est porté sur l'Agence espagnole pour la protection des données. L'exécution des activités prévues dans le projet devrait démarrer dès que le contrat aura été signé.

Chypre

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

1. Il n'y a eu aucun développement législatif en relation avec la mise en œuvre des directives 95/46/CE et 2002/58/CE.

Des discussions ont eu lieu au sein des commissions parlementaires des affaires européennes, des questions législatives et des droits de l'Homme concernant l'application de la législation nationale en matière de protection des données (loi 138(I)/2001).

Ces débats ont été suivis d'une note soumise par le commissaire qui traitait:
- de l'évaluation de la conformité à la législation;
- de la sensibilisation du public;
- de l'efficacité de l'exercice des pouvoirs du commissaire et des mesures requises pour optimiser cette efficacité;
- des problèmes et difficultés rencontrés dans le fonctionnement du bureau du commissaire (essentiellement liés au recrutement de personnel).

Pour sa part, la commission parlementaire des affaires européennes a publié un rapport dans laquelle elle commente les questions ci-dessus, notamment, et fait mention spéciale du rôle du groupe de travail et de sa contribution, surtout dans le cadre de l'utilisation croissante des données personnelles au nom de la lutte contre le terrorisme.

2. La loi transposant la directive 2006/24/CE sur la conservation des données de télécommunications a été amendée de sorte à permettre, dans les cas d'enlèvements, d'accéder auxdites données sans qu'il soit nécessaire d'obtenir une ordonnance du tribunal.

Une telle ordonnance doit néanmoins être obtenue dans un délai de 48 heures à compter du moment de l'accès auxdites données et, en l'absence de celle-ci, l'officier de police chargé du dossier doit détruire les données obtenues et en informer le commissaire responsable de la protection des données personnelles.

3. Une loi relative à la prévention des actes de violence lors des manifestations sportives a été adoptée. Celle-ci prévoit, entre autres choses, l'instauration et l'exploitation d'une base de données contenant des enregistrements de données personnelles concernant des personnes qui se sont vu interdire l'accès aux sites sportifs correspondants, en vue de lutter contre la violence lors des manifestations sportives, et plus particulièrement lors des rencontres de football.

B. Jurisprudence

Une plainte relative à la perte du dossier d'un patient à l'hôpital général de Nicosie a été examinée par mon bureau. L'administration hospitalière a admis qu'elle ne retrouvait pas le dossier du plaignant. En conséquence, l'hôpital s'est vu imposer une amende de 2 000 EUR.

Lors de l'examen d'une plainte déposée auprès de mes services par une personne affirmant que les données personnelles la concernant contenues dans une base de données du ministère de l'éducation et de la culture avaient été utilisées illégalement par un syndicat étudiant à des fins de «marketing», nous avons découvert que le responsable de la base de données en question avait pris sa retraite deux ans auparavant et que l'autorité concernée n'avait désigné personne pour le remplacer.

Cette omission ayant conduit à l'absence d'un gardien de la légalité du traitement des données personnelles, nous avons conclu que le directeur général du ministère était responsable de cet état de fait et avons imposé une amende de 1 500 EUR.

C. Questions diverses importantes

- Au cours de l'année 2008, nous avons continué à suivre et à examiner les mesures prises par le nouvel hôpital général de Nicosie conformément aux recommandations formulées suite à notre audit de 2007. Nous surveillons les procédures instaurées en matière de sécurité et d'accès aux données personnelles traitées

par l'hôpital, et sommes tenus informés de l'état d'avancement de la mise en place et de l'utilisation de son système informatique.

- Plusieurs plaintes ont été enregistrées concernant l'utilisation de systèmes de vidéosurveillance sur le lieu de travail et l'exploitation des empreintes digitales des travailleurs pour vérifier leur présence au travail. Étant donné que nous avions déjà émis des orientations sur ces deux questions, nous vérifions la conformité des actions des responsables de données avec nos instructions spécifiques.

- Nous avons aussi examiné les questions de l'accès des enseignants à leurs dossiers personnels et de la catégorisation des absences des fonctionnaires de manière à restreindre la classification en congés maladie et à consigner ces derniers dans un fichier séparé auquel seul le personnel disposant d'une autorisation écrite de l'autorité ad hoc peut avoir accès.

République tchèque

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

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 2008, la procédure d'amendement de la loi n° 127 sur les communications électroniques découlant de la nécessité de transposer en droit national la directive 2006/24/CE sur la conservation de données a été clôturée.

Lors de l'application de la législation nationale et, par extension, de la législation de l'Union ou de la Communauté européenne, les contrôles, dont les inspections sur site, continuent à jouer un rôle capital. Les requêtes auxquelles répondent les inspecteurs peuvent être subdivisées en deux groupes fondamentaux: les plaintes concernant des infractions ponctuelles à la législation et les plaintes suggérant une violation systématique de la loi. Dans le cas d'infractions isolées, le problème est souvent résolu lors de la phase d'inspection préliminaire. Dans ces cas, une mesure corrective peut être imposée sans contrôle formel. Cette approche ne peut pas être utilisée dans tous les cas; elle se limite généralement aux cas où l'irrégularité ne résulte pas d'une action délibérée. Cela étant, les inspecteurs traitent la majorité des plaintes en effectuant les contrôles adéquats, dont des inspections sur site.

Bien que les contrôles demeurent le principal outil de supervision, l'accent est de plus en plus mis sur la sensibilisation à la protection des données personnelles. L'année dernière, par exemple, les spécialistes de l'OPDP ont donné 260 heures de cours et conférences.

Un programme conçu par l'OPDP à l'intention des enseignants a également été lancé. Celui-ci a été approuvé pour trois ans par le ministère de l'éducation, de la jeunesse et des sports. Des séminaires ont été organisés dans les régions. Par ailleurs, cette année a vu la seconde édition du concours annuel d'art et de littérature «C'est ma vie privée! Interdit d'y regarder, d'y fouiller» destiné aux enfants et aux jeunes. Cette fois, les enfants de «SOS Villages » de République tchèque, d'Ukraine, du Kazakhstan, de Russie et de Bosnie-Herzégovine ont également pris part à ce concours, avec succès. L'Office se félicite sincèrement de cette coopération, parce qu'il considère comme essentiel que des enfants qui ont à préparer leur avenir sans l'aide d'une famille soient eux aussi suffisamment informés de leurs droits.

Suite à la reconnaissance internationale qu'a reçu l'Office l'année précédente pour son concours destiné aux enfants et son projet de formation des enseignants (Madrid, 2007, Prix des meilleures pratiques en matière de protection des données dans les services publics européens), les travaux des enfants ont été exposés dans le hall d'entrée du Palais de l'Europe à Strasbourg à l'occasion de la journée de la protection des données.

L'Office a également poursuivi sa collaboration avec la troisième faculté de médecine de l'université Charles en organisant un séminaire sur la menace spécifique qui pèse sur le respect de la vie privée et la protection des données des personnes âgées.

B. Jurisprudence

Dans le cadre de ***l'archivage électronique de l'administration publique*** et de l'introduction des services

d'administration en ligne, les travaux relatifs à la préparation de la législation sur les nouveaux registres électroniques d'administration publique se sont poursuivis. L'OPDP a émis des commentaires et réserves fondamentaux et insisté sur le fait qu'il convenait de débattre des aspects techniques et d'évaluer les risques associés à la protection et à la sécurisation des données personnelles, ce qui explique qu'il soit souvent considéré comme un frein au processus. Néanmoins, bien que l'Office ne soit pas parvenu à faire valoir toutes ses positions, son influence positive sur la solution adoptée en définitive est évidente.

Il a également exercé une influence positive sur la préparation de la ***loi sur le recensement 2011***. Dans ce contexte, il a formulé nombre d'observations sur la nécessité de veiller à ce que, lors du nouveau recensement électronique planifié, dans le cadre du travail du responsable de ce recensement et dans l'éventualité d'une coopération avec des entités extérieures, des règles claires soient mises en place, régissant l'accès à certains types d'informations et la protection des données contre les abus.

En revanche, ses tentatives visant à influer sur le fonctionnement des ***registres médicaux*** n'ont pas été couronnées de succès, le ministère de la santé n'ayant pas accepté la requête de l'OPDP visant à entièrement clarifier le concept des registres centraux. L'Office a demandé une explication justifiant la période de conservation des données dans les différents registres ainsi que la raison pour laquelle le consentement des personnes affectées n'est pas pris en compte, comme c'est le cas dans certains autres États européens.

Toutes les suggestions de l'Office n'ont pas été retenues lorsque la ***loi sur les conflits d'intérêt***, proposée sur initiative parlementaire, a été préparée. Dans ce contexte, l'Office a obtenu des pouvoirs de surveillance spécifiques, mais il reste d'avis que la loi n'établit pas une distinction suffisamment claire entre les agents constitutionnels et autres agents élus qui, en tant que personnalités publiques, disposent d'une garantie de protection de leur vie privée fondamentalement réduite, et les agents de l'administration publique dont la protection de la vie privée doit essentiellement être préservée pour ce qui est des questions sans lien direct avec la conduite de leurs tâches officielles.

C. Questions diverses importantes

En matière d'***activités de contrôle***, en 2008, l'OPDP a réalisé un total de 112 inspections en relation avec la loi n° 101/2000 Coll. (soit le même nombre qu'en 2007), ainsi que 91 contrôles portant sur les communications commerciales non sollicitées en vertu de la loi n° 480/2004 Coll. sur certains services de la société de l'information. La plupart des inspections effectuées par les inspecteurs indépendants et leur équipe de contrôle ont été organisées ponctuellement sur la base de requêtes ou de plaintes d'individus. Seules un peu plus de 10 % 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 2008*** était centré sur 5 grands thèmes:

1. le traitement des données personnelles dans les travaux des autorités judiciaires, avec un accent particulier sur l'exécution des décisions et sur la pratique des tribunaux dans la gestion du registre d'insolvabilité;
2. le traitement des données personnelles en relation avec les systèmes d'information conjoints de l'Union européenne, à savoir le système d'information douanier (SID), EURODAC et le système d'information Schengen;
3. les systèmes d'information publics qui ne sont pas classifiés ailleurs, avec un intérêt particulier pour les institutions de diagnostic, les foyers pour enfants, avec les écoles et centres de soins éducatifs, et plus précisément la manière dont les institutions s'occupant d'enfants qui grandissent en dehors d'une famille standard traitent les données personnelles, de même que le ministère des finances et les bureaux des taxes;
4. le traitement des données personnelles dans le cadre des systèmes de surveillance dans les secteurs public et privé, à savoir dans les bâtiments du ministère de la culture, les hôpitaux, les institutions sociales et dans les bureaux des sociétés privées;
5. le traitement des données personnelles en relation avec la protection des consommateurs, avec un accent spécifique sur les technologies modernes permettant une identification rapide, et surtout sur les systèmes RFID.

Les contrôles reposant sur des plaintes et autres requêtes concernaient un vaste éventail de domaines, tant dans les secteurs public que privé. Parmi les plus visés, l'un de ceux-ci était l'administration publique, où les problèmes relatifs à l'utilisation des registres de la population, par exemple, sont fréquents. Cette source est exploitée par de nombreuses autorités de l'administration publique, tant dans le cadre de la législation sur les registres de la population que sur la base de plusieurs dizaines de lois spécifiques; l'Office est souvent confronté à des tentatives visant à faire une utilisation plus large de ces données que ne le permettent ces lois.

Des plaintes ont aussi débouché sur des contrôles dans le système des soins de santé, où plusieurs infractions à la loi sur la protection des données personnelles ont été identifiées.

L'Office a prêté une attention particulière au traitement des données personnelles en relation avec l'ADN. Un contrôle a été effectué en 2008 à l'Institut de criminologie de la police tchèque, l'exploitant de la base de données nationale de l'ADN. Celui-ci était motivé par des plaintes et s'appuyait sur le plan de contrôle de la période antérieure. Des infractions à la loi sur la protection des données personnelles ont été identifiées, des données sensibles ayant été collectées, traitées et stockées dans une mesure sortant du cadre de l'autorisation statutaire. Dans de tels cas, la loi exige que le consentement de la personne concernée soit obtenu, ce qui n'était pas le cas. Le contrôle a notamment conclu à la mise à l'amende de l'institution et à l'application de mesures correctives, résidant dans la destruction des données personnelles traitées d'une manière contraire à la loi.

Des plaintes et autres requêtes ont également débouché sur un contrôle ciblant des sociétés privées qui effectuaient des tests génétiques de paternité et de parenté à des fins d'identification pour des motifs commerciaux, ainsi que des analyses ADN à des fins de recherche et dans le but de diagnostiquer des maladies génétiques et de prédire l'efficacité de leur traitement. Des infractions à plusieurs dispositions de la loi (obligation de notification, consentement ne couvrant pas toutes les utilisations qui étaient faites des données, certains aspects de la proportionnalité, etc.) ont été identifiées, et une amende de même que des mesures correctives ont été imposées.

Les systèmes de (vidéo)surveillance dans les secteurs public et privé continuent à faire l'objet de nombreuses plaintes et de contrôles en relation avec celles-ci. Il s'agit d'une tendance croissante, bien que de petites victoires (p. ex. plus de retenue dans l'installation de caméras dans les écoles) aient pu être remportées grâce aux nombreux contrôles effectués et à des programmes de sensibilisation intensifs menés par l'Office, sous la forme d'avis, de consultations, etc.

Les activités de contrôle précitées n'incluent pas celles qui concernent les ***communications commerciales non sollicitées*** («pourriel commercial»). En 2008, cet agenda spécial comportait 1 458 plaintes et autres requêtes reçues par l'OPDP, dont 1 311 ont été traitées, avec 91 contrôles clôturés et 81 sanctions imposées.

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) a été adoptée le 31 mai 2000 et est entrée en vigueur le 1er juillet de la même année. 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° 714 du 26 juin 2008 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° 1069 du 6 novembre 2008);
- la section 263 du Code pénal (cf. décret n° 1068 du 6 novembre 2008).

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. En 2008, la DPA a rendu son avis sur plusieurs lois et règlements ayant une incidence sur la vie privée et la protection des données.

B. Jurisprudence

En février 2008, une boîte de nuit a demandé à la DPA l'autorisation, au titre de la section 50, paragraphe 1, de la loi sur le traitement des données à caractère personnel, de traiter des données sur ses clients en vue de garantir la sécurité et la quiétude de son environnement la nuit.

Son intention était de mettre en place les initiatives suivantes:
- créer un système de contrôle d'accès électronique basé sur les empreintes digitales (modèles) et sur les photos de ses clients;
- créer une liste interne de clients qui se sont vu interdire l'accès à la boîte de nuit suite à des actes de violence, à des actes de vandalisme, à des menaces ou à l'utilisation et/ou à la vente de stupéfiants. Celle-ci contiendrait des informations sur la durée et sur les motifs de l'interdiction.

Après avoir présenté le dossier au Conseil, la DPA a conclu que la boîte de nuit pouvait utiliser les empreintes (modèles) et photos de ses clients avec leur accord explicite.

Si un client revient sur son consentement, la boîte de nuit est tenue de supprimer ses empreintes et sa photo.

La DPA a également conclu que la boîte de nuit pouvait être autorisée à traiter des données sensibles (telles des données concernant la santé (consommation de drogue) et les antécédents judiciaires) dans le respect des conditions suivantes:
- Le traitement des données sensibles en relation avec une interdiction d'accès et la gestion de celle-ci ne peut s'effectuer qu'avec le consentement écrit du client. Ce consentement doit être explicite et conforme aux critères de la loi sur le traitement des données à caractère personnel. En d'autres termes, il doit être donné librement, spécifique et éclairé.
- Si le client revient sur son consentement, les données relatives au motif de l'interdiction doivent être supprimées.

- Le traitement des données sensibles doit s'effectuer en conformité avec les mesures de sécurité spécifiées et énumérées dans une annexe.

Les employés de la boîte de nuit doivent être informés du fait que l'usage qu'ils feront de la liste des clients *persona non grata* sera consigné dans un journal et que celui-ci pourra être exploité en vue d'identifier toute utilisation non autorisée de la liste des hôtes indésirables.

C. Questions diverses importantes

En novembre 2007, il a été porté à l'attention de la DPA que des données sensibles relatives à des personnes physiques avaient été divulguées dans le cadre de la publication de présentations PowerPoint.

La DPA a dès lors ouvert, de sa propre initiative, plusieurs cas à l'encontre d'autorités publiques et de responsables privés. La plupart des dossiers ouverts en 2007 ont été clôturés en 2008, avec des critiques de la DPA à l'égard des responsables des publications.

Suite à ce problème, la DPA danoise a également demandé que les autorités publiques danoises veillent à ce que leurs sites internet ne contiennent pas de données intégrées de ce type en relation avec des personnes physiques.

Par ailleurs, elle a recommandé aux autorités publiques de vérifier si de telles données avaient été divulguées à des tiers par d'autres canaux, p. ex. aux participants de réunions, etc. Dans l'affirmative, les autorités publiques sont invitées à prendre des mesures afin de retirer les données ou à demander aux destinataires de les supprimer.

Description du problème de sécurité et moyens de prévention:
Ce problème de sécurité se pose avec des présentations PowerPoint contenant des graphiques Excel ou des tableaux sous forme d'objet imbriqué.

En ouvrant cet objet, il est possible d'accéder aux données sous-jacentes, lesquelles sont susceptibles de contenir des informations sensibles (pour ce faire, il suffit d'enregistrer le fichier .ppt sur votre ordinateur, puis de l'ouvrir dans votre application PowerPoint et de cliquer sur le graphique ou sur le tableau en question).

Ce problème s'est principalement posé avec des présentations PowerPoint, mais il est également présent dans d'autres types de fichiers Office, tels que les documents Word, si un fichier d'un autre programme (par exemple Excel) a été imbriqué.

Le problème de sécurité peut être évité de la manière suivante:
1) en convertissant la présentation PowerPoint au format .pdf;
2) en insérant les graphiques et tableaux sous la forme d'images et non d'objets.

La même procédure est utilisée pour l'insertion de graphiques et de tableaux dans des documents Word.

Estonie

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

Au cours de la période de référence 2008, d'importants développements ont eu lieu concernant la mise en œuvre de la loi sur la protection des données à caractère personnel (ci-après PDPA, *Personal Data Protection Act*). La nouvelle version de la PDPA est entrée en vigueur le 1er janvier 2008.

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. 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 (un «détaché à la protection des données à caractère personnel», conformément à la directive 95/46).

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

Comme mentionné ci-avant, 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».

Par ailleurs, une nouvelle disposition portant sur la divulgation des données a été proposée. Depuis janvier 2008, toute personne a le droit de demander que ses données personnelles, légalement classées à usage public, ne soient plus divulguées ni utilisées. Dès lors, toute personne garde le contrôle de tout nouvel usage de ses données après leur divulgation, ce que ne permettait pas la version précédente de la loi.

De même, la nouvelle version de la PDPA régit la collecte de données à caractère personnel pour l'évaluation de la solvabilité – 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 estonien ne peuvent remonter à plus de trois ans, et les données antérieures doivent être supprimées. Cet amendement vise principalement à garantir que chaque responsable du traitement de données est au clair sur 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. Une personne peut empêcher le traitement de ses données personnelles lorsque la base légale de la divulgation et du traitement ne peut être vérifiée. Lorsque le traitement initial des données 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), la poursuite de leur traitement ne peut pas être interdit.

B. Jurisprudence

Traitement de données personnelles à des fins journalistiques sans le consentement de la personne concernée

La nouvelle version de la PDPA, entrée en vigueur le 1er janvier 2008, a modifié les dispositions relatives au traitement des données personnelles à des fins journalistiques et à la réalisation d'enregistrements audio ou vidéo dans les lieux publics.

Malheureusement, les premières expériences négatives à propos de ce sujet sensible se sont fait jour. Par exemple, en 2008, l'inspection estonienne de la protection des

données a lancé une procédure délictuelle basée sur une plainte émanant d'une personne privée qui était apparue sur une chaîne de télévision. Selon le plaignant, l'équipe de tournage de la chaîne de télévision l'avait filmé, dans son exploitation agricole, sans lui avoir demandé son autorisation et sans son consentement. Le reportage a été diffusé dans un programme d'information populaire de la chaîne, en dépit de l'interdiction du plaignant.

Le traitement de données personnelles n'est autorisé qu'avec le consentement de la personne concernée, et il convient d'établir clairement la quantité de données pour laquelle l'autorisation de traitement a été donnée, le but du traitement des données et les personnes à qui la transmission des données est autorisée. Le silence ou l'inaction ne sont pas réputés valoir consentement.

Dans ce cas, l'hypothèse selon laquelle le plaignant était informé de la visite de l'équipe de tournage ne peut pas être considérée comme un consentement de celui-ci. Par conséquent, l'équipe a commencé à filmer sans le consentement du plaignant. Par ailleurs, aucun consentement n'a été demandé pour la diffusion du reportage dans le programme d'information.

L'exemption prévue dans la nouvelle version de la PDPA stipule que les données personnelles peuvent être traitées et divulguées dans les médias à des fins journalistiques sans le consentement de la personne concernée si l'intérêt public est prédominant et si une telle procédure est conforme aux principes de l'éthique journalistique. Dans ce cas, l'intérêt public n'a pas pu être établi avec certitude, et par conséquent, l'exemption ne pouvait entrer en ligne de compte.

La chaîne de télévision s'est vu imposer une amende de 760 EUR pour avoir filmé et diffusé le reportage sans le consentement de la personne concernée.

C. Questions diverses importantes

Pour la seconde année consécutive, l'inspection de la protection des données a défini, de sa propre initiative, les priorités des opérations de surveillance pour l'année. Plusieurs sujets ont été retenus et traités en profondeur à cette occasion, et l'inspection a publié un avis ou un document d'orientation pour chacun d'eux sur son site internet (http://www.aki.ee). Les agents de l'inspection ont retenu les sujets qu'ils considéraient les plus problématiques dans le domaine de la protection des données personnelles et de la liberté de l'information.

Des analyses et des contrôles sur site ont été effectués sur cette base, et des lignes directrices/documents d'orientation y afférents ont été préparés.

Voici les priorités choisies et les lignes directrices publiées pour la période de référence: traitement des données personnelles des financiers des partis politiques, traitement des données personnelles des hôteliers, traitement des données personnelles des passagers, prise de vues dans les institutions pédagogiques, consignation du traitement des données personnelles sensibles par les entreprises de sécurité, publication de listes d'étudiants et de diplômés. Par ailleurs, l'inspection a rédigé un questionnaire d'auto-évaluation à l'intention des responsables du traitement des données en vue de préciser et d'analyser les procédures et le système de traitement des données en vigueur au sein de l'entreprise.

Finlande

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 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.

Modifications

Au cours de l'année de référence, aucun amendement n'a en soi été apporté à la loi sur les données personnelles (523/1999), mais les dispositions relatives aux données de crédit en ont été extraites pour former une loi à part entière. La période de transition de la loi sur les données de crédit a pris fin le 1er novembre 2008. La loi assure une protection partielle des données relatives aux personnes morales et insiste sur le fait que les responsables des données doivent disposer de suffisamment de compétences en matière de protection des données. Un nouveau chapitre, le chapitre 5a, a été ajouté à la loi sur la protection de la vie privée dans la vie professionnelle. Celui-ci contient des dispositions détaillées quant à l'utilisation qui peut être faite des données de crédit personnelles dans la vie professionnelle

Au cours de l'année de référence, les amendements requis par la directive (2006/24/CE) ont été introduits dans la loi sur la protection de la vie privée dans les communications électroniques (516/2004). Le délai de mise en œuvre de ceux-ci est le 15 mars 2009.

En 2006, le Parlement finlandais a demandé au gouvernement de commencer à préparer la législation sur la protection générale des données personnelles dans le cadre de l'identification biométrique. Selon le ministère de la justice, qui est responsable de ces travaux, les dispositions générales relatives au traitement de l'identification biométrique seront préparées parallèlement à la révision globale de la loi sur les données personnelles (95/46/CE, article 8, paragraphe 7), qui devrait démarrer plus tard.

B. Jurisprudence

Le 17 juillet 2008, la Cour européenne des droits de l'homme a rendu son jugement dans l'affaire «I contre Finlande» (n° 20511/03). Cette affaire portait, entre autres, sur le droit d'une personne à savoir, sur la base du fichier

journal, qui a eu accès à son dossier médical. La législation finlandaise exige que les données soient protégées, notamment en vue de garantir expressément que les informations de ce type sont accessibles. Toutefois, le système d'information de l'hôpital est conçu de telle sorte que l'administration des droits d'accès et le fichier journal ne spécifient pas de manière détaillée l'identité des personnes qui ont traité les données. Par conséquent, et en application du principe des poursuites obligatoires, le tribunal pénal ne pouvait pas reconnaître la culpabilité de quiconque en cas de délit. Dans son arrêt, la Cour européenne des droits de l'homme a déclaré qu'il s'était présenté une situation où, du fait des caractéristiques fonctionnelles d'un système d'information non contrôlé conformément à la législation, la protection de la vie privée de la personne concernée, telle que définie à l'article 8 de la Convention européenne des droits de l'homme, avait été violée. Cette décision revêt une importance toute particulière, compte tenu du fait que la Cour européenne des droits de l'homme y a appliqué la Convention des droits de l'homme à un système d'information électronique et à ses carences.

Le 16 décembre 2008, la Cour de justice des Communautés européennes (grande chambre) a rendu son arrêt sur la publication des données relatives aux revenus perçus. Cette affaire avait trait au champ d'application de la directive 95/46/CE, au traitement et à la mobilité des données personnelles en matière de fiscalité, à la protection des individus et à la liberté d'expression. La Cour a laissé le soin à une juridiction nationale de déterminer l'existence d'un traitement aux fins de journalisme tel que défini à l'article 9 de la directive 95/46/CE. Par ailleurs, selon l'arrêt, la directive sur la protection des données doit être appliquée au traitement des données personnelles dérivées de sources de données publiques et à l'utilisation des listes ou services déjà publiés. L'affaire en question est toujours en instance devant la Cour administrative suprême de Finlande.

Le Conseil compétent pour la protection des données a tranché sur le dossier ouvert par le bureau du médiateur pour la protection des données quant à l'authentification des demandeurs de crédits rapides par téléphone mobile. Dans sa décision, le Conseil pour la protection des données a conclu que la pratique selon laquelle le créancier identifie les demandeurs de crédit sur la seule base de leur nom, de leur numéro de sécurité sociale, de leur adresse et de leur numéro de téléphone via un SMS reconnu comme demande de crédit ne peut pas être considérée comme suffisamment fiable. En conséquence, le Conseil a interdit au répondant, qui suivait un processus d'authentification couramment utilisé dans le secteur, de traiter les données personnelles de la manière susmentionnée. Le répondant a introduit un recours à l'encontre de la décision du Conseil pour la protection des données devant la cour d'appel compétente. Suite à cette affaire notamment, une proposition visant à adopter une loi générale sur l'identification a été déposée en Finlande.

C. Questions diverses importantes

Attention aux lois spéciales

Selon la section 10 de la Constitution finlandaise, la protection des données personnelles doit être ancrée dans la législation. C'est ainsi qu'il existe, à l'heure actuelle, quelque 650 lois spéciales régissant la protection des données personnelles. Concernant le transfert de données entre les autorités, une autre loi générale s'applique, outre la loi sur la protection des données. Il s'agit de la loi sur la transparence des activités gouvernementales. Les tragiques fusillades qui ont eu lieu dans les écoles de Jokela et Kauhajoki ont ramené sur le devant de la scène la question du fonctionnement global du cadre législatif. À cet égard, une attention toute particulière a été accordée à la législation sur le bien-être des étudiants, sur les armes à feu et sur les soins de santé. Il a été établi que les autorités de différents secteurs de l'administration n'avaient pas accordé une attention suffisante à l'état de la législation. Cela étant, il était facile de s'apercevoir que le personnel chargé d'appliquer la législation à l'échelon local n'avait pas reçu suffisamment d'informations et d'orientations. Raison pour laquelle, confrontés à des problèmes, ses membres étaient incapables d'agir, fût-ce dans les limites autorisées par la législation.

Études réalisées

Au cours de l'année de référence, le bureau du médiateur pour la protection des données a réalisé plusieurs études. La loi nationale sur le traitement électronique des données clients dans les secteurs de l'aide sociale et des soins de santé contient une disposition spécifique

prévoyant la désignation d'un responsable de la protection des données au sein de chaque unité. En outre, elle exige du directeur de chaque unité qu'il établisse des lignes directrices spécifiques applicables en matière de protection des données. Selon notre étude, la mise en œuvre des dispositions a bien commencé, mais il reste des points à améliorer. Dans le même temps, un vaste programme de formation destiné aux responsables de la protection des données à été lancé. Son volet le plus complet se situe au niveau universitaire.

Lors de l'enquête «police du web», nous avons analysé la légalité du traitement réservé aux données personnelles dans les services basés sur le web en Finlande. Cette étude se concentrait notamment sur les réseaux sociaux, les services destinés aux enfants et aux jeunes ainsi qu'aux services collectant des données personnelles sensibles. Il en ressort que beaucoup reste à faire concernant le respect de l'obligation d'information. Des mesures spéciales ont été appliquées à certains des fournisseurs de services passés au crible.

Notre troisième étude évaluait le fonctionnement de la loi sur les données personnelles et, dans une certaine mesure, le système de sanctions criminelles. Au cours de celle-ci, nous avons analysé, entre autres, les sentences prononcées par les tribunaux et les décisions prises par le ministère public. L'étude a révélé que le nombre de délits relatifs à la protection des données personnelles continue à augmenter lentement mais sûrement, hausse imputable selon nous à la sensibilisation aux droits liés à la protection des données et à l'importance de cette dernière, à la sécurisation croissante des systèmes d'information et au renforcement des compétences professionnelles de la police et des magistrats en la matière. Cela étant, certains se demandent si le système de sanctions est suffisamment strict.

Recherche scientifique

Dans le cadre de leurs activités de recherche, les scientifiques sont souvent amenés à traiter des données personnelles sensibles issues de sources diverses. L'expérience a montré que les chercheurs sont souvent peu au fait des exigences qui leur incombent en termes de protection des données. Raison pour laquelle nous avons mis en œuvre un projet très complet de lignes directrices basées sur le web en coopération avec différentes autorités. Ce projet avait pour but d'améliorer le degré de protection des données dans la recherche scientifique, de faciliter le travail des chercheurs et d'améliorer les pratiques au sein des autorités d'où proviennent les informations. Il a notamment débouché sur des lignes directrices virtuelles assorties des systèmes d'assurance qualité requis et sur plusieurs manuels identifiant les meilleures pratiques en la matière.

France

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

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. Un premier décret d'application avait été adopté le 20 octobre 2005 puis fait l'objet d'une modification le 25 mars 2007 en vue d'apporter les modifications procédurales nécessaires.

B. Jurisprudence

L'Ordonnance du Conseil d'État du 19 février 2008 consacre le rôle juridictionnel de la CNIL

La CNIL dispose depuis la loi du 6 août 2004 d'une formation de sanction habilitée à engager des procédures et prononcer d'éventuelles sanctions à l'encontre des responsables du traitement de données. La nature et le statut de cette formation de jugement ont été précisés par le Conseil d'État à l'occasion d'une décision du 19 février 2008. Le Conseil d'État a en effet considéré que la «formation restreinte» de la CNIL devait être qualifiée de «juridiction» au sens de l'article 6-1 de la Convention européenne des droits de l'homme et des libertés fondamentales. Cette décision est importante et démontre qu'outre son rôle de gardien des libertés publiques, la CNIL a su s'imposer en tant qu'autorité de régulation et assurer, ainsi, l'effectivité du droit de chacun à la protection de ses données à caractère personnel.

C. Questions diverses importantes

L'adoption des délibérations

Au cours de l'exercice 2008, la CNIL a siégé 50 fois au cours de 36 séances plénières et 14 formations contentieuses. Ces réunions ont conduit à l'adoption de **586** délibérations, soit une progression de **50 %** par rapport à l'exercice 2007.

La CNIL a adopté en 2008:

- **391** autorisations (+**84 %** par rapport à 2007;
- **18** refus d'autorisation;
- **29** avis sur des traitements de données sensibles ou à risques.

Les saisines

La CNIL a reçu 6 760 saisines en 2008

En 2008, la CNIL a été saisie de 4 244 plaintes et 2 516 demandes de droit d'accès indirect, (soit un nombre en légère diminution (-5 %) par rapport à 2007 (2 660 demandes), mais toujours en nette progression (+ 58 %) par rapport à 2006 - 1 595 demandes -).

Si le volume des plaintes connaît également un très léger recul, il confirme néanmoins les attentes très fortes des citoyens en termes de respect des libertés.

Les déclarations de fichiers connaissent une évolution considérable en 2008 puisqu'elles s'élèvent à 71 990 contre 56 404 en 2007, soit une augmentation de l'ordre de **27 %**.

Les contrôles

En 2008 **218 missions de contrôle** ont été réalisées, soit une **augmentation de 33 %** par rapport à l'année précédente. Au début des années 2000, les contrôles n'excédaient pas la trentaine. Rappelons que le fait de s'opposer à un contrôle de la CNIL constitue un délit puni d'un an d'emprisonnement et de 15 000 euros d'amende. À cet égard, la première condamnation pour «délit d'entrave» a été prononcée par le Tribunal de grande instance de Paris en janvier 2009, suite à deux oppositions de contrôle en février et avril 2008.

Les conditions d'application de la loi «informatique et libertés» ont ainsi été contrôlées auprès de **145 organismes.**

Les contrôles menés par la Commission sont effectués afin de permettre **la mise en œuvre du programme annuel** adopté par la CNIL qui définit les thèmes jugés prioritaires par les commissaires.

Dans ce cadre, **la thématique du vote électronique** a été centrale. Vingt contrôles ont été réalisés pour des opérations de vote par voie électronique organisées en matière d'élections professionnelles. Il s'agissait d'apprécier le secret du scrutin, le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales et la surveillance effective du vote.

Le secteur **des collectivités locales** a également fait l'objet de contrôles en raison des nombreux fichiers, aux finalités diverses (état civil, listes électorales, action sociale, police municipale, gestion foncière, inscriptions scolaires, parfois sensibles), qu'elles détiennent et du caractère des données ainsi détenues.

L'année 2008 a été marquée par **la fin du contrôle du fichier STIC** (Système de traitement des infractions constatées) géré par le ministère de l'intérieur. Ce fichier a donné lieu à près d'une vingtaine de contrôles sur place auprès de commissariats, services régionaux de police judiciaire, tribunaux, préfectures ou direction régionale des renseignements généraux et permis une analyse très fine de son fonctionnement.

Le deuxième axe des contrôles opérés en 2008 est la réalisation de missions de vérification sur place dans le cadre des plaintes reçues par la CNIL. **25 % des contrôles réalisés en 2008** ont ainsi été décidés dans le cadre de l'instruction des plaintes.

Les sanctions
Depuis la loi du 6 août 2004, la CNIL dispose de pouvoirs de sanction qui lui confèrent le droit de prononcer des amendes d'un montant maximal de 150 000 euros (300 000 euros en cas de récidive), dans la limite de 5 % du chiffre d'affaires.

Au total pour l'année 2008, la CNIL a prononcé:
- 9 sanctions pécuniaires correspondant à des amendes comprises entre 100 et 30 000 euros;
- 1 avertissement;
- 126 (+ 20 %) mises en demeure.

Le correspondant informatique et libertés (CIL)
L'article 22 de la loi prévoit qu'en présence d'un «correspondant à la protection des données personnelles», dit correspondant informatique et libertés (CIL), dans l'organisme, celui-ci est dispensé des formalités déclaratives les plus courantes. Ces fichiers sont désormais inscrits dans un registre tenu par le CIL. En revanche, les traitements dits «sensibles», nécessitant une autorisation ou un avis, continuent à être soumis à la CNIL.

Au 31 décembre 2008, **3 679** organismes avaient désigné un CIL, ce qui correspond à une augmentation de **104 %** par rapport à l'année 2007. Le nombre total de CIL à la date du 31 décembre 2008 était de 989 car de nombreux organismes mutualisent leur correspondant informatique et libertés. **89 %** des désignations concernent le secteur privé. Le secteur public représente pour sa part **11 %**.

Le CIL doit permettre au responsable de traitements de respecter les obligations qui lui incombent et notamment, les droits des personnes concernées : droit d'accès, droit de rectification et de radiation, droit d'opposition. Il a ainsi pour mission de conseiller le responsable de traitements afin que les orientations stratégiques privilégiées soit conformes à la loi «informatique et libertés». Il doit également l'alerter en cas de manquements afin d'éviter toute sanction pénale. Le CIL apparaît ainsi comme source de sécurité juridique et témoigne des aspirations éthiques des organismes.

Les temps forts de l'activité 2008
Le fichier Edvige
La CNIL s'est prononcée en 2008 sur la création du fichier de police «Edvige»
La CNIL avait été saisie en mars 2008 par le ministère de l'intérieur d'un projet relatif à la création d'un fichier national mis en œuvre dans le cadre de la réforme des services français du renseignement confié à la direction centrale de la sécurité publique (DCSP).

Le ministère de l'intérieur avait souhaité que le décret de création du fichier «Edvige» ne soit pas publié au Journal officiel. Toutefois, dans un souci de transparence démocratique et d'information des citoyens, la CNIL a demandé que ce texte soit publié afin qu'un débat public s'instaure. Elle a obtenu satisfaction puisque tant l'acte créant ce fichier que son avis ont été publiés.
La publication de la création de ce fichier a également pour conséquence de permettre le contrôle sur place et sur pièces de ce fichier par la CNIL, ce qui constitue une garantie supplémentaire.

La CNIL a obtenu ensuite que le traitement ne fasse l'objet d'aucune interconnexion, d'aucun rapprochement ni d'aucune forme de mise en relation avec d'autres fichiers, notamment ceux de police judiciaire.

La CNIL est également intervenue pour que l'enregistrement de données relatives à des personnalités

publiques, syndicales, religieuses ou politiques (élus locaux et nationaux) soit nettement circonscrit, s'agissant en particulier de l'enregistrement de données ayant trait au «comportement» ou aux «déplacements» de ces personnalités.

Le projet de décret initial ne prévoyait aucune limite dans la durée de conservation des données enregistrées. La CNIL a donc œuvré pour qu'une durée limitée à 5 ans soit définie s'agissant des informations collectées sur une personne faisant l'objet d'une enquête administrative lors de l'accès à certains emplois (de sécurité etc..).

La CNIL a émis des réserves sur plusieurs aspects
S'agissant de la collecte d'informations relatives aux mineurs, la CNIL a rappelé son attachement au principe selon lequel une telle collecte doit rester exceptionnelle et encadrée de garanties renforcées. Elle a fait valoir le souhait que l'âge minimum de collecte d'informations relative à des mineurs soit portée à 16 ans contre 13 ans actuellement.

La question de l'âge des personnes susceptibles d'être fichées doit être mise en relation avec l'absence de limite dans la durée de conservation des données. Si des mineurs peuvent en effet, être à l'origine de «*troubles à l'ordre public*», il ne paraît pas légitime que de tels faits puissent leur être opposés 30 ans plus tard. Le droit à l'oubli, doit être garanti pour tous, y compris pour les citoyens de demain.

La CNIL a par ailleurs estimé que la possibilité offerte de collecter des informations relatives aux origines ethniques, à la santé et à la vie sexuelle des personnes n'était pas assortie de garanties suffisantes.

Elle a également souligné qu'elle ne disposait pas d'informations précises sur les niveaux de sécurité technique accompagnant le fonctionnement du fichier «Edvige» ni sur l'existence éventuelle d'un dispositif de traçabilité permettant de vérifier les conditions d'accès aux données figurant dans le fichier par les autorités publiques. Ces informations sont cependant nécessaires pour lui permettre d'exercer pleinement son contrôle.

Enfin, la CNIL a regretté l'absence de procédure formalisée de mise à jour et d'apurement des fichiers. Elle a pris acte cependant de l'obligation annuelle pesant sur le directeur général de la police nationale de rendre compte à la CNIL de ses activités de vérification, de mise à jour et d'effacement des informations enregistrées dans le fichier «Edvige».

À la suite de ses observations et des réactions suscitées par la publication du décret EDVIGE, le Gouvernement a retiré ce texte. Il a saisi la Commission de nouvelles propositions concernant, en particulier, la durée de conservation des informations relatives aux mineurs et les conditions d'enregistrement de certaines données sensibles, tout en annonçant qu'il renonçait à enregistrer dans ce fichier toutes données relatives aux personnalités publiques.

Le développement de la biométrie
Les dispositifs biométriques soumis à autorisation ou à avis de la CNIL sont en constante progression. Aussi, depuis 2004, plus de 1 800 demandes ont été adressées à la CNIL dont 1 500 concernent des dispositifs mis en œuvre conformément aux règles édictées par la CNIL en matière de reconnaissance du contour de la main ou d'empreintes digitales.

La CNIL, par l'intermédiaire de son service de l'expertise, joue un rôle d'accompagnement des entreprises lors de la conception de leurs systèmes d'exploitation de manière à garantir la protection des données des personnes. Ce service s'est tout particulièrement investi dans les systèmes présentés ci-après.

Le visa biométrique ou VISABIO
Ce nouveau système de visa biométrique avait fait l'objet d'une expérimentation en 2004 dans le cadre du projet pilote BIODEV. VISABIO devrait concerner chaque année plus de deux millions de ressortissants étrangers issus de pays soumis aux formalités de visa. L'objectif poursuivi est de permettre la collecte et le stockage au sein d'une base centralisée de données biométriques: la photo d'identité numérisée ainsi que les dix empreintes digitales du demandeur, combinées avec les données précédemment collectées au cours de la procédure de demande de visa.

Si l'utilisation de telles données permet indéniablement de faciliter les contrôles d'identité et l'authentification des pièces d'identité ainsi produites, la CNIL considère

que ce procédé doit être encadré dans des limites strictement définies. La CNIL déplore tout particulièrement qu'aucune attention n'ait été accordée à la possibilité de ne conserver les données biométriques que sur les visas biométriques, et non dans une base centrale. La CNIL souligne enfin l'importance toute particulière que revêt la collecte des empreintes digitales des mineurs de plus de 6 ans. Cette collecte ne doit pas être considérée comme une simple mesure technique, mais exige au contraire un réel débat de fond.

Le Passeport biométrique
En 2007, la CNIL avait fait part de son avis relatif au projet de décret. Le décret, dont la mise en œuvre pratique devait intervenir avant le 28 juin 2009, prévoit la délivrance de passeports constitués d'un dispositif électronique doté non seulement d'une photo d'identité numérisée, mais également de deux empreintes digitales conformément aux dispositions du règlement du Conseil de l'Union européenne du 13 décembre 2004.

Ce décret prévoit par ailleurs la conservation dans le fichier DELPHINE de la photo d'identité numérisée du demandeur de passeport ainsi que celle de huit de ses empreintes digitales. Ce stockage de données entraine des changements significatifs dans cette base de données.

La CNIL a fait part des réserves que suscite ce projet dès lors qu'il donne lieu à la constitution de la première base de données biométriques de ressortissants français à des fins administratives. Elle a tout particulièrement souligné que le traitement automatisé et centralisé de ces données n'est acceptable que dans la mesure où il est justifié par des considérations liées à l'ordre public ou à la sécurité intérieure. Sur ce point, la CNIL estime que les arguments avancés pour légitimer la création d'une telle base de données - l'amélioration des procédures de délivrance ou de renouvellement des passeports ou plus généralement la lutte contre la fraude – n'emportent pas totalement la conviction.

Le stockage des photos d'identité et des empreintes numérisées dans une base de données centralisée paraît en effet disproportionné au regard des objectifs affichés. Face aux réserves de la CNIL, le ministre de l'intérieur s'est engagé à ce que les empreintes digitales numérisées ne puissent être utilisées à des fins d'identification et qu'aucun dispositif de reconnaissance ne puisse être exploité à partir de la base de photos d'identité numérisées.

La CNIL a également déploré que cette nouvelle procédure de délivrance des passeports soit adoptée par le biais d'un règlement et non par la voie législative dès lors que les changements ainsi introduits vont au-delà des préconisations européennes. Le champ de cette réforme et les enjeux considérables qui la sous-tendent auraient incontestablement mérité qu'un débat public s'instaure et qu'un projet de loi soit élaboré.

La Reconnaissance vocale et des réseaux veineux
En 2008, la CNIL a autorisé pour la première fois l'exploitation de dispositifs reposant sur la reconnaissance de la voix et du réseau veineux du doigt. Ces autorisations ont été adoptées après que des expertises techniques approfondies aient été menées. La CNIL s'est ainsi assurée que ces dispositifs ne présentaient pas de risques au regard de la protection des données.

La reconnaissance vocale
Le système de reconnaissance vocale a pour objet de sécuriser et de faciliter la gestion des mots de passe utilisés pour accéder au système d'information d'une société en l'occurrence, la société Michelin. Le procédé ainsi mis en œuvre permet de générer et de réinitialiser automatiquement les mots de passe. Il repose sur la reconnaissance du gabarit de l'empreinte de la voix laquelle est numérisée puis segmentée par unités échantillonnées. Lors de la procédure d'enrôlement, chaque employé enregistre le gabarit de son empreinte vocale. Lorsqu'il souhaite renouveler son mot de passe, il lui appartient d'appeler un automate d'appel spécifique. Le système effectue alors une comparaison entre les mots répétés par l'utilisateur et le profil de référence.

À l'occasion de cette expertise, la Commission s'est assurée que les employés disposaient d'une information suffisante et que toutes les mesures étaient prises pour garantir la sécurité des données et prévenir ainsi tous risques d'usurpation d'identité.

La reconnaissance du réseau veineux
La CNIL a également autorisé pour la première fois en 2008 la mise en œuvre de cinq dispositifs reposant

sur la reconnaissance du réseau veineux du doigt de la main dont l'objet est le contrôle de l'accès aux locaux ou à des systèmes d'information. Cette technologie constitue un concurrent sérieux pour les technologies désormais classiques (empreintes digitales, iris, contour de la main…). Elle repose sur la reconnaissance de l'entrelacement des vaisseaux sanguins. Ce procédé présente l'avantage de reconnaître un réseau dissimulé sous la peau si bien qu'il n'est pas possible, actuellement au moins, de capturer et de copier cette biométrie à l'insu de la personne concernée.

À l'issue d'une expertise technique, 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 présente moins de risques que l'empreinte digitale.

Vidéosurveillance

La CNIL enregistre depuis les cinq dernières années un nombre croissant de déclarations de vidéosurveillance. Pour le seul exercice 2008, 2 588 déclarations ont été effectuées contre 1 317 en 2007.

Le nombre de plaintes a également connu une très forte progression au cours des exercices écoulés. Il s'établit à **173** soit une **hausse de 43 %**. Conformément à sa mission, la CNIL a procédé à de nombreux contrôles sur place et prononcé plusieurs mises en demeure à l'encontre d'organismes ayant installé des systèmes de vidéosurveillance sans avoir respecté les formalités prévues par la loi.

Or, l'importance considérable que prend la vidéosurveillance exige qu'une clarification soit opérée s'agissant des textes qui lui sont applicables.

Un cadre légal complexe, source d'insécurité juridique

Actuellement, les systèmes de vidéosurveillance peuvent relever de deux régimes juridiques distincts:

- **la loi du 21 janvier 1995** qui soumet les systèmes de vidéosurveillance visionnant les lieux ouverts au public à une autorisation préfectorale;
- **la loi «informatique et libertés» du 6 janvier 1978, modifiée en 2004**, qui réglemente les systèmes de vidéosurveillance installés dans les lieux non ouverts au public, tels qu'une entreprise, ou encore les systèmes implantés dans les lieux publics lorsqu'ils sont couplés à une technique biométrique (de reconnaissance faciale par exemple).

En pratique, ce cadre juridique, qui fait coexister deux dispositifs distincts, manque de lisibilité. Son application devient délicate dès lors que la majorité des dispositifs de vidéosurveillance ont désormais recours à des systèmes numériques qui en tant que tels constituent des traitements automatisés de données personnelles et relèvent donc de la compétence de la CNIL indépendamment de leur lieu d'installation. Face à cette situation, la CNIL estime nécessaire de clarifier rapidement le régime actuel de la vidéosurveillance afin de disposer d'un meilleur encadrement des pratiques.

La question du contrôle, par un organisme véritablement indépendant, des dispositifs de vidéosurveillance, constitue désormais, dans les sociétés démocratiques modernes, une exigence fondamentale.

La mise en place de systèmes de vidéosurveillance exige une réelle adhésion de la population. Si certaines études d'opinion montrent que la population est globalement favorable à la vidéosurveillance, pour autant les Français ne sont pas disposés à renoncer à la protection de leurs droits individuels.

Ainsi, pour alimenter sa réflexion, la CNIL a confié à IPSOS **la réalisation d'une étude sur l'opinion des Français vis-à-vis de la vidéosurveillance**. L'étude réalisée en mars 2008 auprès d'un échantillon de 972 personnes, représentatives de la population française âgée de 18 ans et plus, confirme, qu'une large majorité de Français (71 %) se déclarent favorables à la présence de caméras de vidéosurveillance dans les lieux publics. 65 % d'entre eux estiment que la multiplication des caméras permettra de lutter contre la délinquance et le terrorisme.

L'idée que ces dispositifs de vidéosurveillance soient placés sous le contrôle d'un organisme indépendant séduit une large majorité des Français (79 %) qui voient en la CNIL l'organisme le plus indiqué pour assurer ce contrôle.

C'est à la seule condition de disposer tant d'un régime de la vidéosurveillance encadré par des textes clairs et protecteurs des droits des personnes que d'un organe de contrôle indépendant que l'on pourra parler de «vidéo protection» selon l'expression consacrée par le ministre de l'intérieur.

Allemagne

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

Loi de mise en œuvre de la directive relative au respect des droits de propriété intellectuelle

Le 11 avril 2008, le Bundestag allemand adoptait la loi de mise en œuvre de la directive relative au respect des droits de propriété intellectuelle (directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle), entrée en vigueur le 1er septembre 2008 (Journal officiel fédéral I 2008, 1191). Celle-ci porte amendement de plusieurs lois relatives à la protection des droits de propriété intellectuelle.

Ainsi, la loi sur les brevets, la loi sur les modèles d'utilité, la loi sur les marques commerciales, la loi sur la protection des semi-conducteurs, la loi sur les modèles déposés et la loi sur la protection des droits d'obtenteur ont dans une large mesure été amendées par l'emploi d'un libellé identique. Plus particulièrement, cette loi accorde aux détenteurs des droits, et surtout à l'industrie cinématographique et musicale, qu'elle entend protéger contre le «piratage» opéré par les sites d'échange de fichiers sur l'internet, un droit à l'information opposable, en vertu du droit civil, aux fournisseurs d'accès internet en vue d'identifier les contrevenants potentiels à la législation en vigueur. Toutefois, une ordonnance judiciaire est nécessaire pour obtenir ces informations, ce qui, du point de vue de la protection des données, est indispensable pour l'exploitation des données relatives au trafic.

Il n'est pas permis d'utiliser des données conservées à des fins d'utilisation ultérieure pour obtenir des informations. Lors de la transposition en droit allemand de la directive relative à la conservation des données, le législateur a explicitement restreint l'utilisation des données conservées aux fins des enquêtes criminelles et de l'élimination des dangers, comme en témoigne la section 113b, paragraphe 1, 1ère phrase, de la loi sur les télécommunications.

La question de savoir s'il est acceptable de rechercher les adresses IP, procédure requise pour identifier l'utilisateur, doit encore être tranchée. L'identification peut par exemple se faire par le biais de fichiers «espions» qui, sous couvert de la connexion vers un support que recherche l'utilisateur du site de partage de fichiers, ont pour seul but de déterminer les adresses IP de la personne en question. Le téléchargement de la piste musicale, par exemple, ne s'effectue donc en fait pas. Dans d'autres cas, les sites de partage de fichiers sont passés au crible au moyen de la somme de contrôle de fichiers de données protégés par copyright. Si le dossier ouvert sur l'ordinateur comporte les fichiers recherchés, son adresse IP sera aussi trouvée. Il s'agit ici aussi d'un cas de collecte dérobée d'adresses IP des membres de sites de partage de fichiers visant une exploitation subséquente des données sans lien avec le but initial.

Loi relative à la prévention des dangers posés par le terrorisme international

La loi relative à la prévention des dangers posés par le terrorisme international, entrée en vigueur le 1er janvier 2009 a conféré à l'Office fédéral d'investigation criminelle (BKA) d'importants pouvoirs visant la défense du territoire contre le terrorisme international.

Ces nouvelles tâches introduisent une faille dans l'architecture fédérale de la sécurité. À l'origine, en République fédérale d'Allemagne, les missions de police relevaient de la compétence des états fédérés (Länder). L'attribution de pouvoirs de prévention au BKA modifie cette répartition des compétences.

Du point de vue de la protection des données, il convient de mentionner deux points critiques d'une importance capitale.

Tout d'abord, le doute est permis quant au caractère approprié, nécessaire et adapté des pouvoirs conférés au BKA en matière de collecte et de traitement des données en vue d'exécuter les tâches qui lui sont assignées. Outre ses missions de police traditionnelles, le BKA se voit en effet doté de pouvoirs spéciaux d'investigation incluant même la fouille en ligne de systèmes télématiques. Compte tenu de la compétence que conservent les états fédérés eu égard à la prévention des dangers posés par le terrorisme international, on peut s'interroger sur l'adéquation de cette abondance de nouvelles compétences pour les quelques rares cas dans lesquels le BKA sera

amené à intervenir lui-même. Personnellement, je vois d'un œil critique la coexistence des compétences du BKA et des autorités policières des Länder, notamment dans la mesure où elle conduit à des situations dans lesquels ces deux instances pourraient prendre des mesures défenses parallèles et, ce faisant, traiteraient des données personnelles à plusieurs reprises.

L'autre point crucial de mon analyse critique de cette loi concerne le respect de la vie privée. Ces dernières années, la Cour constitutionnelle fédérale a, à plusieurs reprises, ordonné au législateur de veiller à protéger les aspects fondamentaux de la vie privée dans le contexte des opérations de collecte de données, notamment en prévenant autant que possible les intrusions dans ce domaine. Par ailleurs, cette interdiction de collecter des données doit être complétée par des dispositions visant à exiger l'effacement immédiat des informations relevant de l'intimité et à prévenir leur utilisation si, dans un cas exceptionnel, ces aspects fondamentaux n'ont pas été respectés. À cet égard, la législation relative au BKA présente des écueils.

B. Jurisprudence

Arrêt de la Cour constitutionnelle fédérale quant à l'admissibilité de la fouille en ligne de systèmes télématiques

Dans son arrêt du 27 février 2008 sur les fouilles en ligne, la Cour constitutionnelle a déclaré que l'accès dérobé à des systèmes télématiques n'était admissible que dans certaines conditions très strictes. Par conséquent, certains faits doivent indiquer, dans un cas bien spécifique, qu'il existe une menace imminente pour un intérêt de premier plan protégé par la loi. Ceci inclut la vie, l'intégrité physique et la liberté des individus, et le patrimoine public dont l'exposition à une menace porte atteinte aux notions fondamentales ou à l'existence de l'État ou de personnes. En outre, le législateur doit garantir la protection des droits fondamentaux des personnes concernées en mettant en œuvre des mesures appropriées.

Au niveau fédéral, l'autorisation de fouiller les systèmes télématiques en ligne a pour la première fois été érigée au rang de règle de droit dans la loi relative à la prévention des dangers posés par le terrorisme international par l'Office fédéral d'investigation criminelle (voir point A).

Dans son arrêt susmentionné, la Cour constitutionnelle fédérale a mis en place un nouveau droit fondamental, celui-ci visant à la garantie de la confidentialité et de l'intégrité des systèmes télématiques. Ce droit – comme le droit à l'autodétermination informative élaboré dans l'arrêt de 1983 sur le recensement de la population – est une évolution particulière du droit général à la vie privée. Ce nouveau droit fondamental protège les citoyens contre les nouvelles menaces associées à l'utilisation des systèmes télématiques. Compte tenu de la rapidité du progrès technologique et des changements qui se font jour dans les conditions de vie, lesdits systèmes sont omniprésents et sont souvent devenus indispensables. L'internet en tant que réseau complexe d'ordinateurs en est un parfait exemple. L'une des conséquences de cette évolution réside dans la collecte et le traitement automatisés des données relatives au comportement et aux caractéristiques des utilisateurs, souvent à l'insu de ceux-ci. Cette collecte permet la création de profils personnels très complets. Le nouveau droit fondamental s'applique à tous les systèmes télématiques susceptibles de contenir des données à caractère personnel détaillées et significatives. Il entend protéger la confidentialité des personnes titulaires du droit à faire leurs propres choix concernant leur système, ses performances, ses fonctions et son contenu. Dans l'éventualité où des tiers seraient en mesure d'accéder à ces systèmes sans autorisation, il s'agirait d'ores et déjà d'une violation de ce droit fondamental – que l'accès aux données soit aisé ou qu'il ne soit possible que moyennant des efforts considérables.

Décisions préjudicielles de la Cour constitutionnelle fédérale concernant la législation sur la conservation des données

Le 28 octobre 2008, la Cour constitutionnelle fédérale a encore restreint l'accès des services répressifs aux données conservées au titre de 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». En mars 2008, la Cour avait déjà décidé que, dans l'attente de son arrêt définitif, les autorités compétentes ne pourraient accéder aux données de trafic conservées que si celles-ci étaient utilisées dans le cadre de la poursuite de crimes graves (p. ex. meurtres, cambriolages et chantages) énumérés à la section 100a du Code fédéral de procédure criminelle.

Plusieurs Länder ayant, au cours des douze derniers mois, adopté des textes législatifs autorisant les services de renseignement et les agences de protection civile à accéder aux données conservées dans le contexte de la prévention des dangers, la Cour a, dans son arrêt d'octobre, étendu la restriction aux possibilités offertes à ces autorités d'utiliser lesdites données.

Le tribunal administratif de Berlin exempte un fournisseur de l'obligation de conserver les données

Dans une décision préjudicielle datant du 17 octobre 2008, le tribunal administratif de Berlin a interdit à l'autorité de régulation (Agence fédérale des réseaux, Bundesnetzagentur) d'imposer une amende, par les moyens légaux à sa disposition, à un fournisseur qui refusait de se soumettre à l'obligation de conservation des données. Le tribunal a motivé cette décision en arguant qu'il n'existait pas de règles de compensation suffisantes des coûts au regard des investissements que doivent consentir les fournisseurs de télécommunications pour s'assurer des ressources technologiques et humaines nécessaires à la conservation des données. Par conséquent, le risque de préjudice financier pour le fournisseur contrebalance l'avantage que retire l'État de la possibilité d'accéder aux données conservées. Le fournisseur concerné propose essentiellement ses services à des clients commerciaux. Il est donc très peu probable que les services répressifs lui demandent des données. Dans un premier temps, cette décision n'affecte que le fournisseur à l'origine de la procédure. Plusieurs fournisseurs souhaitant obtenir une décision analogue se sont eux-mêmes pourvus devant le tribunal en vue de bénéficier d'une exemption de la conservation obligatoire des données. Entretemps, l'autorité de régulation a fait appel de la décision du tribunal administratif devant la juridiction compétente.

Le tribunal administratif de Wiesbaden décide de soumettre la question de la légalité de la directive relative à la conservation des données à la Cour européenne de justice

Le 27 février 2009, le tribunal administratif de Wiesbaden décidait de soumettre à la Cour européenne de justice, pour décision préjudicielle, la question de savoir si la directive relative à la conservation des données (2006/24/CE) était compatible avec la législation européenne. Selon le tribunal, la conservation des données va à l'encontre du droit fondamental à la protection des données. L'individu n'est pas à l'origine de l'immixtion mais peut être intimidé, même en l'absence d'un comportement répréhensible, par les risques d'abus et le sentiment d'être sous surveillance. La directive ne respecte donc pas le principe de proportionnalité garanti par l'article 8 de la convention européenne des droits de l'homme. http://www.vorratsdatenspeicherung.de/content/view/301/1/lang,de/

C. Questions diverses importantes

L'année 2008 a été marquée par la révélation de plusieurs cas graves d'infraction à la protection des données. Au début de l'année, les médias ont dévoilé que les employés d'un supermarché d'une grande chaîne de discounters étaient subrepticement surveillés. Au printemps et à l'été, les informations relatives à l'ampleur de la vente illégale d'adresses et de données bancaires se sont succédé à un rythme effréné. Une grande entreprise allemande de télécommunications était impliquée dans ce trafic à divers égards, de la surveillance des communications de grands patrons et de comités d'entreprise à des défaillances frauduleuses considérables au niveau des centres d'appel et de la protection des données. Toutefois, des guichets d'enregistrement et d'autres agences publiques étaient eux aussi mêlés à l'affaire.

Suite à cela, à la fin de l'année, le gouvernement allemand a présenté un amendement à la loi fédérale sur la protection des données (BDSG). Conformément à celui-ci, la faveur accordée au commerce des données personnelles à des fins publicitaires doit être abolie. Désormais, les personnes concernées doivent régulièrement donner leur consentement avant que l'utilisation et le transfert de leurs données à des fins publicitaires soient autorisés. Entre autres mesures, cet amendement entendait aussi introduire un audit en matière de protection des données. Selon ce projet, un label sera attribué aux entreprises qui se soumettent à des audits et respectent des exigences plus strictes en matière de protection de données (qui restent à déterminer). Concernant le projet de loi, des demandes de changements considérables portant sur certains passages ont été déposées. Ce projet est actuellement en débat au Bundestag. L'issue de ces délibérations est incertaine.

Le 14 janvier 2009, le gouvernement fédéral a adopté le projet de loi visant à renforcer la sécurité des technologies de l'information en République fédérale d'Allemagne (BR 62/09). Cette loi vise à accorder à l'Office fédéral pour la sécurité de l'information (BSI) des pouvoirs très étendus notamment dans le domaine du stockage et de l'évaluation des données relatives à l'usage et au trafic sur l'internet. Dans une résolution, la Conférence des commissaires de protection des données de l'État fédéral et des Länder a rappelé que les mesures envisagées pour renforcer la sécurité informatique ne devaient pas être mises en œuvre au détriment de la protection des données.

Par ailleurs, le 4 février 2009, le gouvernement fédéral a adopté le projet de loi concernant un portail citoyen. Ce texte visant à garantir la confidentialité, l'intégrité et l'authenticité des échanges de courriers électroniques. L'objectif fondamental des portails citoyens réside dans la création d'une infrastructure sécurisée pour les échanges de courriers électroniques (De-Mail) et le stockage des données personnelles (De-Safe) nécessaires à la communication entre citoyens et administrations, par exemple en relation avec des documents et des certificats. Il est prévu que seules les sociétés privées devraient être responsables de la mise en œuvre et du fonctionnement des services. Le commissaire fédéral pour la protection des données et la liberté de l'information (BfDI) a proposé de sécuriser les communications au moyen d'un chiffrement de bout en bout entre l'expéditeur et le destinataire. Toutefois, le stockage de données personnelles dans un coffre-fort électronique ne peut être réellement sûr que si les données sont chiffrées lors de leur stockage et que seule la personne concernée en détient la clé électronique.

Grèce

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

Nouvelle loi visant à renforcer la confidentialité des appels téléphoniques

Suite à un scandale fortement médiatisé en 2005, lorsqu'il est apparu que près de 200 téléphones portables étaient sur écoute, dont ceux du Premier ministre grec et d'autres membres du gouvernement, une nouvelle loi (loi 3674/2008) a été introduite en 2008 en vue de renforcer la confidentialité des appels téléphoniques.

Les principales dispositions de cette nouvelle loi sont les suivantes :

- Chaque fournisseur de services de télécommunications doit adopter une politique de sécurité. Toute politique de même que ses amendements/actualisations doivent être approuvés par les autorités grecques en charge de la confidentialité des communications (ADAE; cette institution n'a rien à voir avec le HDPA) et communiqués au HDPA et à l'autorité de régulation des télécommunications et des postes (EETT).
- Chaque fournisseur doit désigner un collaborateur chargé de veiller à la conformité et à la protection de la confidentialité des télécommunications. Le nom de cette personne doit être communiqué aux autorités compétentes.
- Il incombe au fournisseur de services de télécommunications de prendre toutes les mesures techniques et organisationnelles requises afin de garantir la confidentialité de toutes les communications et d'auditer régulièrement leurs systèmes et infrastructures.
- Tous les collaborateurs du fournisseur doivent respecter la confidentialité.
- Toutes les communications vocales s'effectuant par des moyens ne relevant pas du contrôle du fournisseur doivent être protégées par des techniques de chiffrement.
- Dans le cas de centres de commutation mobiles/numériques, il est obligatoire d'enregistrer toutes les opérations d'administration du logiciel de chaque centre dans des journaux de sécurité. Ces journaux doivent être enregistrés sur des supports dûment protégés, qui doivent garantir l'intégrité de ceux-ci. Tout accès direct ou indirect à ces fichiers est strictement interdit. Les modalités détaillées de la gestion de ces journaux seront fixées dans un règlement émis par l'ADAE.
- L'ADAE devrait effectuer des inspections/audits réguliers des infrastructures matérielle et logicielle du fournisseur afin de garantir la conformité avec la législation.
- Dans le cas d'une faille de sécurité ou d'un risque de faille, l'employé du fournisseur chargé de veiller à la confidentialité doit en informer le fournisseur ou le représentant légal de celui-ci, le ministère public, l'ADAE et tout abonné potentiellement concerné. Cette notification doit se faire par écrit et, si une communication directe n'est pas possible, toute autre méthode commode peut être utilisée.
- Suite à la notification de la faille, et en attendant que le ministère public et l'ADAE aient décrété des mesures spécifiques, aucun collaborateur du fournisseur ne peut divulguer d'informations concernant la faille de sécurité ou le risque de faille, et toutes les mesures qui s'imposent doivent être prises pour sécuriser les éventuelles preuves.
- Dans le cadre de cette nouvelle loi, le code pénal grec a été amendé en conséquence. Les violations de la confidentialité des appels téléphoniques, en ce compris les données de trafic et de localisation, sont considérées comme des contraventions de simple police, tandis que les preuves obtenues au travers de ces violations ne sont pas recevables dans les affaires criminelles dont sont saisis les tribunaux.
- Enfin, un plan national de sécurité devra être développé afin de protéger les communications électroniques (et non les seuls appels téléphoniques) du secteur public et les fournisseurs de réseaux et de services de communications électroniques. Les destinataires du plan de sécurité mettront les mesures en œuvre dans un délai de 6 mois. Une commission législative, au sein duquel le HDPA est également représenté, a été mise sur pied à cette fin. Toutefois, à ce jour, le gouvernement grec n'a pris aucune initiative.

Interception légale de communications électroniques dans les cas de pédopornographie

Conformément à la loi 3625/2007, le protocole facultatif à la Convention des Nations unies relative aux droits de l'enfant concernant la vente d'enfants, la prostitution

des enfants et la pédopornographie a été ratifié par le Parlement grec. En vertu de cette loi, l'article 348A du code pénal grec a été amendé de sorte la pédopornographie commise par l'intermédiaire de systèmes électroniques ou via l'internet est désormais un délit. Conformément à la loi 3666/2008 (article 2, paragraphe 7a), la liste des crimes pour lesquels une interception des communications électroniques est autorisée par la loi, a été amendée de manière à inclure la pédopornographie.

Directive 2006/24/CE
La commission législative du ministère de la justice a finalisé un projet de loi transposant la directive 2006/24/CE en droit national. Ce projet n'a pas encore été adopté par le Parlement.

B. Jurisprudence

Décision 27/2008
L'autorité hellénique chargée de la protection des données a été informée, via un article de presse, de l'installation de systèmes de vidéosurveillance dans deux écoles secondaires de la préfecture de Karditsa. Elle a jugé illégal le traitement qui était fait des données personnelles des élèves et des enseignants dans la cour et les couloirs de l'école. En effet, elle a estimé qu'un tel traitement n'était pas conforme au principe de proportionnalité, compte tenu du fait que son objectif (à savoir assurer la sécurité du site et contrôler l'accès des véhicules/tiers) pouvait être réalisé par d'autres moyens moins intrusifs.

Décision 30/2008
Suite à une plainte soumise par une personne concernée et à un audit réalisé subséquemment par le HDPA, il a été confirmé qu'une société fournissait à ses clients un service de détection de mensonges (application «Layer Voice Analysis») afin de détecter si les personnes concernées avec lesquelles elle était en contact disaient la vérité. L'autorité chargée de la protection des données a estimé que l'utilisation de cette application au cours d'un entretien téléphonique en vue de vérifier si la personne concernée mentait ou non, surtout si la personne en question n'en était pas préalablement informée, était contraire à l'article 4 de la loi 3471/2006.

Décision 48/2008
Suite à une requête de l'Institut national d'assurance sociale (NSII), le HDPA a rendu un avis dans le dossier suivant. Le directeur de cette institution a émis 330 contrats de travail liant des personnes et le NSII. Le HDPA a considéré qu'il n'était pas contraire à la loi sur la protection des données de permettre l'accès aux informations ci-dessus aux membres compétents du Parlement, et notamment aux noms et aux adresses des 330 personnes retenues pour des contrats spécifiques, ainsi que toutes les candidatures soumises à cet effet, assorties de la documentation pertinente, de manière à ce que les députés puissent vérifier la légitimité des décisions. Par ailleurs, il a été estimé que la méthode par laquelle les membres compétents du Parlement accéderaient aux données concernées devrait être arrêtée par le NSII et le Parlement. La décision du HDPA reposait sur l'idée selon laquelle l'accès des députés compétents aux données susmentionnées était nécessaire aux fins du contrôle parlementaire, lequel vise à vérifier, après examen des qualifications des candidats retenus et exclus, si les personnes sélectionnées sont les plus qualifiées pour conclure un contrat de travail avec le NSII.

Décision 50/2008
Suite à une requête émanant d'un ancien résident d'orphelinat, le HDPA a statué que l'adulte adopté pouvait recevoir légalement les données personnelles de ses parents biologiques, conservées dans le dossier d'adoption, dans le but de les retrouver. Ceci comprend toutes les informations relatives à l'identité des parents biologiques ainsi que toute autre information susceptible d'aider la personne adoptée à retrouver ses parents.

Décision 52/2008
Le HDPA a reçu une requête d'une banque d'investissement concernant l'octroi d'une autorisation pour l'installation et l'utilisation d'un système biométrique ayant recours aux empreintes digitales des collaborateurs pour contrôler l'accès à des applications électroniques spécifiques de la banque. Le HDPA a décidé, par un vote majoritaire, que ce traitement spécifique des données n'était en principe pas contraire aux dispositions de la loi 2472/1997, puisqu'il visait exclusivement le contrôle d'accès de certains employés exécutant des transactions sur des sommes colossales. Le HDPA a statué que lorsque le traitement visait l'exécution sûre de transactions

et la prévention du blanchiment d'argent ou d'autres opérations illégales, il était légal. Il a également décidé que ce traitement particulier n'allait pas à l'encontre du principe de proportionnalité pour les motifs suivants: a) le système en question est destiné à être utilisé dans un environnement appliquant des normes de sécurité très strictes, pour des applications de transactions financières spécifiques, et le pourcentage des employés qui utilisera ce système est proportionnel (en d'autres termes, il est réduit) à l'immixtion que ce traitement causera dans la vie privée des employés; b) le système est proportionné pour les affaires de la banque en question, qui concernent essentiellement les activités d'investissement de compagnies maritimes; et c) le fonctionnement du système sert les employés eux-mêmes, puisqu'il dissuade les usurpations d'identité tout en garantissant la transparence en cas d'erreur ou de malveillance.

Décision 66/2008

Une personne concernée a introduit auprès du HDPA une plainte à l'encontre d'une banque pour non-respect du droit d'accès à ses données. Le HDPA a statué que le responsable des données n'est pas en droit d'annoncer à la personne concernée qu'une enquête a été ouverte à son encontre concernant le blanchiment de fonds issus d'une activité criminelle ou que les informations liées à la conclusion de l'enquête ont été transmises à la commission chargée d'évaluer et d'examiner lesdites informations (article 31 de la loi 3691/08). Toutefois, la restriction du droit d'accès de la personne concernée cesse si la banque ne transmet pas les données et informations collectées à la commission compétente après avoir estimé que lesdites informations ne constituent pas une preuve du blanchiment. Par ailleurs, si les données personnelles appartenant à un tiers ont également été traitées par le responsable, affectant la manière dont la personne concernée a été traitée, lesdites données sont également réputées concerner celle-ci et elle a donc le droit d'y accéder.

Hongrie

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

Directive 95/46/CE
Néant.

Directive 2002/58/CE
Les règles générales régissant la publicité électronique ont été considérablement modifiées. Selon la loi XLIII de 2008 relative aux critères et aux restrictions applicables aux activités de publicité commerciale, *«la publicité adressée aux personnes physiques, et notamment aux destinataires d'activités de marketing direct, ne peut être envoyée par courrier électronique ou au moyen de n'importe quel outil équivalent que si le destinataire a expressément et préalablement consenti»* à recevoir de telles publicités. Dans ces cas, l'autorité nationale de communication est compétente pour les procédures de surveillance et est habilitée à décider si la communication électronique en question est ou non une publicité et si son envoi est contraire à la loi. Le principal amendement réside dans le fait que les restrictions ne s'appliquent qu'aux publicités envoyées aux personnes physiques. Les données n'appartenant pas à des personnes physiques ne bénéficient pas d'une protection aussi stricte.

B. Jurisprudence

En 2006, une organisation civile a demandé au commissaire d'ouvrir une enquête à l'encontre de Philip Morris Hungary Ltd. concernant le traitement réservé aux données personnelles dans le cadre d'une campagne de marketing direct, p. ex. par la collecte de points. Les données personnelles collectées étaient également utilisées pour envoyer des brochures d'information personnalisées relatives à des produits du tabac. Le commissaire a demandé un avis à l'autorité hongroise en charge de la concurrence, afin de déterminer si de telles méthodes de marketing direct pouvaient être considérées comme de la publicité pour les produits du tabac.

Selon la section 13, paragraphes (1) et (2) de la loi LVIII de 1997 sur les activités de publicité commerciale, «*il est interdit de faire la publicité du tabac et des produits du tabac, directement ou indirectement*». S'appuyant sur l'avis de l'autorité de la concurrence, le commissaire est parvenu à la conclusion que les données personnelles ne pouvaient pas être collectées puis utilisées dans le but d'envoyer des brochures personnalisées relatives aux produits du tabac, même avec l'accord de la personne concernée. Le commissaire a donc conseillé au responsable du traitement des données de mettre un terme à l'opération et a exigé, par voie de résolution, que les données traitées illégalement soient bloquées, effacées ou détruites.

Il est impossible de faire appel de cette résolution par les canaux administratifs. Philip Morris Hungary Ltd. a donc porté l'affaire devant les tribunaux compétents. Ceux-ci ont conclu que «le destinataire ayant lui-même demandé que les informations lui soient envoyées dans une enveloppe scellée, celles-ci ne peuvent pas être considérées comme de la publicité». Compte tenu de cette décision, le commissaire a révoqué sa résolution, et le tribunal a rendu une ordonnance de non-lieu. Par la suite, la loi XLIII de 2008 relative aux critères et restrictions applicables aux activités de publicité commerciale est entrée en vigueur.

À la lumière de la nouvelle loi, le commissaire a jugé nécessaire de rouvrir l'affaire et d'examiner l'activité de traitement des données. Selon la nouvelle loi, les informations envoyées sans équivoque au destinataire sont considérées comme de la publicité interdite pour un produit du tabac. De ce fait, les données collectées sont traitées d'une manière incompatible avec les objectifs spécifiés, explicites et légitimes. Le commissaire a donc interdit ladite activité de traitement par voie de résolution. Cette fois, Philip Morris Hungary Ltd. n'a pas fait appel de la décision.

C. Questions diverses importantes

Le commissaire a émis un avis en relation avec un décret du ministère des finances visant à réguler les tests d'aptitude psychologique préalables à l'exercice du service civil à l'administration hongroise de contrôle financier et fiscal (APEH). Selon ce décret, les personnes sous traitement psychiatrique ou potentiellement atteintes de troubles psychiatriques entravant leur adaptation, leur intégration dans l'entité ou leur efficacité au sein de

l'entité ne peuvent occuper un poste au sein de celle-ci. Le commissaire a indiqué que certaines catégories de données, dont les données relatives à l'état de santé, ne peuvent être traitées – si la loi l'exige – que moyennant le consentement écrit de la personne concernée. Toutefois, la base légale n'autorise pas, en soi, le traitement de ces données; d'autres critères doivent aussi être rencontrés, et plus particulièrement la limitation des finalités. Le fait qu'une personne a reçu un traitement psychiatrique ne signifie pas forcément qu'en occupant un poste, elle influencerait ou mettrait en péril la légalité des activités de l'entité. Il a aussi souligné que si une personne ne peut exercer un emploi du fait d'une maladie probable, c'est sa dignité humaine qui est compromise. Les dispositions du décret en question peuvent conduire à une discrimination, ce qui est clairement contraire à la constitution hongroise ainsi qu'aux dispositions de la loi CXXV de 2003 sur l'égalité de traitement et l'égalité des chances. Il a encore rappelé qu'un tel décret ministériel ne peut, en tant que source de loi, fournir les bases juridiques du traitement des données. Seule une loi adoptée par l'Assemblée nationale le peut. Le commissaire a donc demandé au ministre des finances d'abroger ce décret.

Dans un autre dossier, le commissaire a examiné l'activité de traitement des données d'une société multinationale exploitant des systèmes GPS. Ceux-ci étaient utilisés dans les véhicules de la société par les collaborateurs ayant un emploi du temps flexible, condition pour l'utilisation de la géolocalisation. Toutefois, aucune différence n'était faite entre les données collectées pendant et en dehors des heures de travail, ce qui signifie que l'entreprise traitait des données personnelles sans le consentement de la personne concernée. Le traitement n'était pas non plus conforme au principe de la limitation des finalités, puisque les données de géolocalisation étaient aussi enregistrées en dehors des heures de travail. Dans son avis, le commissaire a exprimé l'opinion selon laquelle les systèmes GPS ne peuvent transmettre des données que pendant les heures de travail. Les données personnelles «hors travail» ne peuvent être traitées par l'employeur. Pour que le traitement soit légal, les employés devraient avoir la possibilité de désactiver la balise GPS lorsqu'ils utilisent le véhicule à des fins privées.

En octobre, le commissaire a reçu le projet de loi concernant la mise en place du système central de notification des crédits. À cet égard, le commissaire a fait savoir qu'il était opposé à l'introduction d'une «liste positive».

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 2008 ayant eu une incidence significative sur la protection des données en Irlande, il convient de mentionner de nouvelles réglementations visant à transposer la directive «vie privée et communications électroniques» (2002/58/CE) en Irlande. Ces nouvelles réglementations renforcent les pénalités applicables aux délits en matière de communications non sollicitées et veillent à ce que la charge de la preuve du consentement de l'abonné incombe au défendeur.

La directive 2006/24/CE sur la conservation des données générées et traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public (amendant la directive 2002/58/CE) n'avait pas encore été transposée dans le droit irlandais fin 2008. Une loi à cet effet devrait être adoptée au Parlement dans le courant de l'année 2009.

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 ni à des mesures coercitives. À titre de règlement à l'amiable, le responsable du traitement des données peut, par exemple, offrir une contribution financière à la personne concernée ou à un organisme caritatif approprié. Si nécessaire, 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. Dans le courant de l'année 2008, le commissaire a été impliqué dans des procédures judiciaires en relation avec les droits des personnes concernées en vertu des lois de 1998 et de 2003 sur la protection des données et du Statutory Instrument 535 de 2003 (mise en œuvre de la directive 2002/53/CE en Irlande). En voici quelques exemples:

Appel contre un ordre du commissaire visant à faire effacer des données
En novembre 2008, le tribunal d'arrondissement de Dublin a jugé recevable un recours introduit par un responsable du traitement des données à l'encontre d'un ordre exécutoire émanant du commissaire au titre de l'article 10 des lois de 1988 et de 2003 sur la protection des données (portant transposition des pouvoirs de l'autorité de contrôle à ordonner l'effacement de données, définis à l'article 28 de la directive 95/46/CE). L'affaire en question portait sur certains enregistrements relatifs à un traitement psychiatrique que le responsable du traitement des données avait conservé. Conformément à la section 6A des lois sur la protection des données [portant transposition de l'article 14 (a) de la directive], la personne concernée avait demandé l'effacement de ces enregistrements au motif de la souffrance causée par leur conservation. La demande a été refusée par le responsable du traitement des données. Le commissaire a conclu que la personne concernée avait des motifs justifiables plus impérieux que les arguments avancés par le responsable du traitement des données pour la conservation de celles-ci. En conséquence de quoi, le commissaire a ordonné l'effacement des données. Le responsable du traitement des données a fait appel de cette décision, et cet appel a été jugé recevable.

Le commissaire obtient gain de cause dans le cadre d'un appel contre un avis juridique d'information
Le commissaire a obtenu gain de cause dans le cadre d'un recours introduit devant les tribunaux par un journal. Ce dernier protestait contre un avis juridique émis en relation avec une enquête portant sur son refus de permettre un citoyen d'accéder à des informations le concernant. Le journal arguait que l'exemption prévue à la section 22A des lois irlandaises sur la protection des données (portant transposition de l'article 9 de la directive) n'exigeait pas de lui qu'il fournisse des informations suite à cet avis. Il avançait que fournir de telles informations saperait l'exemption prévue par la section 22A. Le tribunal a rejeté l'appel au motif que l'exemption ne s'appliquait pas aux prérogatives d'inspection conférées au commissaire par les sections 10 et 12 des lois sur la protection des données.

Poursuites pour l'envoi de messages textuels (SMS) non sollicités – coopération avec le superviseur de la protection des données de l'île de Man

Suite à des plaintes concernant l'envoi de SMS non sollicités, le bureau a ouvert une enquête sur une société basée en dehors de la juridiction de l'Irlande (sur l'île de Man). Cette société avait toutefois du personnel à Dublin et utilisait une infrastructure technique implantée en Irlande pour envoyer les messages. Une équipe du bureau a collecté des preuves au cours d'une inspection sur site. D'autres éléments probants ont été collectés dans la juridiction de l'île de Man avec l'aide du superviseur de la protection des données de celle-ci. Des poursuites pour violation du *Statutory Instrument* 535 de 2003 (qui met en œuvre la directive 2002/58/CE en Irlande) ont été lancées en novembre 2008. Le tribunal a infligé des amendes à la société concernée, après que celle-ci a plaidé coupable et admis que rien ne lui permettait d'affirmer que les utilisateurs des numéros de téléphone portable concernés avaient valablement consenti à recevoir des SMS publicitaires.

Poursuites pour inobservance du pouvoir d'accès aux données du commissaire

Après avoir tenté à plusieurs reprises d'obtenir des informations de la part d'une entreprise publique dans le cadre de l'investigation d'une plainte, le bureau a émis un avis d'information à l'encontre de la société l'enjoignant de coopérer en communiquant les données nécessaires à l'exercice de ses obligatoires légales. La société n'ayant pas fourni les informations demandées dans le délai de vingt et un jour dont elle disposait pour se conformer à cet avis, le bureau a entamé des poursuites à son encontre en juin 2008. La société, qui plaidait non coupable, a été condamnée et mise à l'amende. C'était la première fois que le bureau se voyait contraint de poursuivre une entité pour inobservance d'un avis émis en relation avec le pouvoir d'accès aux données du commissaire.

C. Questions diverses importantes

Comme nous le mentionnions dans le rapport de l'année dernière, à la suite d'un grand nombre de plaintes reçues au sujet de certaines entreprises actives dans le secteur du marketing par SMS, en 2007, le bureau 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. Suite à ces inspections, des procédures ont été ouvertes à l'encontre de plusieurs sociétés. L'une d'entre elles a contesté la base juridique de ces poursuites, contestation qui a été rejetée par la Haute Cour. Le bureau va donc maintenir ses poursuites.

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).

Nouvelle législation

Transposition de la directive 2006/24/CE: la législation relative à la conservation des données de trafic a été modifiée par la contribution de l'autorité de protection des données en vue de transposer la directive 2006/24/CE. Actuellement, les données de trafic peuvent être conservées pendant vingt-quatre mois (trafic téléphonique) et douze mois (communications électroniques) aux fins de la répression de la criminalité – et ce, quel que soit le délit concerné. Les amendements législatifs apportés ont précisé plus avant le rôle de l'autorité italienne de protection des données à cet égard et ont introduit des sanctions spécifiques en cas de non-respect des exigences en matière de conservation des données de trafic (section 162 *bis* du Code de protection des données).

Exigences simplifiées s'appliquant aux mesures de sécurité et aux notifications: des dispositions simplifiées ont été introduites en 2008 concernant certaines exigences que doivent respecter les travailleurs indépendants et PME (y compris les artisans) en matière de protection des données. Ainsi, certaines dispositions du Code de protection des données ont été modifiées en vue d'éliminer des procédures lourdes liées, pour l'essentiel, à l'adoption de mesures de sécurité minimales. Les mécanismes permettant de notifier certaines opérations de traitement à l'autorité italienne de protection des données ont aussi été simplifiées plus avant, les informations à inclure dans le formulaire de notification (conformément à l'article 17 de la directive 95/46/CE) étant désormais précisées. Par ailleurs, des décisions spécifiques ont été prises par l'autorité de protection des données en vue de contribuer à cet exercice de simplification dont le but est de garantir le respect des droits des individus (voir ci-dessous).

Flux de données transnationaux: parmi les grandes innovations réglementaires adoptées, citons les nouvelles dispositions adoptées en matière de flux de données transnationaux à destination de pays tiers. Faisant suite à une requête soumise par l'autorité italienne de protection des données au Parlement, un libellé faisant expressément référence à l'usage de règles d'entreprise contraignantes en la matière a été ajouté au Code de protection des données. En conséquence, la section 44 du Code de protection des données dispose désormais que les transferts de données à destination de pays tiers sont autorisés pour autant que l'autorité de protection des données les aient approuvés et qu'ils soient assortis des garanties adéquates pour les droits des personnes concernées «telles que déterminées par le Garante, notamment dans le cadre de clauses de sauvegarde contractuelles ou par l'entremise de règles de conduite applicables à l'ensemble des sociétés appartenant à un même groupe.»

Sanctions: des modifications significatives ont été apportées eu égard aux sanctions que l'autorité italienne de protection des données est en droit d'imposer. Lesdits amendements, qui élargissent considérablement les pouvoirs dont dispose l'autorité, portent essentiellement sur les sanctions administratives, les peines criminelles envisagées par le Code de protection des données étant restées sensiblement les mêmes. Globalement, les amendements apportés étaient les suivants: a) augmentation des amendes en cas d'infractions; b) introduction de nouvelles catégories de comportements répréhensibles; c) introduction de mécanismes permettant de mieux adapter les sanctions aux circonstances, selon la gravité de l'infraction, l'importance et/ou la taille de la base de données affectée par la violation, l'implication d'un grand nombre de personnes concernées et la situation financière du contrevenant.

Durée du mandat des membres des autorités de contrôle indépendantes: dans l'attente d'un texte législatif destiné à rationnaliser les réglementations applicables aux autorités de contrôle indépendantes, le Parlement a harmonisé la durée du mandat de tous les membres/commissaires desdites autorités, qui a été fixé à sept ans, non renouvelables.

Convention sur la cybercriminalité: l'Italie a ratifié la Convention sur la cybercriminalité adoptée en 2001 par le Conseil de l'Europe. L'instrument de ratification ne comprenait pas de clause générale à incorporer dans les règles de procédure judiciaire afin de garantir une protection adéquate des droits de l'homme, et plus particulièrement du «principe de proportionnalité» prévu par l'article 15 de la Convention. Cette exigence a été soulignée par l'autorité italienne de protection des données, notamment eu égard à l'avis rendu par le groupe de travail «Article 29» sur le projet de Convention; notre autorité de protection des données a donc suggéré qu'une clause *ad hoc* soit ajoutée à chaque disposition légale régissant les activités d'investigation et de préparation des procédures judiciaires, en vertu de laquelle toute investigation ou procédure entamée par les autorités judiciaires et/ou policières compétentes doit prendre en compte la pertinence des données examinées, veiller à ce que l'ampleur de celles-ci ne soit pas excessive et faire en sorte que les mesures prises soient proportionnées. L'instrument de ratification a également modifié les dispositions relatives aux données de trafic (section 132 du Code de protection des données) en permettant aux autorités policières, dans certaines circonstances, d'ordonner aux fournisseurs de services informatiques et/ou internet de conserver et de protéger les données relatives au trafic sur l'internet, à l'exclusion des données de contenu, pour une période maximale de 90 jours, afin d'effectuer des devoirs d'instruction ou en vue de détecter et de réprimer des délits spécifiques. Cet ordre de police doit être notifié au ministère public et validé par celui-ci.

Utilisation des répertoires d'abonnés au téléphone à des fins de publicité: un décret gouvernemental a introduit une dérogation provisoire à la législation en vigueur applicables aux répertoires d'abonnés au téléphone. Celle-ci dispose que le traitement des données contenues dans lesdits répertoires à des fins de publicité et/ou de marketing n'est autorisé que moyennant le consentement libre, préalable, éclairé et spécifique des personnes concernées. Cette dérogation a été reçue défavorablement par l'autorité italienne de protection des données, car elle empiète sur les garanties auxquelles elle avait donné corps, notamment, par diverses mesures et dispositions. Ces nouvelles dispositions permettent d'utiliser légalement à des fins de publicité les données personnelles contenues dans des bases de données élaborées sur la base de répertoires d'abonnés au téléphone compilés avant le 1er août 2005. Cette autorisation s'applique jusqu'au 31 décembre 2009 et ne concerne que les responsables des données, les bases de données ayant été compilées avant le 1er août 2005.

Vidéosurveillance dans les copropriétés: l'autorité italienne de protection des données a attiré l'attention du Parlement et du gouvernement sur le fait qu'il serait judicieux d'adopter une législation régissant certaines questions en relation avec le traitement des données personnelles résultant du développement d'équipements de vidéosurveillance dans les copropriétés. L'autorité est plus particulièrement en faveur d'une régulation des processus décisionnels ayant trait à l'installation de caméras vidéo dans les copropriétés ainsi que du nombre de votes de locataires requis pour approuver une telle décision.

Auditions parlementaires: l'autorité de protection des données a été entendue à plusieurs reprises en 2008 sur des questions de première importance par les commissions parlementaires concernées, soit dans le cadre d'initiatives d'information, soit lors des débats conduisant à l'adoption de lois affectant la protection des données à caractère personnel. Ainsi, l'autorité a notamment été entendue sur des questions abordées par la commission de la justice de la Chambre des députés (Chambre basse) dans le contexte d'une audition sur le projet de loi du gouvernement visant à réformer la législation relative à l'interception des communications. L'autorité a également apporté sa contribution aux débats portant sur le traitement des données du registre des contribuables et l'accès à celles-ci lors d'une audition tenue par la commission bicamérale compétente en la matière. À cet égard, référence peut également être faite à deux auditions informelles sur des questions relatives au secteur de l'assurance et sur des projets de loi concernant

l'introduction d'un système de prévention des fraudes dans le secteur du crédit à la consommation.

B. Jurisprudence

Responsabilité pénale d'un journaliste ayant publié des informations sur la santé d'un enfant. La Cour de cassation italienne (plus haute instance judiciaire du pays) a statué qu'un journaliste et le directeur d'une publication hebdomadaire étaient responsables au pénal pour avoir publié des informations sur la santé de la petite fille d'un présentateur très connu. La Cour de cassation a appliqué les sanctions pénales prévues en cas d'infraction au Code de conduite des journalistes annexés au Code de protection des données. Cet arrêt a confirmé le statut juridique particulier dudit code de conduite, puisque, conformément à la législation italienne, la conformité du traitement de données personnelles au code de protection des données est une condition *sine qua non* à sa légalité.

La saisie conservatoire de photos affectant la vie privée est légale. La Cour de cassation a statué qu'un tribunal avait légitimement ordonné la saisie conservatoire de photos et de négatifs conservés dans les locaux éditoriaux d'un journal (arrêt n° 17408/2008) et sur lesquels figurait un homme politique connu dans le parc de sa villa. La question avait préalablement été soulevée devant l'autorité italienne de protection des données, qui avait estimé que la publication de ces photos prises par le biais de méthodes intrusives avait violé la législation relative à la vie privée et avait donc interdit toute nouvelle publication desdites photos. La Cour de cassation a statué que la saisie ordonnée ultérieurement par un tribunal à l'encontre d'un autre journal qui avait à son tour publié les photos en dépit de l'interdiction de l'autorité, était légale. La Cour a estimé qu'il y avait là une violation de la vie privée de la personne concernée, conformément à l'avis émis par l'autorité italienne de protection des données, étant donné que les photos en question révélaient la vie privée de cet homme politique contre son gré, à son domicile, et avaient été prises de manière intrusive, au moyen d'un équipement technique spécifique.

Procédures de faillite et casiers judiciaires. La Cour de cassation a statué que, conformément à la législation récemment adoptée sur les procédures de faillite (décret n° 5/2006), toute référence à la déclaration de faillite doit être effacée des certificats émis par le bureau du casier judiciaire à la demande de la personne concernée (à savoir du failli) au terme de la procédure de faillite/liquidation, compte tenu du fait que le décret en question rejetait explicitement les dispositions relatives à la réhabilitation des faillis (décision n° 40675/2008).

C. Questions diverses importantes

Sécurité garantie pour les bases de données publiques et privées

Traitement des données de trafic par les fournisseurs de services de téléphonie et internet: L'autorité italienne de protection des données a adopté une disposition générale (datée du 17 janvier 2008), conformément à la section 132 du Code italien de respect de la vie privée, concernant le stockage et le traitement des données de trafic générées par les fournisseurs de services de téléphonie et internet. Celle-ci visait à garantir une sécurité accrue eu égard aux données de trafic conservées par les fournisseurs pour des raisons légales (et notamment à des fins de répression de la criminalité).

Les mesures développées par le Garante précisent qui doit conserver quelles données et définissent des dispositions techniques et organisationnelles afin de garantir un stockage sécurisé des données en question.

Il indique notamment que les fournisseurs de contenus internet, les gestionnaires de moteurs de recherche, les organisations et organismes publics mettant des réseaux téléphoniques et internet à la disposition de leur personnel et/ou utilisant des serveurs mis à disposition par d'autres entités, les cybercafés et autres établissements analogues sortent du champ d'application des obligations de conservation fixées – conformément aux définitions exposées dans la direction 2002/22/CE sur le service universel ainsi que dans les directives 2002/58/CE et 2006/24/CE. Plusieurs mesures techniques ont été définies afin de protéger les données, dont de robustes procédures d'authentification, biométriques et autres, un audit approfondi des bases de données et systèmes informatiques, le chiffrement de bases de données, la collecte centralisée et sécurisée de fichiers journaux et des mesures de sécurité physiques destinées à protéger les salles informatiques et centres de données.

Sans préjudice des amendements réglementaires décrits ci-dessus, les opérateurs de télécommunications devront mettre en œuvre lesdites mesures avant le 30 avril 2009.

Cette prolongation de délai a été accordée par l'autorité italienne de protection des données suite, notamment, aux requêtes formulées en juillet par les associations professionnelles de fournisseurs de services de communications électroniques demandant un délai de transition supplémentaire afin de pouvoir mettre pleinement en œuvre les mesures de sécurité complexes en question.

Administrateurs système: l'autorité italienne de protection des données a jugé nécessaire de prendre des mesures spécifiques vis-à-vis des «administrateurs système» en vue de souligner leur importance dans le contexte du traitement des données personnelles et de sensibiliser tant les responsables du traitement que le grand public à la sensibilité des tâches dont ils s'acquittent. Dans le contexte des inspections effectuées par l'autorité italienne de protection des données ces dernières années, il serait souhaitable que la plupart des entreprises et grandes organisations publiques et privées accordent une grande importance aux administrateurs système, quoi que cela ne soit pas toujours le cas, le risque étant de sous-estimer les conséquences résultant d'activités non contrôlées desdits administrateurs, qui sont également censés surveiller et contrôler l'usage des systèmes informatiques. En conséquence, un appel a été lancé à tous les responsables d'opérations de traitement effectuées, en tout en partie, à l'aide d'outils électroniques afin qu'ils tiennent compte de la nécessité de considérer les risques et niveaux de criticité liés aux tâches confiées aux administrateurs système. Parallèlement, un premier train de mesures organisationnelles a été défini afin de sensibiliser les organismes et organisations publics et privés à l'existence de certaines fonctions techniques, aux responsabilités qu'impliquent lesdites fonctions et, dans certains cas, à l'identité des personnes actives en tant qu'administrateurs système pour les divers services et bases de données pris en ligne de compte. Parmi lesdites mesures, citons, à titre d'exemples, la nécessité de soigneusement évaluer les qualifications personnelles des candidats, la désignation individuelle de chaque administrateur système, la gestion d'une liste des administrateurs système existants (surtout lorsque ceux-ci ont à traiter des données relatives aux ressources humaines), la fourniture des informations pertinentes aux personnes concernées et au personnel, ainsi que la garantie de ce que des systèmes sont mis en place pour consigner l'accès (via authentification informatique) des administrateurs système aux systèmes de traitement et aux bases de données.

Données fiscales et vie privée

Diffusion des données des déclarations fiscales via l'internet par le bureau de perception italien: l'autorité italienne de protection des données a interdit au bureau de perception italien de poster les déclarations fiscales de tous les Italiens sur l'internet quelques jours après la publication des données sur le site internet dudit bureau. Elle a estimé que la diffusion des données était contraire à la législation sectorielle qui autorise le recours à différents mécanismes moins intrusifs pour obtenir des informations sur les revenus des contribuables. Elle a aussi jugé que la publication des données sur l'internet était disproportionnée par rapport à l'objectif consistant à rendre disponibles les informations en question.

Les conséquences résultant de cette divulgation globale, non filtrée, des données concernant tous les contribuables italiens étaient légions. Un nombre considérable d'internautes en Italie et à l'étranger ont pu accéder à une grande quantité de données en l'espace de quelques heures, celles-ci étant disponibles au travers d'une source unique. Ils ont eu l'occasion de copier les données, de créer leurs propres bases de données, de modifier et/ou de traiter les données, de créer des listes de profils et de faire circuler les données avec tous les risques que l'on imagine.

Par ailleurs, il a pu être établi que le bureau de perception avait négligé de demander l'avis de l'autorité italienne de protection des données – obligatoire en vertu de la loi – avant de décider de publier les données sur l'internet.

Registre des contribuables: une décision adoptée en septembre 2008 faisait le point sur les risques identifiés par l'autorité italienne de protection des données après plusieurs inspections effectuées en relation avec le registre des contribuables (qui contient les fiches de

plusieurs millions de contribuables italiens et auquel un nombre considérable d'utilisateurs, dont des organismes publics et privés, peut accéder à l'aide de différents outils) et exposait les mesures technologiques et organisationnelles requises pour renforcer la sécurité de l'accès et rendre le traitement des données conforme à la législation de protection des données. Compte tenu du fait que les principaux risques étaient associés à l'absence d'informations sur le nombre global d'utilisateurs disposant d'un accès à ces données, à une surveillance insuffisante des accès et de l'utilisation inappropriée des mots de passe et noms d'utilisateurs et à des mesures technologiques inadéquates pour assurer la sécurité des données, l'autorité italienne de protection des données a exigé une surveillance régulière des organismes et organisations disposant d'un droit d'accès, une analyse de tous les flux de données à destination et au départ du registre, et notamment des informations détaillées relatives aux entités à même d'accéder aux registres, des bases juridiques applicables, de la nature et du type de données transférées, le partitionnement des données accessibles afin de garantir que l'utilisateur ne puisse consulter que les seules données auxquelles il a accès, la mise en place de systèmes d'alerte destinés à détecter et à prévenir les failles de sécurité, l'application de mécanismes d'authentification (avancés), la consignation des accès, la restriction du nombre maximal d'accès simultanés, la mise en œuvre de canaux de connexion sécurisés en cas de gestion des flux de données sur le web, ainsi que la désactivation opportune des utilisateurs qui ne sont plus habilités à accéder aux données en question.

Mesures de simplification

Comme nous l'avons déjà indiqué, l'exercice de simplification relatif à certaines exigences en matière de protection des données s'est poursuivi tout au long de l'année 2008, avec la contribution de l'autorité italienne de protection des données. Les modalités pratiques de celui-ci ont été fixées dans une décision émise au début de l'année afin d'encore faciliter les opérations de gestion et de comptabilité standard, tant dans le secteur public que privé, surtout lorsqu'aucune donnée sensible ou judiciaire n'est traitée. Pour ce faire, des mécanismes simplifiés ont été arrêtés quant aux obligations d'information des personnes concernées, sans pour autant mettre en péril le degré de protection garanti par la loi. Par ailleurs, les responsables du traitement des données ont été invités à ne pas demander le consentement des personnes concernées s'ils ne traitent les données personnelles qu'à des fins de gestion et/ou de comptabilité standard, y compris dans le cadre de l'exécution d'obligations contractuelles, précontractuelles ou réglementaires. Conformément au principe de l'équilibrage des intérêts et aux circonstances spécifiques, l'autorité de protection des données a décidé que les responsables du traitement dans le secteur privé étaient autorisés à utiliser les adresses électroniques communiquées par les personnes concernées auxquelles ils doivent fournir un produit et/ou un service sans le consentement explicite desdites personnes, dans le cadre de leurs opérations de gestion et/ou de comptabilité standard, pour autant que le courrier consiste à envoyer directement leurs propres matériels publicitaires et/ou commerciaux, à réaliser leurs propres études de marché et/ou à transmettre leurs propres communications commerciales. Dans une autre décision, l'autorité italienne de protection des données a fixé les modalités simplifiées destinées à mettre en œuvre des mesures de sécurité minimales concernant certaines catégories de traitement des données. Celles-ci avaient pour but – conformément aux dispositions déjà définies dans la législation de simplification (voir ci-dessus) – de garantir un niveau de sécurité adéquat en tenant compte des caractéristiques propres aux PME et aux opérations de traitement aux seules fins de la gestion et/ou de la comptabilité.

Soins de santé et données sensibles

Orientations pour le traitement des données dans le cadre des essais cliniques de médicaments: ces orientations ont été publiées en 2008 afin de vérifier les garanties que doivent fournir les responsables du traitement lorsqu'ils traitent les données personnelles liées aux patients participant à des essais cliniques de médicaments. Une consultation publique a ensuite été lancée concernant ces orientations. Ces orientations exigent, notamment, que les données et échantillons biologiques soient conservés pendant une période plus courte, qu'une distinction plus claire soit établie entre consentir à un traitement médical et consentir au traitement de données personnelles, qu'une clause spécifique soit formulée en vue d'obtenir le consentement des patients pour qu'ils puissent faire entendre leur voix en tant que personnes concernées, notamment dans le cadre des

opérations de traitement effectuées par d'autres entités qui collaborent à la recherche en question, peut-être à l'étranger, et que des mesures de sécurité plus strictes soient adoptées. L'autorité de protection des données a également rédigé une note d'information modèle qui peut être utilisée par les compagnies pharmaceutiques qui soutiennent les études en vue d'informer les patients sur le traitement de leurs données par les centres de test. Les mesures de sécurité ont été renforcées, surtout dans le contexte des transferts de données électroniques; des procédures d'authentification obligatoires pour l'accès aux données ont été spécifiées, de même que pour l'utilisation de systèmes de stockage et d'archivage basés sur des protocoles de chiffrement et de communication sécurisés pour transférer les données entre les centres de test, la base de données de la compagnie pharmaceutique et les contrôleurs de l'étude.

Lutte contre le dopage: suite à un rapport soumis par l'association italienne des coureurs cyclistes professionnels (ACCPI), qui se plaignait à l'autorité italienne de protection des données du fait que les règlements appliqués par le Comité olympique italien (CONI) afin d'effectuer les contrôles antidopage hors périodes de compétition étaient contraires à la législation italienne en matière de protection de la vie privée, l'autorité a rendu une décision concernant le traitement des données personnelles dans le domaine de la lutte contre le dopage. Dans celle-ci, l'autorité soulignait que le traitement des données personnelles par le CONI, organisme public, devait être conforme à la législation en vigueur et tenir compte des instruments internationaux pertinents. Elle a dès lors ordonné au CONI de modifier la note utilisée pour informer les personnes concernées (athlètes) en vue de fournir des informations spécifiques sur les données à mettre à disposition, en précisant si cette communication se fait à titre obligatoire ou facultatif et quelles sont les conséquences d'une non-communication desdites données, notamment concernant les informations géographiques détaillées. Par ailleurs, la portée de la communication des données en question devait être clarifiée en précisant les (catégories de) destinataires et le transfert ou non des données à l'étranger.

Justice

Les travaux visant à garantir le respect des principes de protection des données en relation avec les activités judiciaires se sont poursuivis en 2008. Dans ce cadre, l'autorité de protection des données a adopté des «orientations sur le traitement des données par les experts auprès des tribunaux». Celles-ci précisent les obligations que doivent respecter ces professionnels lorsqu'ils ont à traiter d'importants volumes de données personnelles dans le cadre de procédures judiciaires. Le «Code de pratique applicable aux enquêtes à décharge par les conseils juridiques et détectives privés» a également été adopté en 2008. Ce code définit les garanties que doivent fournir les conseils juridiques et détectives privés lorsqu'ils traitent les données personnelles de leurs clients – depuis la préparation de l'action jusqu'à la phase qui suit le procès. Plus particulièrement, ce Code fixe des modalités simplifiées en relation avec les notes d'information, des mesures techniques et organisationnelles strictes en vue de protéger les données et une période de conservation limitée applicable aux informations collectées aux fins déjà évoquées.

Informations commerciales

L'autorité de protection des données a arrêté une décision quant au traitement des données effectué par une entreprise qui gérait des bases de données propres générées en extrayant des informations d'autres systèmes de classement (mis sur pied par des entités publiques et privées) en vue de fournir à ses clients – pour l'essentiel des professionnels du monde des affaires tels que des banques, des sociétés financières, des entreprises et agences d'information – des services de renseignement axés sur des informations «commerciales» relatives aux entités cibles données (autres entreprises, professionnels, etc.). Dans une décision datée du 30 octobre 2008, l'autorité ordonnait à l'entreprise en question de prendre toutes les mesures requises et appropriées pour protéger les personnes concernées et veiller à: a) empêcher que des informations qui ne permettent pas de tracer directement la personne concernée, parce que liées à des événements concernant d'autres entités, soient mises en relation avec ladite personne; b) établir une distinction entre les cas où, sur la base des informations disponibles, aucun lien entre un élément préjudiciel et l'entité cible n'est identifié et ceux où le taux de fiabilité commerciale a été jugé «faible». Par ailleurs, l'autorité a interdit à la société: a) d'utiliser des informations non pertinentes et, dans tous les cas, sans lien direct avec les entités cibles; b) de fournir à

ses clients des données relatives au nombre de requêtes lancées sur le dossier d'une entité cible donnée; c) de traiter les données issues de listes électorales pour effectuer des contrôles de cohérence lors de la fourniture de ses services; d) de traiter les données personnelles relatives aux déclarations fiscales rentrées par les contribuables pour 2005 et stockées suite à leur publication par le bureau de perception italien (voir ci-dessus). Il a également été ordonné à la société d'effacer lesdites données sans délai.

Communications électroniques

Déchets électriques et électroniques et protection des données: dans une décision datée du 13 octobre 2008, le Garante a attiré l'attention des personnes morales, administrations publiques, autres organismes et personnes physiques qui mettent au rebut des dispositifs usagés contenant des données personnelles au lieu de les détruire sur la nécessité de prendre des dispositions et mesures adaptées, par exemple avec l'aide de tiers disposant de connaissances techniques requises, afin de prévenir tout accès non autorisé aux données personnelles contenues sur les équipements électriques et électroniques en question. Toute personne prévoyant de réutiliser et/ou de recycler des équipements électroniques et électriques usagés ou des composants de ceux-ci doit s'assurer qu'aucune donnée personnelle n'est présente et/ou intelligible sur ledit équipement et, le cas échéant, obtenir l'autorisation d'effacer de telles données et/ou de les rendre inintelligibles.

Facturation détaillée: dans une décision datée du 13 mars 2008, le Garante a autorisé tous les fournisseurs de services de communications électroniques accessibles au public, en vertu de la section 124(5) du Code, à indiquer, dès le 1er juillet 2008, les numéros des communications dans leur intégralité sur les factures détaillées demandées par leurs clients, à la condition qu'ils permettent à leurs utilisateurs de passer des communications et de demander des services au départ de n'importe quel terminal en ayant recours à des méthodes de paiement autres que la facturation et à la conditions qu'ils fournissent à tous leurs abonnés des notes d'information appropriées qui seront incluses dans au moins deux factures et seront publiées sur les sites internet des fournisseurs.

Télémarketing: suite à plusieurs plaintes et notifications ayant trait à des appels téléphoniques non sollicités effectués par et/ou au nom de plusieurs opérateurs téléphoniques et/ou sociétés de commercialisation des produits et services, l'autorité italienne de protection des données a interdit à plusieurs sociétés spécialisées dans le développement et la vente de bases de données de continuer à traiter les données personnelles (à savoir les numéros de téléphone) de plusieurs millions d'utilisateurs. Les numéros de téléphone en question avaient été collectés et utilisés illégalement, les personnes concernées n'en ayant pas été préalablement averties et n'ayant pas consenti spécifiquement au transfert de leurs données à d'autres sociétés.

Cette interdiction s'étendait également aux autres sociétés qui avaient acheté les bases de données des sociétés en question en vue de contacter les utilisateurs et de commercialiser leurs produits et services par l'intermédiaire de centres d'appel. Les ordres d'interdiction ont fait suite à plusieurs avertissements et inspections de l'autorité de protection des données; ces inspections avaient été réalisées sur les sites des sociétés qui avaient généré et vendu les bases de données, en relation avec les opérateurs téléphoniques et sociétés qui les avaient achetées, et aux centres d'appel qui avaient contacté les utilisateurs en question.

Il convient de noter qu'une des sociétés proposait, sur son site internet, les données de plus de 15 millions de ménages italiens, regroupés par niveau de revenus et style de vie, sans en avoir informé les personnes concernées ni avoir obtenu leur consentement de communiquer leurs données à des tiers.

Il convient de rappeler à cet égard qu'une récente modification législative (voir Section 1) permet de déroger aux règles ci-dessus relatives au consentement de l'abonné, en vertu de quoi les données personnelles contenues dans des bases de données élaborées à partir de répertoires d'abonnés au téléphone compilés avant le 1er août 2005 peuvent être utilisées légalement à des fins de publicité jusqu'au 31 décembre 2009. Cette autorisation ne concerne que les responsables des données, les bases de données ayant été compilées avant le 1er août 2005.

Données de localisation géographiques et «boîtes de contrôle» installées sur les cars: dans une décision rendue au terme d'activités de vérification préalables, l'autorité italienne de protection des données a autorisé le traitement de données de localisation géographique par les services de transport public locaux, de même que d'autres informations relatives au «mode de conduite» et à plusieurs paramètres (p. ex. pression de l'huile de freinage au début et à la fin du freinage, vitesse du véhicule pendant le freinage, etc.) collectées au moment d'accidents via un «enregistreur d'événements».

L'autorité italienne de protection des données a permis les opérations de traitement en question pour autant que celles-ci répondent à un certain nombre d'exigences: Les personnes concernées (chauffeurs) sont censés recevoir des explications détaillées quant à la nature des données traitées et aux caractéristiques du système eu égard aux différents objectifs poursuivis; l'accès aux données traitées doit être réservé aux seules personnes chargées de cette mission par la société et légalement habilitées à accéder aux données du fait de leurs tâches; les données ne doivent pas être conservées plus longtemps qu'il n'est nécessaire pour réaliser lesdits objectifs – en anonymisant, le cas échant, les informations relatives à la localisation géographique et en ne traitant ces informations que sous la forme de données agrégées en vue de surveiller et de planifier le service de transport public. Les données relatives au «mode de conduite», collectées en vue d'octroyer des primes aux chauffeurs qui adaptent leur style de conduite aux normes de l'entreprise, doivent être traitées conformément aux restrictions légales applicables, et plus particulièrement à celles définies à la section 10 du règlement CE n° 561/2006 du 15 mars 2006. Il est nécessaire de préalablement se conformer aux procédures à mettre en place conformément à la section 4(2) de la loi n° 300/1970 – selon laquelle l'accord des syndicats doit être obtenu et/ou des dispositions des agences locales du ministère de l'emploi sont requises pour surveiller les collaborateurs à distance. L'entreprise devra notifier à l'autorité italienne le traitement, notamment, des données de localisation géographique et désigner le fournisseur de services comme responsable du traitement aux termes de la section 29 du Code de protection des données.

Plaintes officielles
Archives de journaux en ligne: l'autorité de protection des données a répondu a plusieurs plaintes introduites par des individus concernant la disponibilité d'articles de journaux (anciens) via les archives en ligne d'un journal. Ces requêtes indiquaient que les articles archivés ne reflétaient plus la situation actuelle, les personnes en question s'étant amendées depuis leur publication. L'autorité a estimé que la mise à disposition de ces articles servait un objectif de recherche (historique) et d'analyse; par conséquent, le consentement des personnes concernées n'est pas requis et les données peuvent être traitées au-delà des délais nécessaires pour réaliser l'objectif premier de leur publication. Ce traitement est légal et pertinent. Les données ne doivent pas être effacées et/ou anonymisées comme le demandaient les plaignants. Toutefois, l'autorité a admis que les mécanismes de récupération des données des moteurs de recherche externes avaient un impact disproportionné sur les droits des plaignants, étant donné qu'ils lient définitivement une personne donnée à des événements et comportements appartenant au passé. Par ailleurs, les informations en question peuvent également être diffusées sur l'internet à des fins sans lien aucun avec la recherche historique, du fait des mécanismes actuels de conservation des chaînes de recherche. Les plaintes ont donc été jugées partiellement recevables et il a été décidé que, si les pages internet contenant les données personnelles des plaignants devaient rester inchangées dans les archives en ligne de l'éditeur (accessibles via son site internet), elles ne devaient pas être indexées par les moteurs de recherche externes les plus employés sur la base du nom des personnes. Des outils techniques permettent de répondre à cette exigence («protocole d'exclusion des robots», utilisation de la «métabalise robots»). L'éditeur a reçu un délai de 60 jours pour se conformer à cette décision. L'autorité de protection des données s'est réservé le droit d'effectuer des investigations plus poussées concernant les implications de cette problématique, en coopération avec tous les acteurs pertinents.

Tests de paternité à des fins judiciaires, sans le consentement de l'enfant: une plainte avait trait à un père qui avait fait réaliser un test génétique sur son fils sans l'en informer, dans le cadre d'une enquête qu'il menait en vue d'établir un cas de consanguinité. Une agence

de détectives privés avait récupéré deux mégots de cigarette jetés par le fils de cet homme, à la demande du conseil juridique de celui-ci. Les échantillons biologiques avaient été testés sans que la personne concernée en soit informée, en vue d'établir la compatibilité génétique entre père et fils. L'autorité italienne de protection des données a statué que les tests de paternité/maternité ne peuvent pas être effectués sans le consentement de l'enfant si lesdits tests ne sont pas indispensables à des fins judiciaires. L'autorité de protection des données a rappelé que les données génétiques ne peuvent être collectées et traitées qu'avec le consentement «préalable, écrit» et éclairé de la personne concernée. La seule dérogation possible à cette exigence réside dans la nécessité d'étayer une plainte en justice ou de présenter une défense dans une action, à condition toutefois que le test soit absolument «indispensable» et soit effectué conformément aux conditions définies par l'autorité italienne de protection des données, et notamment à l'obligation de fournir des informations spécifiques à la personne concernée si le test génétique a pour but d'établir la paternité/maternité. L'autorité de protection des données a estimé que les droits du fils à la protection de ses données avaient été violés et a interdit tant au père qu'à son conseil juridique de traiter plus avant les informatiques génétiques indûment collectées de la manière décrite ci-dessus.

Informations commerciales: au cours de l'année dernière, plusieurs plaintes ont été introduites à l'encontre d'une société gérant la plus importante base de données d'informations commerciales d'Italie, qui fournit des informations sur les performances commerciales et la solvabilité des entreprises aux banques, agences financières, professionnels et société. Outre les nombreuses plaintes déposées à cet égard, l'autorité italienne de protection des données s'est attaquée à cette problématique en général via une décision qui visait spécifiquement l'entreprise en question (voir ci-dessus).

Contrôles

Les activités de contrôle ont encore été renforcées en 2008, dans le droit fil de la tendance générale à la hausse signalée les années antérieures. Ces activités se sont concentrées sur des questions d'intérêt général pour plusieurs catégories de personnes concernées. Plus particulièrement, d'importants contrôles approfondis ont été effectués sur les opérations de traitement réalisées par: a) les organismes financiers et fiscaux; b) les institutions bancaires; c. les sociétés d'information commerciale; d) les opérateurs de télécommunications, en relation avec les communications publicitaires non sollicitées et avec la création de profils de clients sur la base des données de trafic; e) les organismes de crédit à la consommation; et f) les entreprises réutilisant des données publiques, et notamment les listes électorales et les données contenues dans les registres publics de biens mobiliers et immobiliers. De nombreuses inspections ont été effectuées vis-à-vis d'entités publiques et privées utilisant des systèmes de vidéosurveillance, dans le but de vérifier que le traitement était légal et conforme à la décision générale rendue à cet égard par l'autorité italienne de protection des données. Il convient également d'accorder de l'importance aux contrôles effectués dans les hôpitaux publics traitant des données sensibles, en relation avec l'adoption de mesures de sécurité minimales.

Lettonie

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

Loi sur la protection des données à caractère personnel

La directive 95/46/CE a été transposée en droit national par la loi sur la protection des données à caractère personnel, entrée en vigueur le 20 avril 2000, dont les derniers amendements remontent au 6 mars 2008. La loi sur la protection des données a été modifiée le 21 février 2008. Les principaux changements portaient sur l'exception au droit qu'a une personne concernée d'accéder à ces données, lorsque le traitement des données est effectué dans le cadre des intérêts de l'État en matière fiscale, et sur le traitement des données des compagnies d'assurance en vue d'indemniser les sinistres au titre d'une police d'assurance.

Loi sur l'Inspection nationale des données

Afin de garantir la totale indépendance de l'Inspection nationale des données de Lettonie, une loi a été élaborée à cet égard. Compte tenu de la nécessité de réviser les ressources nécessaires en vue de garantir le bon fonctionnement de l'autorité indépendante de protection des données dans le contexte économique qui prévaut en Lettonie, le projet de loi a été mis à jour à la fin de l'année 2008 et au début de l'année 2009. Il devrait être soumis au gouvernement vers la mi-2009.

Réglementation relative au transfert de données à destination de pays tiers

En 2008, l'Inspection nationale des données de Lettonie a poursuivi ses activités dans le cadre de la rédaction du règlement du cabinet des ministres définissant des normes contractuelles standard pour les transferts de données personnelles à des pays tiers. Ce règlement met en œuvre les exigences relatives au contenu des contrats fixées dans les décisions 2001/497/CE et 2004/915/CE de la Commission sur les clauses contractuelles standard en matière de transfert des données.

Réglementation relative à la formation et à la certification des agents de protection des données

La loi sur la protection des données à caractère personnel définit les modalités de notification du traitement des données. Depuis 2008, une autre solution existe: l'agent de protection des données dans les institutions privées et publiques. L'Inspection nationale des données a donc élaboré un règlement du cabinet des ministres (n° 80, du 5 février 2008), «Procédure relative à la formation des agents de protection des données», entré en vigueur le 9 février 2008. Ce règlement spécifie la procédure de formation et de certification des agents de protection des données, ainsi que le programme de formation. La formation peut être assurée par l'Inspection nationale des données et par d'autres institutions des secteurs public et privé, seule l'Inspection peut faire passer les examens. En 2008, celle-ci a organisé deux examens, et sept agents, issus tant du secteur privé que gouvernemental, ont été certifiés.

Renforcement des amendes applicables aux actions illicites en lien avec des données personnelles

Le 3 juillet 2008, le code letton des infractions administratives a été modifié en vue d'y renforcer les amendes applicables aux actions illicites en lien avec des données personnelles. Ces amendements sont entrés en vigueur le 7 août 2008. Désormais, l'amende la plus élevée qui puisse être infligée à une personne morale s'élève à 10 000 lats (soit quelque 14 230 EUR).

Réglementation relative à la conservation des données des services de communications électroniques à des fins de maintien de l'ordre

Les directives 2002/58/CE et 2006/24/CE ont été transposées en droit national par la loi sur les communications électroniques.

Depuis 2007, l'Inspection nationale des données est l'autorité chargée de compiler les statistiques relatives à la conservation des données générées ou traitées dans le cadre de la fourniture de services et/ou réseaux de communications électroniques accessibles au public par les fournisseurs de ces services et réseaux conformément à l'article 19 de la loi sur les communications électronique et de 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 communication, et modifiant la directive 2002/58/CE. Le règlement du cabinet des ministres (n° 820, du 4 décembre 2007), «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 le transfert de données conservées par les fournisseurs de services de communications électroniques, de même que l'ordonnance relative à la façon de compiler et de soumettre les informations statistiques sur les données demandées», définit les délais pendant lesquels les fournisseurs sont tenus de conserver les informations statistiques et de les soumettre à l'Inspection nationale des données. 2008 a été la première année au cours de laquelle l'Inspection a compilé les statistiques.

B. Jurisprudence

En 2008, l'Inspection nationale des données a reçu 140 plaintes. La plupart portait sur un traitement des données personnelles sans base légale ou sur un traitement des données dépassant le cadre déclaré. Suite aux contrôles réalisés dans le domaine de la protection des données personnelles, l'infraction à la loi sur la protection des données à caractère personnel a été confirmée dans 28 cas. Dans 18 % des cas, des avertissements ont été émis (contre 10 % des cas en 2007). Ce pourcentage a donc augmenté. En outre, en 2008, le nombre d'amendes administratives infligées aux contrevenants a progressé de près de 40 % par rapport à 2007. Les plaintes avaient essentiellement trait au traitement de données personnelles sans base légale, à la violation des droits des personnes concernées (articles 10 et 11 de la directive 95/46/CE) et à des infractions au principe de la proportionnalité dans le traitement des données.

Les infractions les plus courantes avaient trait à:
- la publication de données personnelles sur l'internet;
- la vidéosurveillance;
- la copie de passeports;
- le traitement des données effectué par les services d'entretien domestique;
- le traitement des données des agences de notation et le transfert de données à des tiers.

En 2008, le nombre d'infractions relatives à la publication de données personnelles sur l'internet a augmenté en comparaison avec 2007. Par ailleurs, la coopération avec la police s'est intensifiée concernant les cas d'usurpation d'identité dans lesquels l'identité des suspects a pu être établie.

C. Questions diverses importantes

Les principaux débats auxquels l'Inspection nationale des données a pris part en 2008 au niveau national portaient sur les questions suivantes: Tout autre usage a été exclu.
- élaboration du concept du système national de services de santé en ligne;
- organisation du système de souscription en ligne d'une police d'assurance automobile et résolution de la problématique du droit des personnes handicapées à une réduction sur leur assurance automobile, celle-ci requérant un accès à des données sensibles;
- considérations nationales relatives aux transferts de données de passagers aux États-Unis et échange de données personnelles avec les États-Unis dans le cadre du programme d'exemption de visa;
- mise en place d'une base de données commune de données biométriques et traitement des données biométriques sur les passeports.

Cas particuliers (liés aux principaux problèmes qui ont fait l'objet de plaintes):
1. Une part significative des plaintes reçues avait trait aux cotes de crédit. Les données personnelles des débiteurs sont transférées à des tiers en vue du recouvrement des créances. Les données actuelles et historiques sont également communiquées à des tiers sans le consentement de la personne concernée. Dans la plupart des cas, ces transferts sont considérés comme un traitement de données sans base légale et sortant du cadre autorisé.
2. La publication de données personnelles sur l'internet sans le consentement des personnes considérée peut souvent constituer une violation de la loi sur la protection des données à caractère personnel. Une telle opération du responsable du traitement des données est considérée comme un traitement de données sans base légale.

3. L'employeur a transféré à des tiers des copies de documents d'identité de ses employés ou clients. La copie de documents d'identité est considérée comme un traitement de données personnels sortant du cadre autorisé, et le transfert de ces données à des tiers comme un traitement de données sans base légale, sortant du cadre autorisé.

Recommandations élaborées

En 2008, l'Inspection nationale des données a élaboré deux recommandations. Compte tenu du nombre de plaintes relatives à l'usage de systèmes de vidéosurveillance et aux courriers électroniques non sollicités, et afin de promouvoir une meilleure compréhension de ces problèmes, l'Inspection nationale des données a rédigé:

- une recommandation sur le traitement des données en relation avec la vidéosurveillance;
- une recommandation sur les communications commerciales.

Système d'information Schengen

En 2008, l'Inspection nationale des données a contrôlé des institutions et autorités ayant accès au Système d'information Schengen (SIS). Ces activités ont été menées conformément aux articles 96, 97 et 98 de la Convention de Schengen.

Protection des données en milieu scolaire

En 2008, l'Inspection nationale des données a organisé plusieurs ateliers destinés aux enseignants et au personnel administratif des écoles concernant la protection des données en milieu scolaire. Les principes généraux de la protection des données y ont été expliqués, et des points plus particuliers y ont été débattus, dont l'accès aux résultats scolaires (projet «e-class»), la publication d'informations sur les pages internet de l'école, la conservation des données médicales, la vidéosurveillance, etc.

Lituanie

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

Le 1er février 2008, le Seimas (Parlement) de la République de Lituanie a adopté un amendement à la loi relative à la protection des données à caractère personnel (le nouveau texte entrera en vigueur le 1er janvier 2009).

Le nouveau libellé définit les dispositions de la loi relative à la protection des données à caractère personnel régissant le traitement des codes d'identification personnels. Les responsables du traitement des données employant des outils automatisés pour traiter des données personnelles de nature sanitaires en vue d'assurer la protection de la santé ou des données personnelles à des fins de recherche médicale doivent en informer l'Inspection publique de la protection des données et réaliser un contrôle préalable. Le terme «vidéosurveillance» a été défini, et des règlements ont été adoptés concernant le traitement des images à caractère personnel, mais aussi des données personnelles utilisées à des fins de marketing direct ou d'évaluation de la solvabilité. Des dispositions ont également été arrêtées quant au statut des personnes et unités responsables de la protection des données et à la procédure de gestion des plaintes. Le libellé de la nouvelle loi relative à la protection des données à caractère personnel établit l'indépendance de l'Inspection publique de la protection des données en tant qu'institution de contrôle (au sens de la directive 95/46/CE) et accorde un mandat de 5 ans au directeur de l'Inspection.

Le 14 novembre 2008, la loi visant à modifier et à compléter la législation sur les communications électroniques de la République de Lituanie (entrée en vigueur le 15 mars 2009) a été adoptée, transposant ainsi les dispositions de la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communication électronique accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

La loi stipule que les données de trafic de l'abonné ou de l'utilisateur enregistré de services de communication électronique peuvent être stockés pour une durée maximale de six mois à compter de la date de la communication, hormis dans les cas où la facture fait l'objet d'une contestation légale ou où les données sont nécessaires à des fins de récupération de créances, ainsi que dans les cas prévus à l'article 77, paragraphe 2, de cette loi. Afin de garantir un accès aux données en cas de crimes graves et très graves, tels que décrits dans le code pénal de la République de Lituanie, lorsque de tels renseignements sont nécessaires à des fins d'investigation, de détection et de poursuite des actes criminels, les fournisseurs de réseaux et/ou de services de communication (électronique) publics doivent stocker leurs informations pour une période de six mois à compter de la date de la communication, conformément à la procédure établie par la loi, afin de permettre aux institutions compétentes d'accéder gratuitement aux données qu'ils ont générées ou traitées. Cette obligation porte également sur la conservation des données liées aux appels infructueux générées ou traitées et stockées (données téléphoniques) ou enregistrées (données internet) par les fournisseurs de réseaux et/ou de services de communication (électronique) publics lors de la fourniture des services appropriés.

Si les données susmentionnées sont nécessaires aux entités effectuant des activités opérationnelles, aux juges d'instruction, aux procureurs, aux tribunaux ou aux juges pour empêcher, investiguer et détecter des actes criminels, les institutions habilitées par le gouvernement, à la demande des entités effectuant des activités opérationnelles, à savoir les fournisseurs de réseaux et/ou de services de communication électronique, doivent conserver lesdites informations pendant une période plus longue, mais ne dépassant pas six mois supplémentaires. Ledit stockage doit être financé par des fonds publics, conformément à la procédure établie par le gouvernement (article 77, paragraphe 2, de la législation sur les communications électroniques de la République de Lituanie).

Le 12 novembre 2008, l'ordonnance du directeur de l'Inspection publique de la protection des données n° 1T-71 (1.12), «De l'approbation des exigences générales relatives aux mesures organisationnelles et techniques

de protection des donnée», a été ratifiée. Ces exigences générales précisent les mesures organisationnelles et techniques que doivent mettre en œuvre un responsable du traitement des données et un préposé au traitement des données en vue de protéger les données personnelles contre toute destruction, altération ou divulgation non intentionnelles ainsi que contre tout autre traitement illégal.

B. Jurisprudence

Publication sur l'internet des données personnelles de personnes ivres

L'Inspection publique de la protection des données a reçu deux plaintes concernant la publication de données personnelles sur le site internet du commissariat central de la police de la ville de Vilnius. Après enquête, l'Inspection a appris que le chef de la police de Vilnius avait pris la décision de publier sur le site internet du commissariat les données personnelles (prénom, nom, année de naissance, lieu et date de l'infraction administrative commise, degré d'ébriété et sanction infligée) des personnes prises en état d'ébriété au volant. Son objectif était d'informer le public, de l'éduquer et de prévenir les infractions administratives.

L'Inspection publique de la protection des données a statué que lesdites actions de la police étaient illégales, étant donné que la collecte des données personnelles des plaignants avait pour but d'imposer une sanction. Plus tard, les données personnelles des plaignants ont été traitées dans le registre des infractions au code de la route et des accidents de la circulation. Conformément au paragraphe 2 de l'article 6 de la loi sur les activités de police, il est interdit de divulguer des informations personnelles stockées dans les systèmes d'information de la police à des tiers, à moins qu'une loi ou un autre acte légal ne l'autorise. En vertu de l'article 3, paragraphe 1, alinéa 1, de la loi relative à la protection des données à caractère personnel, le responsable du traitement des données doit s'assurer que les données personnelles sont collectées à des fins spécifiques et légitimes et ne sont pas ultérieurement traitées à des fins incompatibles avec les objectifs fixés avant leur collecte. L'Inspection était d'avis que lesdites données ne pouvaient pas être publiées sur l'internet dans le but d'informer le public, de l'éduquer et de prévenir les infractions administratives étant donné:

- que ces objectifs divergent de ceux déterminés avant la collecte des données personnelles;
- que, selon la loi sur les activités de police, il est interdit de divulguer les informations personnelles consignées dans le registre;
- qu'il n'existait aucun critère permettant de conclure à un traitement légal des données personnelles.

L'Inspection publique de la protection des données a ordonné au commissariat central de la police de Vilnius de mettre un terme à la publication des données personnelles des citoyens mis à l'amende pour avoir enfreint le code de la route (nom, prénom, année de naissance, date et lieu de l'infraction, degré d'ébriété établi, article du code des infractions administratives de la République de Lituanie portant sur l'infraction commise et sanction infligée) sur la page internet produite en vue d'informer le public, de l'éduquer et de prévenir les infractions à la législation administrative.

Le commissariat central de la police de Vilnius a fait appel des décisions de l'Inspection publique devant un tribunal. Le tribunal administratif du district de Vilnius a conclu que l'article 5, paragraphe 1, alinéa 6, de la loi relative à la protection des données à caractère personnel devait s'appliquer (les données personnelles peuvent être traitées si ce traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement des données ou par un tiers auquel sont divulguées les données, à moins que les intérêts de la personne concernée ne priment sur lesdits intérêts). Par ailleurs, le tribunal a statué que les données telles que le lieu et la date de l'infraction administrative, le degré d'ébriété et les sanctions infligées ne pouvaient pas être considérées comme des données personnelles.

Un recours a été introduit à l'encontre de la décision du tribunal administratif du district de Vilnius auprès de la Cour administrative suprême de Lituanie.

La Cour administrative suprême de Lituanie a conclu que les données telles que le lieu et la date de l'infraction administrative, le degré d'ébriété et les sanctions infligées doivent être considérées comme des données

personnelles si elles sont publiées conjointement avec le prénom et le nom de la personne concernée.

La Cour a également statué que le commissariat central de la police de Vilnius avait divulgué des données personnelles sur son site internet sous couvert d'un intérêt légitime (article 5, paragraphe 1, alinéa 6, de la loi relative à la protection des données à caractère personnel). Pour résumer les dispositions du code des infractions administratives, on peut conclure que celui-ci oblige les institutions publiques, en ce comprises les forces de police, non seulement à expliquer les infractions commises et à infliger une sanction appropriée, mais aussi à développer et à mettre en œuvre des mesures prévenant lesdites infractions. Par ailleurs, ce code stipule également que la prévention des infractions est l'un des objectifs poursuivis par les amendes administratives. Il apparaît donc que des mesures préventives liées aux sanctions administratives peuvent être élaborées et mises en œuvre sur la base d'informations, et notamment de données personnelles, collectées au cours des procédures.

La pratique judiciaire montre que la conduite de véhicules motorisés en état d'ébriété est considérée comme une infraction très grave au code de la route. Le code des infractions administratives prévoit des sanctions particulièrement sévères pour ce type d'infractions, car elles sont susceptibles de mettre directement en danger la santé et la sécurité des usagers de la route. En conséquence, mettant en balance, d'une part, la publication temporaire (pendant un mois) des données personnelles d'un individu qui s'est rendu coupable d'une infraction administrative grave et, d'autre part, la prévention d'une menace pour la vie, la santé et la sécurité des usagers de la route, la Cour est parvenue à la conclusion qu'en l'espèce, le droit des personnes concernées au respect de la vie privée est moins important que l'intérêt public résidant dans la prévention des infractions graves au code de la route. Les intérêts des personnes concernées ne priment pas sur l'intérêt légitime de la police.

Publication de données personnelles sur l'internet à des fins électorales

La commission électorale centrale de la République de Lituanie a informé l'Inspection publique de la protection des données que les données personnelles des candidats aux élections législatives seraient traitées sur l'internet, afin que l'Inspection puisse effectuer un contrôle préalable et autoriser ledit traitement. Conformément aux règles soumises par la commission électorale centrale de la République de Lituanie, les données personnelles (prénom, nom, parti politique, lieu et date de naissance, citoyenneté, nationalité, état civil, noms des membres de la famille, déclarations de patrimoine, etc.) des candidats sont disponibles sur le site internet de la commission pour une période illimitée. Ce délai ne dépend pas de l'élection ou non du candidat au Parlement.

Conformément à l'article 4 de la loi relative à la protection des données à caractère personnel, ces données ne doivent pas être stockées plus longtemps que nécessaire aux fins du traitement. Lorsque les données ne sont plus requises, elles doivent être détruites. S'appuyant sur cette disposition, l'Inspection publique de la protection des données a demandé à la commission électorale centrale de la République de Lituanie de déterminer pendant combien de temps les données personnelles des candidats seraient publiées sur l'internet. La commission a refusé de définir une limite dans le temps, et l'Inspection a dès lors décidé de lui refuser l'autorisation de publier les données personnelles des candidats sur son site internet.

La commission électorale centrale de la République de Lituanie a fait appel de cette décision.

Le tribunal administratif du district de Vilnius a décidé que la décision de l'Inspection publique de la protection des données était légitime et qu'il n'y avait aucune raison pour que la commission soit autorisée à publier de telles données sur son site internet pour une durée illimitée.

Un recours a été introduit à l'encontre de la décision du tribunal administratif du district de Vilnius auprès de la Cour administrative suprême de Lituanie.

La Cour administrative suprême de Lituanie a vu les choses sous un autre angle.

Selon elle, la commission électorale centrale de la République de Lituanie traite ces données personnelles en vue d'informer les électeurs pour qu'ils puissent effectivement exercer leur droit électoral. Elle estime qu'il

ne fait aucun doute que les données relatives aux candidats aux élections législatives sont nécessaires pendant la campagne électorale. Les informations relatives aux candidats, élus ou non, restent indéniablement pertinentes pour le calcul et l'annonce des résultats électoraux. Une fois que le député a prêté serment, l'électeur a de bonnes raisons de vouloir savoir qui représente ses intérêts. De même, pendant le mandat du député élu, il reste en principe possible de remplacer un candidat qui ne peut pas siéger. À la lumière de ces informations, les données relatives aux candidats comme aux élus sont de la plus grande importance pour les électeurs et restent d'actualité depuis la décision de se porter candidat à un siège au Parlement jusqu'à la fin de la législature.

La durée illimitée de la publication des documents relatifs aux candidats peut se justifier par l'importance des élections en tant que participation citoyenne à la gouvernance de l'État. Les élections démocratiques sont une forme capitale de gouvernance de l'État impliquant la participation des citoyens et constituent donc également une valeur essentielle dans la formation des institutions politiques représentatives de l'État. Les élections ne peuvent être considérées comme démocratiques et leurs résultats comme légitimes et légaux si elles sont organisées au mépris des principes des élections démocratiques établis par la constitution, dans le non-respect des procédures électorales démocratiques.

Veiller à ce que les électeurs soient correctement informés est une condition sine qua non à la tenue d'élections légitimes et légales. Par ailleurs, plus les données sont complètes, plus la confiance des électeurs est stimulée, non seulement vis-à-vis des différents candidats mais aussi vis-à-vis des autorités représentatives elles-mêmes: les électeurs peuvent accéder aux données relatives aux élections antérieures et à leur organisation, trouver des informations sur les candidats précédents et non seulement faire leur choix quant aux candidats acceptables mais également vérifier si les procédures électorales sont dignes de confiance et décider s'ils souhaitent participer aux élections en général. Par conséquent, la constitution d'archives spécifiques sur les élections et la divulgation des données peuvent se justifier par l'intérêt légitime poursuivi, à savoir promouvoir la confiance des électeurs dans les institutions représentatives elles-mêmes.

Considérant que la divulgation des informations concernant les députés est conforme aux objectifs légitimes, à savoir renforcer la confiance des électeurs dans la formation des institutions représentatives et garantir que les procédures électorales sont légales et transparentes, et que la réalisation desdits objectifs n'est pas uniquement importante pendant des élections spécifiques, la Cour administrative suprême de Lituanie a statué que les données relatives aux élections pouvaient être divulguées pendant une période illimitée.

C. Questions diverses importantes

Traitement des données personnelles dans les institutions financières

Soucieuse de déterminer l'ampleur et la légalité du traitement des données personnelles des individus s'adressant à des institutions financières en vue d'obtenir un service de crédit rapide par SMS ou via l'internet, l'Inspection publique de la protection des données a contrôlé la légitimité du traitement des données personnelles dans six institutions financières. Ces contrôles ont mis au jour les méthodes d'identification personnelle (des clients): une personne produit un document confirmant son identité personnelle; une personne s'enregistre et paie au départ de son compte bancaire personnel, et si les données coïncident, la personne reçoit un SMS contenant un mot de passe de connexion; une personne remplit une demande sur l'internet ou par téléphone avant de passer en personne au service clients afin de signer un contrat, en présentant un document d'identification personnelle; une personne s'enregistre par SMS ou via l'internet et paie au départ de son compte bancaire personnel, qu'elle a mentionné pendant son enregistrement, et, si les données correspondent, elle reçoit un SMS contenant un mot de passe de connexion; une personne fournit son numéro de téléphone sur l'internet et reçoit un SMS contenant un code qu'elle doit entrer sur le site internet, remplit le formulaire de demande et paie une redevance fixe au départ de son compte bancaire personnel. Une institution financière exige qu'une copie de documents personnels appartenant aux individus qui ne sont pas des utilisateurs du service de transactions bancaires électroniques lui soit envoyée par télécopie ou par courrier électronique à des fins d'identification. L'Inspection publique de la protection des données est d'avis que la fourniture à

distance d'un document d'identité personnel dans de telles conditions ne peut pas être considérée comme un moyen suffisant d'identification personnelle.

Les données fournies par les personnes sont vérifiées par différents responsables du traitement des données: une entreprise reçoit les données relatives aux revenus des personnes via le Conseil du fonds de sécurité sociale de l'État, qui dépend du ministère lituanien de la sécurité sociale et du travail; trois institutions financières reçoivent des données du service du registre de la population dépendant du ministère lituanien de l'intérieur aux fins de l'identification personnelle, de la vérification des données et du contrôle de l'exactitude; toutes les institutions financières reçoivent les données relatives aux dettes personnelles de JV «Creditinfo Lietuva». Trois institutions financières reçoivent des données relatives aux biens immobiliers que possède la personne d'après le registre du patrimoine immobilier, l'une d'entre elles recevant et traitant ces données personnelles de manière illégale et quatre institutions financières se voient fournir des données aux fins de l'identification personnelle et de la vérification par des institutions de crédit (banques).

Diverses infractions à la législation lituanienne relative à la protection des données à caractère personnel ont été décelées lors de l'inspection, eu égard, notamment à la quantité de données personnelles collectées, au traitement des données sans le consentement de la personne concernée, à la réglementation relative au marketing direct (sans que la personne concernée ait la possibilité de consentir au traitement de ses données personnelles à des fins de marketing direct ou en n'ayant établi que le droit de refuser) ou encore à la mise en œuvre de mesures organisationnelles et techniques appropriées. L'Inspection publique de la protection des données a émis des instructions à l'intention des institutions financières passées au crible.

Sensibilisation du public

Le 23 janvier 2008, l'Inspection publique de la protection des données a organisé une conférence sur la Journée européenne de la protection des données pour les jeunes, en collaboration avec la commission des droits de l'homme du Seimas (Parlement) lituanien.

L'événement visait à célébrer la Journée européenne de la protection des données, qui se tient traditionnellement le 28 janvier. Cette année, il avait pour objectif d'attirer l'attention des jeunes Lituaniens sur une problématique d'une importance capitale pour tous, à savoir les droits de l'homme et la protection de la vie privée. L'exposé relatif aux tout derniers documents d'identité présenté par le délégué du centre de personnalisation des documents d'identité du ministère lituanien de l'intérieur a suscité une grande curiosité et beaucoup d'intérêt chez les jeunes. Lors de l'organisation de cet événement, il a été décidé qu'il était capital d'évaluer le degré de sensibilisation des adolescents aux questions des droits de l'homme et de la protection des données et d'identifier les questions qui les inquiètent le plus.

L'événement a rassemblé quelque 80 élèves âgés entre 14 et 18 ans des écoles et collèges de Vilnius. Des brochures contenant des informations concises relatives à une utilisation sûre de l'internet leur ont été distribuées, de même que d'autres documents d'informations.

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)
Aucun amendement n'a été apporté à la loi précitée au cours de l'année 2008.

Loi du 30 mai 2005 relative aux règles spécifiques applicables à la protection de la vie privée dans le secteur des communications électroniques (transposition de la directive 2002/58/CE)
Aucun amendement n'a été apporté à la loi précitée au cours de l'année 2008.

Règlements et législation secondaire
Le règlement grand-ducal du 7 octobre 2008 appuie le renouvellement des mandats pour chacun des trois membres effectifs de la CNPD, de même que la désignation de deux membres suppléants.

Le gouvernement a également adopté un règlement grand-ducal, en date du 1er décembre 2008, définissant les caractéristiques techniques relatives à l'interception des communications au Luxembourg.

Autres nouvelles mesures législatives

La loi fixant les «*conditions dans lesquelles les magistrats et les officiers de police peuvent accéder à certaines bases de données détenues par des personnes morales de droit public*» a été adoptée par le Parlement et publiée au journal officiel le 27 août 2008. Le premier avant-projet de celle-ci avait été commenté par la CNPD en 2006. Les avis alors émis ont été suivis par le gouvernement, qui y a inséré un grand nombre de garanties et de mesures de sécurité, comme l'avait suggéré la Commission nationale. Au cours des débats au Parlement, d'autres inquiétudes ont été exprimées par la commission consultative des droits de l'homme, lesquelles ont conduit à un resserrement des dispositions et à l'ajout de clauses de protection supplémentaires. La loi adoptée contient une vaste palette de restrictions et de précieuses garanties contre tout risque d'utilisation abusive des données personnelles. Toutefois, il apparaît que le texte est trop restrictif pour permettre aux forces de police d'accomplir leurs tâches quotidiennes. Raison pour laquelle il est possible que le Parlement soit à nouveau saisi de ce dossier en 2009 en vue d'amender ces dispositions restrictives.

La Commission nationale a conseillé le gouvernement sur un vaste éventail de projets de loi et de règlements grand-ducaux, dont le règlement grand-ducal relatif à la collecte et au traitement des données personnelles des élèves, le règlement grand-ducal concernant les conditions et modalité de délivrance des documents cadastraux ou la loi amendant la législation électorale de 2003. Parmi les autres sujets abordés, citons le projet de loi sur la libre circulation des personnes et l'immigration ainsi que le projet de règlement grand-ducal y afférent. Ce dernier définit spécifiquement les catégories de données personnelles auxquelles peut accéder le ministre en charge de l'immigration afin d'effectuer tous les contrôles prévus par la loi. Par ailleurs, la CNPD a conseillé le gouvernement concernant la loi sur l'exercice des professions de médecin, dentiste et vétérinaire, ainsi que concernant le projet de règlement grand-ducal correspondant.

La Commission nationale a également émis un avis à l'intention du gouvernement quant à l'enregistrement des numéros d'urgence conformément à la loi sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

B. Jurisprudence

Jurisprudence civile et pénale

Tribunal d'arrondissement de Luxembourg, Cour d'appel siégeant en 5e 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

En 2007, la juridiction d'appel suprême (la «*Cour de Cassation*») a cassé une décision de la Cour d'appel

concernant la validité des preuves collectées en violation des dispositions relatives à la protection des données. La Cour de cassation a fondé sa décision sur l'existence d'une violation du droit à un jugement équitable (article 6 de la Convention européenne des droits de l'homme).

Le 26 février 2008, une nouvelle Cour d'appel a déclaré que la production d'une preuve obtenue de manière illicite (*à savoir 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, 16e chambre correctionnelle, se prononçant sur la violation des articles 5 et 6 de la loi de 2002 relative à la protection des données

Le 27 octobre 2008, le tribunal d'arrondissement de Luxembourg, siégeant en 16e chambre correctionnelle, a créé un nouveau précédent concernant les condamnations pénales d'individus sur la base de la loi de 2002. L'employé d'un cimetière avait installé un système de caméras vidéo dans ledit cimetière, dans ses environs immédiats ainsi qu'à la morgue. Toutefois, il n'avait pas obtenu l'autorisation préalable de la *Commission nationale pour la protection des données*, comme l'exigent les dispositions de la loi de 2002 telle que modifiée. L'employé ayant néanmoins commencé à traiter des données personnelles (p. ex. surveillance en temps réel de personnes, enregistrement de fichiers d'images sur son ordinateur et reproduction de certaines scènes pour son «*propre divertissement*»), la Cour a statué qu'il avait clairement enfreint les dispositions de la loi de 2002 relative à la protection des données et l'a donc tenu pour responsable de ses actions.

C. Questions diverses importantes

Cyber-surveillance de collaborateurs par l'employeur

La CNPD a rédigé une décision fondamentale dans le domaine de la cyber-surveillance des collaborateurs, visant à trouver un juste équilibre entre le respect de la vie privée des personnes concernées au travail et les intérêts légitimes de l'employeur.

Les principes exposés dans ladite décision prennent en compte le nombre de requêtes d'autorisation et d'information reçues par la CNPD à ce sujet. La décision milite en faveur d'un usage modéré des outils de surveillance et définit la portée des mesures de surveillance que peut prendre un employeur. En vertu de celle-ci, une telle surveillance ne peut être assurée qu'à certaines fins, telles que la protection de la fonctionnalité du système informatique, des secrets industriels d'une entreprise et des informations confidentielles, de même que la prévention d'une concurrence déloyale.

À cet égard, l'une des grandes difficultés de la cyber-surveillance réside dans la distinction entre vie privée et usage professionnel. La CNPD soutient que les fichiers et messages enregistrés sur le poste de travail de l'employé doivent être considérés comme professionnels à moins d'être explicitement désignés comme privés.

Les messages privés ne peuvent pas être ouverts ni lus par l'employeur, même si celui-ci a préalablement interdit l'usage des systèmes de messagerie à des fins privées. Par ailleurs, l'employeur ne peut ouvrir ou lire les fichiers marqués comme privés qu'en présence du collaborateur.

Les fichiers et messages professionnels peuvent quant à eux faire l'objet d'un accès lorsque le collaborateur est absent ou après son départ, dans le but de garantir la continuité de l'activité de l'entreprise (mais pas d'évaluer le collaborateur ou d'intenter une action en justice à son encontre).

Dans le souci de maintenir un équilibre entre les intérêts légitimes de toutes les parties, un contrôle total ou permanent est interdit. La cyber-surveillance doit donc être de nature limitée et ne peut être étendue que sur la base d'une preuve justifiée et tangible d'abus.

E-Catering – Saisie automatique de la présence des enfants à la cantine

À la demande de la CNPD, le département de l'éducation nationale a restreint les catégories de données collectées ainsi que la durée du stockage de ces données. Le

droit des personnes concernées à objecter à la collecte et au traitement de leurs données est aussi garanti. Cette action s'inscrit dans un effort européen visant à renforcer le droit des enfants à une vie privée, surtout dans l'environnement scolaire.

Audit des principales compagnies de télécommunications du Luxembourg

Pendant la période 2007-2008, la CNPD a réalisé un audit complet des principales compagnies de télécommunications du Luxembourg. L'objectif poursuivit par la CNPD était d'obtenir un aperçu de la manière dont les opérateurs de télécommunications ont mis leurs activités en conformité avec les dispositions de la loi du 30 mai 2005 transposant la directive 2002/58/CE.

Campagne d'information et de sensibilisation

Pendant l'année 2008, la Commission nationale a poursuivi sa campagne d'information et de sensibilisation, notamment en participant activement aux travaux du comité national d'éthique de recherche ainsi qu'à la seconde Journée de la protection des données organisée par le Conseil de l'Europe. La Commission nationale a fourni des informations sur les nouvelles dispositions de la loi via son site internet et par l'intermédiaire d'entretiens accordés aux médias luxembourgeois.

Malte

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 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. Les dispositions relatives aux fichiers manuels ont pris effet en octobre 2007.

La directive 2002/58/CE a été transposée en partie par la loi sur la protection des données, en vertu des dispositions réglementaires sur le traitement des données personnelles (secteur des communications électroniques) de 2003 (notice légale 16 de 2003), mais aussi par la loi sur les communications électroniques, en vertu des dispositions réglementaires sur les télécommunications (données à caractère personnel et protection de la vie privée) de 2003 (notice légale 19 de 2003). Ces deux règlements d'application sont entrés en vigueur en juillet 2003.

Autres nouvelles mesures législatives
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 (amendant la directive 2002/58/CE) a été transposée dans le cadre juridique national par le biais de deux instruments législatifs qui ont amendé les réglementations susmentionnées. La note légale 198 de 2008, modifiant la note légale 16 de 2003, et la note légale 199 de 2008, modifiant la note légale 19 de 2003, ont toutes deux été publiées au Journal officiel et sont entrées en vigueur le 29 août 2008.

Ces réglementations obligent les fournisseurs de services à conserver les informations définies par la directive pendant un délai d'un an dans le cas de la téléphonie et des données mobiles et de dix mois dans le cas des données liées à l'internet. Lesdites informations ne peuvent être divulguées qu'aux services de police et de sécurité, à leur demande, et uniquement dans le cas de crimes graves.

B. Jurisprudence

Aucune.

C. Questions diverses importantes

Au cours de l'année de référence, le bureau a régulièrement organisé des réunions avec des représentants des différents secteurs, avec pour objectif principal de débattre des questions de protection des données applicables à chacun d'entre eux. Cette volonté de maintenir le contact avec les secteurs a été très bien accueillie, ce dont a besoin le bureau pour développer des lignes directrices et des codes de bonnes pratiques en vue de réglementer l'ensemble des secteurs. À cet égard, des réunions se sont tenues avec divers organes et entités des secteurs de l'éducation, du travail social, des télécommunications, du tourisme, des médias, des services financiers et de la santé. Des entretiens ont également eu lieu avec diverses autorités, dont celles en charge des communications, des services financiers, des ressources et des transports. Le commissaire a également rencontré le médiateur, de hauts fonctionnaires des forces de police et des représentants des services de sécurité.

Au cours de l'année 2008, le bureau a reçu 31 plaintes, ce qui a poussé le commissaire à examiner chaque cas et à communiquer sa décision en fonction du résultat de ses enquêtes et des considérations prises en compte lors de l'analyse. Les motifs de plaintes les plus courants étaient en lien avec l'installation de caméras de surveillance par des personnes privées, avec l'envoi de communications électroniques à des fins de marketing direct dans le non-respect des critères fixés par la loi et avec l'introduction de systèmes biométriques sans notification préalable au bureau.

Au cours de la période de référence, le commissaire a effectué de nombreuses inspections dans le domaine du traitement des données à caractère personnel, que ce soit dans le contexte de l'examen de plaintes, dans le cadre de la stratégie d'évaluation d'un secteur donné par le bureau, de la propre initiative du commissaire ou en vue d'honorer ses obligations européennes.

Tout au long de l'année, le bureau a apporté sa contribution aux plateformes européennes et internationales.

Il 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 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.

Dans le droit fil de la stratégie du bureau visant à sensibiliser l'opinion publique à la protection des données, des présentations ont été données dans différentes organisations et organes dotés d'une personnalité juridique en vue de 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 diffusés à la radio et à la télévision. Les citoyens sont de plus en plus conscients de leurs droits, ce qu'atteste le nombre substantiel de requêtes, par téléphone et par courrier électronique, qui ont été adressées au bureau au cours de la période de référence.

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. Pour commémorer cette journée, le bureau a distribué des affiches et des tapis de souris dans les écoles, en vue de sensibiliser les jeunes générations à cette thématique. Ceci s'inscrit dans l'engagement ferme du bureau à inculquer la nouvelle culture du respect de la vie privée aux enfants, afin de leur permettre d'apprécier et d'exercer ce droit fondamental. Le message de cette année avait trait à l'utilisation de l'internet et à l'importance d'être conscient des risques de voir ses données personnelles divulguées lorsqu'on les transmet sur l'internet. Le bureau a souligné que l'identité de la personne concernée est précieuse et qu'il est donc impératif de la préserver. Dans le cadre de ces activités, 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.

En juin, une loi sur la liberté de l'information a été présentée au Parlement. Elle établit le droit à l'information détenue par les autorités publiques en vue de promouvoir et de renforcer la transparence et la responsabilité au sein du gouvernement. Lorsqu'elle entrera en vigueur, cette loi investira le commissaire à la protection des données des fonctions et obligations d'un commissaire à l'information.

Cette année, le bureau a également perdu son commissaire à la protection des données, M. Paul Mifsud-Cremona, décédé le 14 août. M. Mifsud-Cremona occupait ce poste depuis le 1er janvier 2004. En décembre, après de multiples consultations et en accord avec le leader de l'opposition, le premier ministre a nommé M. Joseph Ebejer nouveau commissaire à la protection des données. Celui-ci devrait être désigné officiellement au début de l'année prochaine.

Pays-Bas

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 nationale par la loi sur la protection des données (*Wet bescherming persoonsgegevens*, ou Wbp). Cette loi du 6 juillet 2000[18], entrée en vigueur le 1er septembre 2001, remplace l'ancienne loi sur l'enregistrement des données (*Wet persoonsregistraties*, ou 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[19]. 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

L'année dernière, l'autorité néerlandaise de protection des données (le «*College bescherming persoonsgegevens*», ou CBP) a su renforcer considérablement son rôle d'organisme de contrôle. Elle a choisi de se concentrer sur la conformité aux règles relatives au traitement des données personnelles et sur la répression en cas d'infractions à la législation. En 2008, le CBP a commencé à appliquer systématiquement les projets arrêtés au cours de l'année précédente et, surtout, à déployer toutes ses ressources humaines et matérielles en vue d'examiner la manière dont les dispositions légales pertinentes sont respectées et, en cas de violation de celles-ci, de prendre des mesures de répression. En 2008, le CBP a également posé des choix plus clairs, sur la base d'analyses des risqués, quant à la manière d'aborder un grand nombre de sujets très différents auxquels il est confronté. Il définit des priorités entre les questions structurelles et violations affectant de nombreuses personnes, et plus particulièrement les groupes vulnérables. L'analyse des risques a été préparée sur la base d'un système développé par nos soins et testé par des experts, ainsi que sur la base des avertissements qui nous parviennent via différents canaux, dans le but de déterminer les secteurs dans lesquels 1) de nombreux citoyens sont exposés à un 2) risque important se retrouver 3) victimes de violations graves et structurelles de la Wbp. C'est sur cette base qu'a été élaboré concrètement le plan stratégique 2008 du CBP.

Les chiffres de 2008 sont prometteurs: le CBP a mené des enquêtes de contrôle dans 95 cas (50 % de plus qu'en 2007) et imposé une sanction (ou menacé de le faire) dans 68 cas, ce qui représente près du double des chiffres de 2007 (2007: 39; 2006: 2!).

L'internet

L'année dernière, l'autorité néerlandaise de protection des données a reçu un grand nombre de plaintes et d'avertissements concernant la publication de données personnelles sur l'internet. Celles-ci avaient tout particulièrement trait à des requêtes d'effacement de ces données et aux droits des individus dont les données sont publiées sur l'internet. En prenant des mesures de répression contre les sites internet qui violent de manière structurelle la Wbp, le CBP entend renforcer la vigilance des responsables du traitement des données et des personnes concernées. Les deux parties doivent être davantage conscientes des droits des personnes concernées et de la nécessité que ces droits soient respectés.

Une mesure d'urgence à l'encontre d'un site internet contenant les données personnelles de fonctionnaires et de personnalités politiques a été couronnée de succès en un temps record: l'accès à ce site a été bloqué en un jour à peine. L'action visant une municipalité qui publiait sur son site les demandes de permis de bâtir qui lui étaient soumises avec les données personnelles et la signature des demandeurs, ainsi qu'avec le nom et la signature du fonctionnaire concerné, a débouché sur l'élaboration d'un nouveau formulaire de demande en ligne qui sera utilisé sur tout le territoire des Pays-Bas.

[18] Loi du 6 juillet 2000 sur les règlements applicables à la protection des données à caractère professionnel (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).

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

Suite à cela, la publication illicite de ces données personnelles a pris fin.

L'autorité néerlandaise de protection des données a déclaré illégal l'enregistrement détourné des adresses IP des visiteurs du site internet Geencommentaar.nl [aucuncommentaire], dans le but de rendre cette liste accessible à des tiers. En réponse à cette décision, le responsable du traitement des données a affirmé que la liste avait été détruite et que le logiciel avait été supprimé du site. Le site internet beoordeelmijnleraar.nl [évaluemonprof] a également été déclaré illicite. Son gestionnaire a donc apporté un certain nombre de modifications à celui-ci. En collaboration avec l'autorité indépendante des postes et télécommunications (*Onafhankelijke Post- en Telecommunicatie Autoriteit*, ou OPTA), le CBP est parvenu à ses fins dans ses efforts vis-à-vis des services de recherche inversée (utilisant un numéro de téléphone pour trouver le nom et l'adresse de l'abonné) ainsi que dans la définition des conditions dans lesquelles le marketing viral est autorisé.

Affaires et vie professionnelle

Les données médicales des travailleurs sont très sensibles. Suite à une enquête menée dans un service de santé et de sécurité sur le lieu de travail, l'autorité néerlandaise de protection des données soupçonne que d'autres services analogues divulguent eux aussi systématiquement ces données aux employeurs. Raison pour laquelle elle a décidé d'examiner le traitement des données au sein d'autres services du même type. Cette enquête se poursuivra en 2009.

Les données sensibles portant sur la situation financière des individus doivent elles aussi faire l'objet du plus grand soin. À deux reprises, le système national d'information sur les dettes (Landelijk Informatiesysteem Schulden) a soumis un modèle de système d'enregistrement à l'évaluation du CBP, lequel l'a rejeté dans les deux cas, estimant que le traitement des données était insuffisamment circonscrit et que les personnes disposant d'un accès à ces données étaient trop nombreuses. Il existait donc un risque de préjudices pour les personnes entrées par erreur dans la base de données.

L'un des problèmes structurels de la protection de la vie privée réside dans le fait que de nombreuses personnes ne savent pas où aboutissent leurs données ni comment celles-ci sont utilisées. Lorsque des personnes font l'objet d'une enquête de détectives privés ou du département de lutte contre la fraude sociale (Afdeling Sociale Recherche), celles-ci doivent en être informées une fois l'investigation terminée. Suite à son enquête, le CBP a établi que, dans de nombreux cas, cette obligation d'information n'est toujours pas observée. L'autorité néerlandaise continuera à faire preuve de vigilance. L'obtention de données susceptibles de déboucher sur une plus grande efficacité énergétique et sur une utilisation plus judicieuse de l'énergie doit aussi s'effectuer en conformité avec la Wbp. Plusieurs clauses de sauvegarde de la vie privée ont été ajoutées à la proposition législative relative à l'introduction de compteurs énergétiques intelligents, suite aux critiques exprimées par l'autorité néerlandaise de protection des données.

Transports

Après plusieurs années de querelles concernant l'utilisation des données relatives aux trajets à des fins de marketing, suite à l'introduction de la carte à puce des transports publics (OV-chipkaart) et après la publication d'une étude réalisée par le CBP quant à l'utilisation de la carte sur le réseau de métro amstellodamois, les compagnies de transport public ont enfin proposé un système répondant aux exigences de la Wbp. L'autorité de protection des données contrôlera la mise en œuvre de celui-ci et sa conformité aux normes définies. Une enquête officielle réalisée en 2008 sur le traitement des données personnelles en relation avec la carte à puce, qui sera obligatoire pour le métro de Rotterdam dès le 29 janvier 2009, a abouti à la conclusion qu'il n'y avait aucune raison de prendre d'autres mesures à ce stade. Le système de tarification au kilomètre peut lui aussi fournir une image détaillée du comportement de chaque automobiliste en matière de déplacements. Le CBP a plaidé en faveur d'une minimisation des données devant la Chambre basse du Parlement.

La surveillance des véhicules qui empruntent certains itinéraires concerne tous les citoyens qui conduisent, y compris ceux qui n'ont rien à cacher. L'autorité néerlandaise de protection des données a développé des lignes directrices concernant la reconnaissance automatique des plaques d'immatriculation. Ces consignes ont pour but de mettre un terme à l'absence de règles claires

quant à ce qui est permis ou non dans la mise en œuvre de cette méthode. La police n'est pas autorisée à conserver ni à traiter les données numérisées. Il s'agit d'éviter une situation dans laquelle tous les automobilistes sont considérés comme des suspects potentiels.

Soins de santé

Un soin particulier et des mesures de sécurité adaptées sont nécessaires lorsque l'on traite des données relatives à la santé de quelqu'un. Dans la proposition législative concernant le dossier médical électronique, il a été tenu compte de l'avis très critique rendu à cet égard par l'autorité néerlandaise de protection des données. En principe, seuls les professionnels entretenant une relation thérapeutique avec les patients doivent avoir accès à leurs dossiers médicaux.

L'autorité néerlandaise de protection des données souligne la nécessité pour les citoyens, et pour les patients en particulier, d'avoir le droit de savoir qui a accès à leurs données, quand et comment, et de savoir que ces données sont traitées en toute sécurité dans d'autres domaines où sont aussi échangées des données personnelles en matière de soins de santé. C'est notamment le cas lorsque les compagnies d'assurance-maladie fournissent à l'administration centrale des informations sur des assurés présentant des problèmes de santé et éligibles à une allocation. C'est aussi le cas quand un assureur révèle des données personnelles à un autre assureur lorsque des polices collectives sont transférées, ou lors du traitement à l'échelle nationale des données à des fins d'enregistrement global des soins au titre de la loi sur les frais médicaux exceptionnels (*Algemene wet bijzondere ziektekosten*). Ce principe s'applique aussi lorsque des données personnelles sont communiquées au Conseil des assurances-maladie (*College voor Zorgverzekeringen*) aux fins du recouvrement des primes des mauvais payeurs, ainsi que lorsque le numéro de registre des citoyens (*Burgerservicenummer*, ou BSN) est employé dans le secteur des soins de santé. Le traitement et la fourniture des données personnelles doivent alors répondre à un certain degré de sécurité.

Or, la conformité au niveau de sécurité requis ne va pas forcément de soi, comme l'a montré une enquête réalisée par l'autorité néerlandaise de protection des données en collaboration avec l'Inspection des soins de santé (*Inspectie voor de Gezondheidszorg*). Aucun des 20 hôpitaux passés au crible ne respectait cette norme, ce qui peut avoir des conséquences graves sur la qualité des soins fournis et sur le respect de la vie privée des patients. Les hôpitaux doivent faire la preuve de ce qu'ils observent la norme et de la procédure qu'ils suivent pour y parvenir.

Jeunes gens

Le traitement numérique des données personnelles en général et par le gouvernement en particulier requiert des garanties expresses. C'est d'autant plus vrai lorsque ces informations ont trait à des enfants ou à des jeunes gens.

En 2008, l'autorité néerlandaise de protection des données a rendu un avis très critique quant à la proposition de loi visant la création d'un indice de référence des jeunes à risque (*Verwijsindex Risicojongeren*). L'autorité était d'avis que cette proposition allait à l'encontre de la Wbp. Ses critiques portaient tout particulièrement sur l'objet de l'indice de référence, trop peu précis, ainsi que sur le manque de transparence des critères régissant l'enregistrement des jeunes gens par les personnes qui leur viennent en aide, lesquels comportent un risque presque inéluctable d'arbitraire. Bien que la proposition de loi soumise le 6 février 2009 réponde aux critiques soulevées par le CBP – entre autres – sur plusieurs points, l'essence du texte reste malheureusement inchangée.

On avance souvent que la réglementation en matière de respect de la vie privée empêche d'appliquer correctement les mesures de protection de l'enfance. Ce mythe a été démonté lors d'une table ronde qui s'est tenue en avril 2007 entre l'autorité néerlandaise de protection des données et des professionnels de l'aide à la jeunesse. Le CBP peut accepter la proposition d'amendement aux mesures de protection de l'enfance, car elle introduit un *droit* à la parole. Si les intérêts de l'enfant exigent que l'on rompe la confidentialité (médecin-patient), les prestataires des soins doivent pouvoir exercer ce droit.

Les écoles primaires transmettent des rapports pédagogiques sur leurs élèves aux écoles secondaires. L'autorité néerlandaise de protection des données a examiné la conformité à l'obligation d'information des parents des enfants concernés. Respecter cette obligation est capital

pour permettre, le cas échéant, de corriger le rapport, lequel peut avoir un effet négatif prolongé sur l'enfant s'il contient des données incorrectes ou obsolètes.

Police et autorités judiciaires

Les cas graves d'utilisation abusive de données personnelles sous la forme d'une usurpation d'identité devraient augmenter aux Pays-Bas. Pour lutter contre cette forme de vol de données personnelles, il est capital de se conformer à l'obligation d'information, de sorte que la personne concernée sache qu'une organisation traite ses données personnelles et quelles sont les données visées. En 2008, l'autorité de protection des données a exploré différentes manières de prévenir et de combattre les usurpations d'identité, en participant à des réunions d'experts et en étudiant la littérature spécialisée.

Garantir un usage correct et transparent des données personnelles est aussi vital à la lumière des pouvoirs renforcés dont disposent la police et les autorités judiciaires en relation avec le traitement des données personnelles. En 2007, l'autorité néerlandaise de protection des données avait estimé que la législation ouvrant la voie à une recherche de parenté basée sur l'ADN dans le cadre d'une procédure criminelle était en contradiction avec la Wbp. Le ministre a tenu compte de ces critiques dans un second projet présenté en octobre 2008.

Concernant la proposition du ministère public (Openbaar Ministerie) visant à étendre les rapports d'enquête, au moyen, par exemple, de l'internet et du téléphone, l'autorité néerlandaise de protection des données a recommandé l'inclusion de garanties appropriées afin de s'assurer que ces rapports ne soient pas extraits par les moteurs de recherche et que toute erreur puisse être rectifiée rapidement. Les instructions relatives aux rapports d'enquête (*Aanwijzing opsporingsberichtgeving*) seront modifiées suite à ces critiques. Le CBP a également émis un avis critique concernant la fourniture de données criminelles issues des bases de données du ministère public à des personnes concernées et à des tiers à des fins sans lien avec la procédure pénale. L'autorité considère que cela ne devrait être permis que dans certains cas, et uniquement lorsque cela s'avère absolument nécessaire. Le critère de l'opportunité n'est pas suffisant.

Le CBP a publié un rapport d'enquête sur l'échange interne de données personnelles au sein des forces de police via le bureau d'information policier. Il s'est avéré que la très grande majorité des zones de police n'étaient absolument pas équipées de manière à pouvoir répondre aux exigences de la loi sur les données policières (*Wet politiegegevens*) entrée en vigueur le 1er janvier 2008.

Pologne

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

Au cours de la période de référence, l'inspecteur général de la protection des données personnelles a pris des mesures en vue d'introduire des amendements à la loi relative à la protection des données concernant, notamment: l'optimisation de l'application des décisions administratives rendues par l'autorité de protection des données en relation avec les obligations non contractuelles; l'introduction dans la loi relative à la protection des données d'une clause pénale en cas d'entrave aux activités d'inspection; la définition de clauses concernant le contenu du protocole d'inspection dans la loi relative à la protection des données; les règles en matière de retrait du consentement au traitement des données personnelles (article 7, paragraphe 5, de la loi); la possibilité d'établir des antennes locales du bureau de l'inspecteur général pour la protection des données; les «approches» des autorités publiques, des entités sous administration autonome et des personnes physiques et morales qui traitent les données personnelles (introduction de l'obligation de répondre à une telle approche dans un délai de 30 jours à compter de la prise de contact); l'abrogation de l'article 29 de la loi relative à la protection des données (concernant la possibilité de révéler des données personnelles aux fins de l'inclusion de celles-ci dans un système d'archivage ou à d'autres fins). La divulgation de données personnelles ne doit avoir lieu qu'aux termes des dispositions de l'article 23 ou 27 de la loi relative à la protection des données.

À l'initiative de l'inspecteur général, un règlement a été adopté par le ministre des affaires intérieures et de l'administration concernant un modèle de formulaire pour la notification à l'inspecteur général des systèmes d'archivage en vue de leur enregistrement. L'objectif de ces nouvelles dispositions consiste à renforcer la transparence des formulaires et à définir les obligations essentielles des responsables du traitement des données ainsi qu'à aider les demandeurs à remplir leurs formulaires de notification, compte tenu du fait que l'ancienne procédure leur posait souvent de sérieux problèmes (la plupart des champs ont été remplacés par des cases d'option). Il convient de mentionner que l'inspecteur général a par le passé refusé à plusieurs reprises d'enregistrer un système d'archivage au motif que des erreurs avaient été décelées dans les formulaires de notification. Cette situation n'était pas sans avoir un impact négatif sur l'activité économique exercée par le demandeur, qui pouvait même se trouver dans l'impossibilité de la poursuivre.

B. Jurisprudence

La période de référence a vu la conclusion de la procédure judiciaire relative à la divulgation à des tiers, par l'opérateur de télécommunications Telekomunikacja Polska S.A., à des fins commerciales, des données personnelles d'abonnés ayant consenti à la communication de leurs données personnelles («opt-out») dans un répertoire téléphonique. Le tribunal administratif a estimé, conformément à l'avis de l'inspecteur général, que le consentement en question (c'est-à-dire l'absence d'objection) à la révélation de données dans un répertoire téléphonique ne revient pas à autoriser la divulgation desdites données à des tiers. Dans d'autres cas portant sur la facturation de frais pour la fourniture d'informations à des personnes concernées par BIK S.A. (agence d'information sur les crédits), le tribunal a suivi l'opinion de l'inspecteur général selon laquelle cette facturation est illégale. Ce dossier est actuellement en instance devant la Cour administrative suprême. Une autre décision importante portait sur l'interdiction de traiter des données personnelles enregistrées à des fins de sauvegarde après la suppression desdites données du système d'archivage. Le tribunal a conclu que de telles pratiques n'étaient pas admissibles. Il a été mentionné qu'une entité décidant d'effacer des données doit les supprimer complètement. Par ailleurs, la Cour administrative a rendu une décision quant à la légalité du traitement des données personnelles de clients de banques par BIK S.A. à des fins statistiques pendant une période de 12 ans (conformément à l'article 105, paragraphe 5, de la loi sur les opérations bancaires). L'inspecteur général pour la protection des données a examiné la question de la protection des données personnelles incluses dans les déclarations de patrimoine des personnes exerçant des mandats dans l'administration publique, dans l'optique de l'obligation de révéler les informations publiques. L'inspecteur général

a jugé illégale la divulgation des adresses où résident les personnes soumettant des déclarations de patrimoine ainsi que des adresses des biens immobiliers leur appartenant. Il s'est également penché sur la question de la publication, sur le site internet du Bulletin d'information public, de résolutions des conseils municipaux mentionnant les prénoms, noms ou adresses des personnes concernées par lesdites résolutions. Dans ce contexte, il a conclu que la révélation de données permettant une identification des personnes en question était inutile pour répondre à l'obligation d'information prévue par la loi sur l'accès aux informations publiques. L'inspecteur a aussi soutenu que de telles pratiques empiétaient sur le droit à la protection de la vie privée de ces personnes et que l'ampleur des données révélées n'était pas pertinente aux fins de la publication des résolutions. Le point de vue susmentionné a été étayé par la décision de la Cour administrative. En 2008, l'inspecteur général a également examiné la légitimité des demandes soumises aux éditeurs de presse, concernant notamment la communication des données personnelles de journalistes nécessaires à l'ouverture d'une action civile à l'encontre de ces personnes pour infraction aux droits individuels dans des publications. Dans la plupart des cas, l'inspecteur général a ordonné la divulgation de ces données, à moins que les données demandées n'aient effectivement été nécessaires pour intenter une action civile à l'encontre des personnes concernées, lorsque cette divulgation était conforme aux dispositions de l'article 29, paragraphe 2, de la loi sur la protection des données.

C. Questions diverses importantes

Dans le contexte de l'adhésion de la Pologne à l'espace Schengen, il a été nécessaire d'examiner l'exactitude du traitement des données personnelles dans le système d'information Schengen. Les entités habilitées qui disposent d'un accès direct au système d'information national en vue d'insérer des entrées dans le SIS et de consulter les informations qu'il contient (police, police des frontières, douanes et consulats) ont fait l'objet de contrôles. Au cours de ces inspections, certaines irrégularités ont été constatées (p. ex. absence d'un registre des personnes autorisées à accéder aux données du SIS, absence d'autorisations écrites, aucune spécification de la portée de l'autorisation à traiter les données personnelles et absence de badges pour le personnel habilité). À cet égard, l'inspecteur général a adressé une requête écrite au commandant en chef des forces de police, au chef de la police des frontières et au directeur des services douaniers leur demandant de prendre des mesures afin de remédier aux lacunes constatées.

En outre, certaines modifications ont été apportées au logiciel utilisé pour remplir les formulaires de notification relatifs à l'enregistrement des systèmes d'archivage de manière à réduire le nombre d'erreurs commises par les demandeurs lors de la préparation de leurs requêtes et de permettre à ceux qui ne possèdent pas de signature électronique sécurisée d'envoyer une demande. Ces changements amélioreront considérablement le processus de l'enregistrement des systèmes d'archivage de données et faciliteront le respect de l'obligation de notifier ce type de systèmes à des fins d'enregistrement pour les personnes qui y sont tenues. Le logiciel en question forme, avec le registre en ligne des systèmes d'archivage de données, la «plateforme électronique de communication avec l'inspecteur général pour la protection des données» (plateforme e-GIODO).

L'interprétation correcte des notions d'adresse IP, de courrier électronique, de cookie, de numéro IMEI, de nom d'utilisateur et de connexion a été analysée par le bureau de l'inspecteur général en réponse au nombre croissant de problèmes relatifs au traitement des données personnelles au moyen de technologies modernes. Cette analyse se voulait un outil utile pour évaluer au cas par cas, sur le plan légal, si les informations précitées peuvent être considérées comme des données personnelles. Par ailleurs, un groupe de travail spécial sur les technologies modernes a été mis sur pied au sein de bureau en vue de développer des opinions, avis juridiques, orientations, notes, politiques, etc. concernant les questions liées au traitement de données personnelles au moyen des technologies de l'information et de la communication au sens large.

En outre, l'inspecteur général a accueilli la 10e réunion des autorités de protection des données d'Europe centrale et orientale, qui s'est tenue du 1er au 4 juin 2008. Parmi les thèmes abordés à cette occasion, citons les questions relatives à la protection de la vie privée des enfants en ligne, les tâches effectuées par les autorités

de protection des données des PECO dans le contexte de l'expansion de l'espace Schengen ainsi que les qualifications, missions et pouvoirs des responsables de la protection des données. Ce forum a également évalué ses activités des dix dernières années. Deux déclarations finales ont été adoptées concernant la poursuite de la coopération au sein du forum et l'égalité de traitement des langues nationales de tous les États membres de l'UE.

Concernant les activités pédagogiques, les employés du bureau de l'inspecteur général ont organisé 62 formations sur la protection des données personnelles, notamment dans les contextes suivants: ministères, tribunaux, office de l'inspection des impôts, conseil national des conseils juridiques, consulat de la République de Pologne à Bruxelles, chambre nationale des conseillers fiscaux, office des marchés publics,… Au total, nous avons ainsi formé quelque 1 700 personnes. Dans le contexte de l'adhésion de la Pologne à l'espace Schengen, des cours spécifiques concernant le traitement des données personnelles contenues dans le SIS ont été organisés en vue de former le personnel des forces de police et de la police des frontières.

Par ailleurs, une nouvelle plateforme d'apprentissage en ligne, «eduGIODO», a été lancée dans le but de diffuser des connaissances sur la protection des données personnelles de manière pratique et moderne. Elle fournit à tous les intéressés une vaste gamme d'informations relatives à la protection des données, organisées en modules consacrés à des thèmes spécifiques (des «ABC»). Cette «université virtuelle» propose différents cours centrés sur la thématique particulière de la protection des données (droits des personnes concernées, principes généraux de la protection des données et obligations des responsables du traitement des données). Deux conférences nationales ont été organisées pour le lancement de la plateforme «eduGIODO», l'une à Varsovie et l'autre à Gdańsk. Les objectifs principaux de ce projet en relation avec les questions liées à la protection des données personnelles y ont été présentés.

Un atelier relatif aux amendements stipulés dans la législation européenne sur la protection des données dans le contexte de la mise en œuvre de l'acquis communautaire en la matière a été organisé par l'inspecteur général pour la protection des données personnelles dans le cadre du programme TAIEX. L'atelier était principalement destiné aux juges et aux procureurs.

L'année dernière, les employés du bureau de l'inspecteur général pour la protection des données ont participé au projet d'échange d'expériences entre autorités de protection des données. Ce projet a été mis sur pied dans le cadre du programme Leonardo da Vinci d'apprentissage tout au long de la vie intitulé «Nouvelles compétences des responsables de la mise en œuvre des dispositions en matière de protection des données». Il a eu pour effet de contribuer à améliorer les connaissances et compétences dans le domaine du droit communautaire, de favoriser l'échange d'expériences en relation avec les activités des autorités de protection des données, d'importer dans le système polonais des pratiques mises en œuvre dans le pays partenaire, d'accroître la mobilité des travailleurs et de renforcer les compétences linguistiques.
L'inspecteur général et l'Association du marketing direct ont signé un accord de coopération visant à améliorer la protection des données personnelles ainsi qu'à garantir le droit à la vie privée des citoyens dans le secteur du marketing direct.

Les activités pédagogiques occupent une place particulière dans les missions de l'inspecteur général pour la protection des données personnelles. Celles-ci sont notamment menées dans le cadre d'une vaste coopération avec les médias. En 2008, l'inspecteur général a donné quelque 100 interviews au cours desquelles il a présenté ses opinions ou commenté et précisé différentes questions relatives à la protection des données.

Portugal

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 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.

La directive 2006/24/CE (directive relative à la protection des données) a été transposée dans la législation nationale par la loi n° 32/2009 entrée en vigueur en août 2009, au terme d'une procédure législative amorcée en 2008 et au cours de laquelle le gouvernement, puis le Parlement, ont invité l'autorité de protection des données à rendre un avis sur le projet. Le texte définitif tient compte, dans une très large mesure, des remarques et suggestions formulées par l'autorité. La période de conservation maximale a été fixée à un an. Les délits pour l'investigation desquels les données de trafic peuvent être utilisées sont précisés dans la loi, de même que l'obligation pour les juges de demander directement les données aux fournisseurs de services de télécommunications lorsque cela se justifie. Une liste des collaborateurs autorisés à accéder aux données de trafic, à des fins prévues par la loi, doit être communiquée à l'autorité de protection des données, de même que des rapports réguliers quant aux données extraites. La communication entre les juges et les fournisseurs de services de télécommunications s'effectue en ligne, au moyen d'un formulaire spécifique.

B. Jurisprudence

Aucune.

C. Questions diverses importantes

Activités générales
L'autorité portugaise de protection des données a considérablement intensifié ses activités en 2008. Le nombre de notifications de traitement de données a doublé pour atteindre près de dix mille.

Pour faire face à cet important volume de travail, l'autorité prend actuellement des mesures en vue de simplifier et d'accélérer le processus décisionnel, sans que cela se fasse au détriment des analyses approfondies que requièrent certains dossiers.

Elle modifie aussi son système d'information, créé et développé par ses propres informaticiens, pour l'adapter à l'actuelle dématérialisation des procédures internes, dans l'optique de renoncer un jour complètement aux documents papier.

Si l'autorité de protection des données développe aussi la procédure de notification électronique pour tous types de traitement de données, en vue de simplifier la procédure pour les responsables du traitement des données et d'accélérer l'octroi des permis, elle a, en 2008, lancé deux notifications électroniques (e-notifications) spécifiques, dans le cadre d'une procédure entièrement automatisée, pour un programme de vidéosurveillance dans les écoles et pour le traitement des données sensibles dans le domaine de l'assistance aux victimes chez les enfants.

Un autre aspect important de l'activité de l'autorité de protection des données réside dans le conseil et la sensibilisation des responsables du traitement des données et des personnes concernées. En outre, il convient de souligner la participation accrue de l'autorité à des séminaires et conférences publics concernant la protection des données dans différents secteurs.

Avis sur des projets de loi
L'autorité de protection a été invitée à formuler 59 avis sur des projets de loi qui, par certains aspects, avaient trait à la protection des données. Les plus importants de ces projets concernaient la transposition de la directive 2005/60/CE sur le blanchiment d'argent et la lutte contre le terrorisme, le recensement de la population, l'amendement de la base de données des électeurs, le traitement des données dans le système judiciaire, la modification du Code du travail et le registre des événements relatifs aux véhicules. L'autorité a également été entendue par

le Parlement sur divers projets de loi dans le cadre de ses compétences consultatives.

La question de la mise en œuvre de la «plaque d'immatriculation électronique» a suscité beaucoup de débats au sein de l'opinion publique, et l'autorité y a fait figure de référence, en émettant des inquiétudes quant à ce projet. Selon le projet de loi à l'étude, ce dispositif sera obligatoire sur tous les véhicules et aura plusieurs objectifs: permettre aux services répressifs de détecter les infractions routières (absence d'assurance, retrait de permis de conduire, amendes impayées, etc.) et faciliter le règlement des péages au Portugal et au sein du système européen de péage électronique. La technologie retenue est le DSRC, qui a une portée de 1 000 mètres.

L'autorité de protection des données a soulevé deux grandes questions en relation avec le projet de loi: bien que la technologie envisagée soit moins intrusive que les options GPS, il convient encore de décider combien de lecteurs seraient installés, dans l'optique de prévenir la possibilité de tracer le parcours d'un véhicule. Cela étant, le dispositif étant obligatoire sur tous les véhicules, il devrait toujours être possible au conducteur de régler le péage de manière anonyme sans laisser de trace électronique permettant de le «suivre».

La loi a été approuvée au gouvernement en février dernier, et il a été décidé que, pour l'instant, ce dispositif ne serait utilisé que pour le règlement des péages. Tout autre usage a été exclu. Certaines règles doivent encore être fixées, et l'autorité participera à ce processus, de même qu'à l'octroi des autorisations pour tout autre traitement des données par la suite.

Projet DADUS

En janvier 2008, à l'occasion de la Journée européenne de la protection des données, l'autorité portugaise de protection des données a lancé un projet novateur appelé DADUS, destiné à introduire la protection des données dans les programmes scolaires, aux côtés des autres matières, suite à un accord avec le ministère de l'éducation et les autorités régionales en charge de l'éducation aux Açores et à Madère.

L'objectif de ce projet consiste à sensibiliser les jeunes à leurs droits en matière de protection des données et à leur fournir des orientations concernant une utilisation plus sûre des technologies de l'information et de la communication, au moyen d'un projet structuré, d'ampleur nationale, s'inscrivant sur le long terme, allant au-delà d'une simple campagne occasionnelle.

Ce projet vise les enfants entre 10 et 15 ans, et son contenu repose sur des plateformes basées sur le web. Ainsi, l'autorité a développé un site dédié pour le projet, sur lequel les enseignants peuvent obtenir un manuel de base de la protection des données, avec divers supports didactiques à utiliser en classe, ainsi qu'un blog permettant une participation active des jeunes, à l'école comme à la maison, et comportant des jeux, des conseils, des textes, des devoirs, des commentaires des élèves et des bandes dessinées.

Le site DADUS contient également un espace spécial dédié aux parents, comportant des informations claires et simples sur la protection des données, leur permettant de surveiller ce que font leurs enfants, et un forum de discussion où échanger leurs expériences, doutes et solutions.

L'année dernière, l'accent était mis sur la présentation du projet aux écoles et sur la distribution de brochures aux enseignants. Les premières réactions se sont révélées très positives et de nombreux professeurs ont immédiatement adhéré au projet pour l'année scolaire 2007-2008, y compris dans les écoles privées. Au cours de la première année du projet DADUS, près de 1 700 enseignants étaient déjà inscrits, et le site et le blog avaient reçu plus de 100 000 visites.

Roumanie

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 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 été modifiée par la loi n° 102/2005 sur la mise en place, l'organisation et le fonctionnement de l'autorité nationale de contrôle du traitement des données personnelles. Le principal amendement réside dans l'abrogation des dispositions relatives à la nécessité d'obtenir un accord préliminaire de l'organe d'investigation criminelle ou du tribunal compétent dans les cas où l'autorité de contrôle entend enquêter sur un traitement de données personnelles effectué dans un contexte pénal.

Une autre modification de la loi n° 677/2001 a été introduite par la loi n° 278/2007, sous la forme de la suppression des frais afférents aux notifications de traitement des données personnelles prévues par la loi n° 677/2001.
Aucune autre modification n'a été apportée à la loi sur la protection des personnes à l'égard sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données au cours de l'année 2008.

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 été transposée dans la législation nationale au moyen de la loi n° 506/2004 sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

La loi n° 506/2004 garantit la protection des données personnelles traitées par les fournisseurs de réseaux de communications électroniques publics, les fournisseurs de services à valeur ajoutée, ainsi que les fournisseurs de registres d'abonnés. Cette loi amende et précise le cadre juridique établi par la loi n° 677/2001 dans le secteur spécifique des communications électroniques.

La directive 2006/24/CE a été transposée dans la législation nationale par la loi n° 298/2008. Celle-ci avait pour objectif de réglementer, à l'échelle nationale, les obligations des fournisseurs de services et de réseaux de communication publics en matière de conservation des données générées ou traitées en relation avec leurs activités pendant une période de 6 mois à compter de la date de la communication électronique, afin de mettre ces données à la disposition des autorités compétentes dans le contexte d'enquêtes criminelles et de la prévention des délits.

En 2008, gardant à l'esprit le statut d'État membre de l'UE de la Roumanie, l'autorité de contrôle a pris en compte, dans le cadre de ses activités de réglementation dans le domaine de la protection des données personnelles, les questions spécifiques observées dans ses activités quotidiennes. Les décisions suivantes ont dès lors été adoptées: la décision n° 90/2008 concernant le niveau adéquat de protection personnelle à Jersey, la décision n° 95/2008 sur l'établissement du formulaire de notification harmonisé, prévu par la loi n° 677/2001, la décision n° 101/2008 sur le traitement des données personnelles relatives à l'état de santé, établissant un modèle d'autorisation pour le traitement desdites données personnelles.

En vue d'accélérer les procédures législatives nationales de mise en œuvre et d'harmonisation de l'acquis communautaire, applicables à divers secteurs d'activité, l'autorité de contrôle n'a eu de cesse de collaborer avec les institutions nationales en émettant des avis d'expert sur certains actes législatifs pendant leur procédure d'adoption. À cet égard, il convient de noter le projet de décision du gouvernement relatif à la procédure d'agrément des fournisseurs de services publics d'authentification électronique, le projet d'ordonnance d'urgence du gouvernement concernant les amendements à la loi sur le régime de libre circulation des citoyens roumains hors Roumanie, le projet d'ordonnance d'urgence du gouvernement sur la réglementation de l'usage des données personnelles dans le secteur policier – transposition de la recommandation 87, paragraphe 15, du

17 septembre 1987 du Conseil des ministres du Conseil de l'Europe.

L'autorité de contrôle a également émis plusieurs avis, opinions, recommandations et instructions en conformité avec les principes et dispositions établis dans les textes législatifs communautaires et nationaux relatifs au traitement des données personnelles.

B. Jurisprudence

Il a été constaté qu'en 2008, les tribunaux ont adopté une pratique standard dans les litiges liés à la protection des données personnelles.

En dépit de la nature très diversifiée des litiges portés devant les tribunaux et des situations soumises à un contrôle judiciaire, la législation sur la protection des données personnelles a fait l'objet d'une interprétation analogue à celle de l'autorité de contrôle.

Ainsi, suite à une enquête menée par l'autorité de contrôle auprès d'une entreprise privée, il a été constaté que cette entreprise traitait les données personnelles par courrier électronique. Une amende lui a donc été infligée pour avoir envoyé des communications commerciales non sollicitées par voie électronique. Le responsable du traitement des données a introduit un recours à l'encontre du rapport d'enquête.

Eu égard aux preuves soumises dans cette affaire, le tribunal s'est assuré que le responsable du traitement des données avait traité les données personnelles des personnes auxquelles il avait envoyé les communications commerciales sans que le destinataire soit en mesure d'exercer son droit de refus. En l'occurrence, le destinataire avait reçu plusieurs communications commerciales sans y avoir préalablement consenti.

À la lumière de ces découvertes, le tribunal a décidé que l'autorité de contrôle avait correctement établi l'existence d'un délit mineur et que l'amende infligée était légale.

Lors d'une enquête menée dans un club sportif, l'autorité de contrôle a constaté que celui-ci avait traité manuellement et automatiquement le numéro d'identification personnelle, le prénom et le nom de famille des supporters qui avaient souscrit un abonnement, sans les informer préalablement de ce traitement ni des droits dont ils disposaient en tant que personnes concernées.

L'autorité de contrôle a sanctionné le responsable du traitement des données pour ne pas avoir notifié aux supporters le traitement qui serait fait de leurs données personnelles et ne pas leur avoir fourni les informations dont ils auraient dû disposer sur leurs droits en tant que personnes concernées et sur les moyens de faire valoir ces droits.

Suite à cette amende, le responsable du traitement des données a émis une notification concernant le traitement qu'il ferait des données personnelles et a communiqué les informations requises par la loi n° 677/2001.

C. Questions diverses importantes

L'activité de contrôle de 2008 s'est concentrée sur les enquêtes prévues dans le plan annuel, ainsi que sur l'examen des cas potentiels de traitement illégal de données personnelles soulevés dans les plaintes et notifications adressées à l'autorité de contrôle.

La majorité des enquêtes *ex officio* se fondaient sur le plan d'investigation annuel élaboré sur la base des questions émergeant des activités de l'autorité, dans les secteurs où des infractions antérieures à la loi n° 677/2001 avaient été constatées et où peu de notifications avaient été soumises.

Ainsi, lors de la mise en œuvre du plan d'investigation annuel, quatre grands champs d'activité ont été surveillés:

- SWIFT;
- soins de santé et centres de maintenance;
- commerce en ligne;
- vidéosurveillance.

SWIFT: il a été décidé que plusieurs questions soulevées au sein du groupe de travail «Article 29», et plus particulièrement le contrôle des données personnelles traitées dans le système de transactions financières internationales (SWIFT), méritaient que des enquêtes *ex officio* leur soient consacrées dans le plan d'investigation annuel.

Dans le droit fil de ses activités de surveillance et de contrôle telles que définies par la loi n° 677/2001, l'autorité de contrôle a vérifié que les obligations légales imposées aux institutions financières par le transfert de données dans le cadre de transactions SWIFT à destination des États-Unis étaient observées et, au début de l'année 2008, elle s'est assurée que lesdites institutions respectaient leur obligation d'informer les personnes concernées.

Ces enquêtes ont révélé que les données sont transmises aux centres opérationnels SWIFT sur la base d'un contrat standard liant chaque participant à SWIFT. Ce contrat prévoit des clauses analogues pour tous les participants et garantit donc des modalités identiques pour le traitement des données personnelles et leur transfert aux centres opérationnels SWIFT.

En vue d'informer les personnes concernées quant au transfert de données SWIFT, les banques ont affiché des notes d'information dans leurs locaux et sur leurs sites internet, lesquelles contenaient des renseignements sur la possibilité d'un transfert aux autorités américaines, à leur demande, de données personnelles liées aux transactions effectuées via SWIFT après le 11 septembre 2001. Ces notes d'information indiquaient également que le ministère américain des finances était en droit de demander à accéder aux données personnelles des clients enregistrées au centre opérationnel SWIFT aux seules fins de la lutte contre le terrorisme et que ces données ne seraient conservées, dans un environnement sécurisé, que pendant la durée requise pour ce faire.

Les contrôles effectués ont révélé que certains responsables du traitement des données n'avaient émis aucune notification quant au traitement des données personnelles à ces fins et que certaines institutions bancaires et financières ne fournissaient pas d'informations adéquates aux personnes concernées comme le prévoit l'article 12 de la loi n° 677/2001. Il leur a donc été demandé de remédier à ces lacunes.

Les responsables du traitement des données ont suivi les recommandations de l'autorité de contrôle.

Soins de santé et centres de maintenance: les contrôles effectués pendant les enquêtes ont révélé que tous les responsables du traitement des données n'avaient pas émis de notification préalable concernant la manière dont ils traitaient les données personnelles.

Exemple: la société X a été sanctionnée pour ne pas avoir notifié les personnes concernées du traitement de leurs données personnelles dans le contexte de la fourniture de biens et de services avant le début des opérations de traitement et pour avoir traité illégalement des données personnelles, aucune information n'ayant été fournie aux personnes concernées à propos de leurs droits légaux.

Une recommandation a été émise dans le rapport d'enquête. Elle invitait le responsable du traitement des données à informer les personnes concernées de leurs droits légaux et de signer des clauses de confidentialité avec les membres du personnel qui ont accès aux données.

Comme il avait été remarqué que la société traitait aussi le numéro d'identification personnelle des clients ainsi que le numéro de compte bancaire, une décision a été émise en vue de mettre un terme au traitement de ces données, l'autorité considérant que cette procédure était excessive eu égard à l'objectif du traitement à des fins de «fourniture de biens et de services» et de «promotion, marketing et publicité», et de supprimer les données traitées avant cette décision.

D'autres contrôles effectués dans ce dossier ont prouvé que le responsable du traitement des données avait observé les mesures imposées par le rapport d'enquête, étant donné qu'il avait cessé de traiter les numéros d'identification personnelles et les numéros de compte bancaire à des fins de «fourniture de biens et de services» et de «promotion, marketing et publicité», et avait supprimé les données traitées jusque là.

Suite aux enquêtes réalisées dans ce secteur spécifique, le nombre de notifications soumises par les responsables du traitement des données a considérablement augmenté, ce qui indique qu'ils sont davantage conscients de leurs obligations en matière de protection des données personnelles.

Commerce en ligne: eu égard au fait que cette activité implique le traitement des données personnelles

d'individus, en ce comprises des données sensibles (p. ex. numéro d'identification, numéro de série et numéro des documents d'identité), ainsi qu'aux risques que comporte la collecte desdites données sur l'internet, l'autorité de contrôle a effectué plusieurs enquêtes auprès de sociétés privées pratiquant la vente en ligne.

Les rubriques «Conditions générales» et «Politique de confidentialité» publiées sur les sites internet des responsables du traitement des données contiennent des informations expliquant pourquoi les données personnelles sont collectées et enregistrées, et indiquent que les données ne seront pas divulguées à des tiers. Toutefois, ils ne fournissent aucun renseignement quant aux droits que confère aux clients la loi n° 677/2001.

Les contrôles effectués ont révélé que la plupart des responsables du traitement des données n'avaient pas émis de notification concernant le traitement réservé aux données personnelles dans ce but avant l'enquête, mais qu'ils observaient l'obligation après celle-ci.

Exemple: une enquête menée en 2006 au sein d'une entreprise dont l'activité consistait en la vente de produits en ligne a révélé que le responsable du traitement des données traitait, via son site internet dédié, les informations personnelles des personnes intéressées par les offres de l'entreprise et celles de ses clients (personnes physiques) et gérait les enregistrements de ces données par voie électronique et sur papier, tombant ainsi sous le coup de la loi n° 677/2001. Les visiteurs du site étaient invités à fournir, via le formulaire en ligne, des données personnelles telles que: prénom, nom, numéro d'identification personnelle, adresse de livraison, adresse électronique et numéro de téléphone. Selon les déclarations faites par les représentants de l'entreprise, il n'était pas obligatoire de fournir un numéro d'identification personnelle pour l'émission d'une facture, et aucun autre motif n'a pu être fourni pour la collecte de ce type de données.

Par ailleurs, la rubrique «Conditions générales» du site internet incluait une note d'information indiquant les catégories de personnes concernées (clients, personnes physiques), mais aucune référence à la loi n° 677/2001 ni aux droits des personnes concernées et aux moyens dont elles pouvaient les faire valoir conformément à l'article 12, paragraphe 1, de la loi n° 677/2001.

À la lumière des problèmes relevés au cours de l'enquête, le responsable du traitement des données a été sanctionné pour ne pas avoir émis de notification en relation avec le traitement des données personnelles et pour avoir traité illégalement lesdites données, puisqu'il n'avait pas fourni d'informations adéquates (complètes) aux personnes concernées.

Suite à l'enquête, il a été noté que le formulaire de commande posté sur le site internet avait été modifié et que la fourniture du numéro d'identification personnelle n'était plus obligatoire.

S'appuyant sur les conclusions de l'enquête, l'autorité de contrôle a émis une décision en vertu de laquelle elle exigeait la suppression des numéros d'identification personnelle enregistrés dans la base de données de la société, le responsable du traitement des données n'ayant pas été en mesure de justifier le traitement de ceux-ci, conformément aux dispositions des articles 4 et 8 de la loi n° 677/2001.

Le responsable du traitement des données observe désormais les mesures imposées par l'autorité.

Vidéosurveillance: l'autorité de contrôle a reçu, au cours de l'année 2008, un grand nombre de plaintes relatives au respect de l'obligation de notification par divers organismes publics utilisant des équipements de vidéosurveillance.

En conséquence, l'autorité a réalisé plusieurs enquêtes en relation avec le traitement des données personnelles au moyen d'équipements de vidéo surveillance, *ex officio* ou après avoir reçu des plaintes ou des informations de personnes concernées.

Lors de ces enquêtes, les points suivants ont fait l'objet d'un contrôle: respect, par les responsables du traitement des données, des mesures de sécurité minimales, établissement d'un objectif légitime et explicite, prévention du stockage excessif de données personnelles traitées au moyen de la vidéosurveillance, octroi à la personne concernée de la possibilité d'exercer ses droits (légaux) et prévention des divulgations de données traitées de cette manière sans motif légal.
Les responsables du traitement des données justifiaient l'installation de caméras de vidéosurveillance par la prévention des vols et autres activités illégales. Les images collectées

sont stockées sur des serveurs pendant un certain temps, selon la capacité de l'unité de stockage, après quoi elles sont supprimées automatiquement. Elles ne sont fournies à la police que lorsque des délits sont commis, et uniquement en réponse à une demande officielle.

Exemple: le responsable du traitement des données soumis à une enquête après une plainte, traitait des données personnelles, à savoir les images obtenues au moyen de caméras de vidéosurveillance installées dans un restaurant.

L'investigation a révélé que des caméras étaient également installées dans les toilettes et permettaient d'identifier les personnes. L'objectif déclaré du système de surveillance était, selon le responsable du traitement des données, de s'assurer de la «sécurité des lieux et des marchandises ainsi que de la prévention des délits».

L'avertissement quant à la présence de caméras de vidéosurveillance n'était affiché qu'à l'entrée du restaurant.

Le responsable des données n'ayant pas indiqué qu'il traitait des données personnelles, il s'est vu infligé une amende pour absence de notification et pour notification trompeuse.

Suite à l'enquête, et tenant compte du fait que les toilettes sont un espace privé réservé aux seuls visiteurs qui les fréquentent à un moment donné, l'autorité de contrôle a considéré qu'installer un système de vidéosurveillance dans ces pièces était excessif, s'inscrivant ainsi dans le droit fil de l'opinion exprimée par le groupe de travail «Article 29» dans son avis n° 67/2002 sur le traitement des données personnelles au moyen d'équipements de vidéosurveillance.

À la lumière des problèmes déjà évoqués, l'autorité de contrôle a émis une décision demandant l'arrêt du traitement des images des personnes utilisant les toilettes du restaurant ainsi que la suppression des données collectées jusque là.

Dans le cas de systèmes de vidéosurveillance installés en vue de répondre aux obligations imposées par la loi n° 4/2008 sur la prévention de la violence lors des événements sportifs, l'autorité de contrôle a mené l'enquête au sein des grands clubs de football de Bucarest et d'autres villes. Celle-ci a révélé que, dans la majorité des cas, aucune information préalable quant au traitement des données personnelles (images) n'était fournie. Raison pour laquelle les responsables du traitement des données se sont vu imposer une amende.

Par la suite, dans la plupart des cas, les responsables du traitement des données ont pris des mesures afin de s'assurer que les visiteurs des stades de football étaient bien informés de la présence d'équipements de vidéosurveillance au moyen d'affichettes placées à des endroits visibles et d'avertissements verbaux émis pendant les manifestations.

Au cours de l'année 2008, en plus du plan approuvé, des enquêtes ont également été menées dans les domaines suivants:

- traitement des données personnelles dans le cadre du *programme national d'évaluation de l'état de santé de la population en matière de soins primaires*;
- traitement des données personnelles des patients au sein du *système de classification des groupes diagnostics*.

Suite aux enquêtes, le nombre de notifications reçues de responsables du traitement des données dont les activités sont soumises au contrôle de l'autorité a considérablement augmenté.

La résolution des plaintes découlant des activités de l'autorité de contrôle est une question capitale. En 2008, le nombre de plaintes reçues a augmenté d'un facteur de 11 en comparaison avec 2007, ce qui montre clairement que le grand public est beaucoup plus au fait des pouvoirs de l'autorité de contrôle et des dispositions en matière de protection des données personnelles et que les citoyens montrent un intérêt accru pour les activités de notre autorité. La majorité des plaintes portaient sur la réception de communications commerciales non sollicitées, sur la communication des données personnelles de débiteurs au bureau des crédits et au centre de risques des banques ainsi que sur la divulgation illégale de données comme celles-là dans d'autres situations.

Slovaquie

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

Un changement mineur, mais néanmoins très important, dans le domaine de la réglementation législative régissant l'existence factuelle et le fonctionnement du Bureau pour la protection des données personnelles de la République slovaque (ci-après dénommé «le Bureau») a été réalisé. Cette modification particulière, la loi n° 428/2002 Coll. relative à la protection des données personnelles (ci-après dénommée «loi n° 428/2002 Coll.»), a elle-même été amendée, le «programme budgétaire sur la protection des données» ayant été transféré de la catégorie budgétaire des services du gouvernement de la République slovaque vers la catégorie de l'administration générale du Trésor. Ce transfert a officiellement renforcé l'indépendance du Bureau en matière budgétaire. Au cours du prochain exercice budgétaire, il ne sera plus nécessaire de soumettre le budget pour approbation dans le cadre du budget des Services du gouvernement. Cet amendement législatif permet néanmoins de ne tenir aucun compte des besoins financiers du Bureau, étant donné que la catégorie de l'administration générale du Trésor relève de l'administration du ministère des finances dont le budget est soumis à la négociation et à l'approbation du Conseil national de la République slovaque.

B. Jurisprudence

En 2005, le Bureau a émis un ordre requérant de l'autorité administrative de l'État, en tant que responsable du système d'archivage, de mette un terme à la divulgation du numéro d'identification nationale (un identifiant d'usage général) de personnes concernées sur le site internet du journal officiel. Le responsable du traitement des données a également été prié de supprimer de son site internet tous les numéros d'identification nationale précédemment publiés. Le destinataire de l'ordre a fait appel de cette décision auprès du Bureau. Cet appel a été déclaré irrecevable. Le responsable du traitement des données a introduit une requête auprès des tribunaux en vue d'obtenir l'annulation de la décision du Bureau. Le tribunal a rejeté la requête et, dans son avis, a statué que la publication de données personnelles est une opération de traitement spécifique. L'une des principales spécificités de cette opération réside dans le fait qu'il s'agit d'un processus qui n'est pas tout à fait réversible et qui comporte diverses conséquences susceptibles d'avoir, en cas de divulgation illégal, un impact négatif sur la personne concernée. La divulgation de numéros d'identification nationale est particulièrement sensible. Enfin, la législation interdit explicitement la divulgation d'un «identifiant d'usage général». Selon le tribunal, la décision du Bureau s'appuyait sur une base appropriée et était conforme aux compétences que lui confère la loi.

C. Questions diverses importantes

Activité d'inspection et émission de notifications
Le département d'inspection du Bureau assure une supervision indépendante de la protection des données personnelles et, du fait de ses activités, renforce la protection d'autres droits et libertés fondamentaux des personnes physiques. Les activités du département d'inspection se concentrent essentiellement sur le contrôle des systèmes d'archivage des responsables et agents du traitement des données, ainsi que sur la gestion des notifications des personnes concernées et d'autres personnes affirmant que les droits dont elles jouissent en vertu de la loi n° 428/2002 Coll. ont été directement affectés.

Contrôle de la protection des données personnelles en chiffres
En 2008, 113 notifications ont été introduites auprès du Bureau par des personnes concernées et autres personnes physiques se plaignant d'une violation de la protection de leurs données personnelles. 65 autres notifications portaient sur des soupçons d'infraction à la loi sur la protection des données. L'inspecteur en chef du Bureau a ordonné 74 procédures *ex officio* à l'encontre de responsables de systèmes d'archivage. 21 notifications datant de 2007 étaient toujours en instance. Au total, en 2008, le département d'inspection a traité 273 notifications. Il a ainsi réalisé 105 contrôles et adressé 34 «demandes d'informations» aux responsables et agents de traitement de systèmes d'archivage. Quelque 75 ordres ont été émis en vue de l'élimination des lacunes identifiées par l'inspection. Un seul responsable du trai-

tement des données a fait usage de son droit d'appel. Son appel a été rejeté.

En 2008, 142 des 252 nouvelles notifications concernaient des responsables du traitement des données issus du secteur privé, et 61 des agents de l'administration publique, généralement soumises par d'autres organes publics. Dans 28 cas, le Bureau a enquêté sur des notifications portant sur des instances gouvernementales autonomes. 8 affaires avaient trait à des organisations de la société civile, des fondations, des partis ou mouvements politiques et des églises ou groupes religieux reconnus. Des institutions de l'administration publique ont fait l'objet d'une enquête à quatre reprises. Dans 9 cas, la notification avait été introduite à l'encontre d'une personne qui n'était pas responsable du système d'archivage au sein de la loi n° 428/2002 Coll.

Sur les 113 notifications soumises par des personnes concernées en 2008, le Bureau a clos 99 dossiers, dont 71 dans le délai légal de base de 60 jours. Si l'examen des autres notifications a duré plus longtemps, c'est qu'il a fallu consulter d'autres institutions, que les systèmes d'archivage ont dû faire l'objet d'une investigation dans les locaux du responsable du traitement des données, que la collecte d'autres éléments de preuve s'est révélée nécessaire ou que les pétitionnaires ont demandé à pouvoir coopérer. Un total de 50 notifications, parmi toutes celles traitées, a été jugé non fondé.

Si un informateur n'est pas satisfait de la suite donnée à sa notification par le Bureau, il peut la réintroduire dans le délai légal de 30 jours. Sur les 99 affaires clôturées en 2008, seules deux ont fait l'objet d'une nouvelle notification au Bureau. Les 97 autres informateurs, soit plus de 96 % d'entre eux, dont les notifications ont été examinées en 2008 ont respecté la décision finale rendue par le Bureau. Au cours de l'année 2008, le département d'inspection a communiqué quatre notifications aux services répressifs.

Il a, au cours de la même année, infligé 14 amendes, d'un montant total de 1 045 000 SKK (34 687,65 EUR) D'une manière générale, les sanctions se trouvaient dans la moyenne basse des amendes possibles, le Bureau disposait d'une certaine marge de manœuvre à cet égard. La pénalité la plus importante infligée s'élevait à 250 000 SKK (8 298,5 EUR).

Activités d'inspection du Bureau à l'échelle nationale

Inspections des systèmes de vidéosurveillance dans les villes et municipalités

En 2008, le département d'inspection a effectué des contrôles sur des systèmes de vidéosurveillance. Cette inspection menée à l'échelle nationale avait pour but d'examiner les systèmes de vidéosurveillance utilisés par les villes et municipalités. Le département a ainsi réalisé 12 contrôles, dont 7 en 2007. Des lacunes ont été constatées dans tous les cas, et les responsables du traitement des données ont été priés d'y remédier. Les problèmes les plus fréquents étaient les suivants: les zones accessibles au public faisant l'objet d'une surveillance n'étaient pas clairement identifiées comme telles, le système d'archivage n'était pas documenté, les enregistrements n'étaient pas détruits au terme du délai prévu par la loi n° 428/2002 Coll. et les responsables n'avaient pas pris les mesures techniques, organisationnelles et humaines requises, sous la forme de directives de sécurité portant sur le système d'archivage vidéo.

Inspections visant le traitement des données personnelles par les exécuteurs testamentaires, notaires et représentants légaux

En 2007, on avait constaté que plusieurs exécuteurs testamentaires s'étaient écartés du cadre de la loi n° 428/2002 Coll. en révélant les numéros d'identification nationale de personnes concernées au tableau officiel (annonce de l'ouverture d'une exécution testamentaire, annonce d'enchères). Les inspections réalisées auprès de leurs bureaux en 2008 ont elles aussi révélé des lacunes dans la mise en œuvre des dispositions de la loi n° 428/2002 Coll. relatives à la sécurité du traitement des données personnelles, surtout dans le cas où le système d'archivage utilisé pour le traitement des données personnelles était connecté à l'internet.

Le département d'inspection a vérifié la conformité à la loi n° 428/2002 des systèmes et procédures de certains cabinets d'avocats et études de notaires slovaques.

L'examen portait notamment sur les points suivants:
- conseil des personnes habilitées;

- contenu des contrats entre responsables et agents du traitement des données;
- conservation des dossiers des ressources humaines, systèmes d'archivage des ressources humaines et systèmes d'informations clients;
- désignation d'un responsable de la protection des données personnelles;
- existence d'un projet ou de directives en matière de sécurité et qualité de ceux-ci.

Le Bureau a ordonné aux instances concernées de remédier aux manquements identifiés, après quoi l'Inspecteur en chef a réalisé une analyse détaillée de l'ensemble du dossier, en concertation avec les représentants compétents du Barreau slovaque et de la Chambre slovaque des exécuteurs testamentaires et de la Chambre des notaires de République slovaque, lesquels sont idéalement placés, de par leur position, pour fournir aux instances concernées des orientations quant à la manière de remédier au plus vite aux lacunes constatées.

Inspections visant le traitement des données personnelles par les responsables du secteur des soins de santé

En 2008, le Bureau a examiné plusieurs notifications émises par des personnes concernées à l'encontre des responsables du traitement des données dans le secteur des soins de santé. Le nombre de ces notifications et l'importance de certaines d'entre elles étant colossales, l'inspecteur en chef a décidé de mener l'enquête afin de vérifier dans quelle mesure les responsables du traitement des données dans le secteur des soins de santé observaient les dispositions de la loi n° 428/2002 Coll. relatives au traitement des données personnelles des patients. Le département d'inspection a ainsi contrôlé des institutions de soins privées et publiques (hôpitaux et cabinets de consultation), des pharmacies et des compagnies d'assurance-maladie. Dans la plupart des cas, les responsables du traitement des données n'avaient pas établi de directives de sécurité définissant clairement les compétences et les fonctions des personnes habilitées, ou leurs responsabilités en relation avec les différents types d'opérations effectuées sur les données personnelles, même dans des situations d'exception (p. ex. fermeture ou déménagement d'un cabinet de consultation ou d'un hôpital). Dans plusieurs cas, le Bureau a noté que des données personnelles étaient obtenues ou divulguées de manière indiscrète dans les services de soins et pharmacies. Il a par ailleurs eu à traiter des soupçons de fuites de données personnelles à destination des compagnies d'assurance-santé concernant les nouveau-nés.

Activités d'inspection spéciales menées dans le cadre de l'adhésion de la République slovaque à l'espace Schengen

Dans le cadre des préparatifs à l'adhésion de la République slovaque à l'espace Schengen, le département d'inspection a réalisé, en 2008, de nouveaux contrôles dans certaines ambassades de la République à l'étranger. Son but était de vérifier si les responsables des systèmes d'archivage observaient bien la loi 428/2002 Coll., si les procédures d'émission des visas Schengen répondaient aux exigences du catalogue Schengen (recommandations et meilleures pratiques) en la matière. En mars 2008, les départements consulaires des ambassades de la République slovaque au Koweït et à Damas ont été contrôlés. En mai 2008, c'était le tour de ceux de Prague et de Brno. La légalité du traitement des données personnelles conformément à l'actuelle version du Système d'information Schengen (SIS I) a été contrôlée au bureau national de SIRENE, au bureau de la coopération policière internationale et au présidium des forces de police.

Coopération internationale

Le Bureau participe régulièrement aux ateliers internationaux organisés au printemps et à l'automne pour les inspecteurs des autorités de protection des données personnelles. Lors de l'atelier de l'automne 2007, organisé à Lisbonne par l'autorité portugaise de protection des données personnelles, il a été décidé que le XVIIIe atelier international des inspecteurs, programmé pour l'automne 2008, aurait lieu en Slovaquie. Cet atelier s'est tenu les 29 et 30 septembre 2008 à Bratislava. Outre les inspecteurs des États membres de l'Union européenne, l'atelier a également accueilli des inspecteurs de pays candidats qui se préparent à rejoindre l'Union européenne. En tout, 63 participants et 10 collaborateurs du Bureau ont pris part à l'atelier. Deux délégués représentaient le Bureau du Contrôleur européen de la protection des données. Les travaux ont été ouverts par le président de la commission parlementaire sur les droits de l'homme, les minorités et le statut des femmes et le président du Bureau. Les inspecteurs ont

abordé cinq thèmes fondamentaux dans le cadre des ateliers suivants:

1. Gestion des plaintes: pouvoirs des autorités de contrôle en matière de gestion des plaintes
2. Échange des meilleures pratiques issues des inspections menées dans les départements consulaires des ambassades concernant la délivrance des visas Schengen
3. Équilibre des intérêts: protection des données personnelles vs. médias de masse
4. Application de mesures de sécurité dans le traitement des données à caractère personnel
5. Traitement des données personnelles en matière d'emploi

Le département d'inspection a présenté les sujets suivants:

- Réalisation des contrôles et règles internes régissant les contrôles
- Documentation et désignation d'un responsable de la protection des données personnelles
- Personne habilitée: mesures organisationnelles et humaines
- Cadre juridique et conditions pour la préparation d'un projet de sécurité
- Cadre juridique du traitement des données personnelles au moyen d'un système de vidéosurveillance et expérience du Bureau dans l'inspection de systèmes de vidéosurveillance

Flux transfrontaliers de données personnelles

Au cours de la période de référence, le Bureau a approuvé trois flux transfrontaliers de données personnelles. Ces flux concernaient des données personnelles traitées dans le contexte de l'emploi, de la gestion des ressources humaines et de l'externalisation d'opérations de traitement. Une décision relative à un transfert transfrontalier à destination d'un pays ne fournissant pas un degré adéquat de protection a été émise vis-à-vis du responsable du traitement des données (importateur) basé en Inde, sur la base des dispositions légales stipulant qu'il est nécessaire d'inclure des clauses contractuelles standard dans le contrat. Deux autres décisions visaient des importateurs américains, suite à l'auto-certification des importateurs dans la «sphère de sécurité» («Safe Harbour»). Sur la base des documents reçus, il est apparu que les responsables du traitement des données ne savaient pas comment utiliser les décisions arrêtées par la Commission européenne en vue de fournir des garanties suffisantes pour la protection des données personnelles pendant et après leur transfert vers des pays tiers. Le Bureau a également traité des demandes d'«enregistrement spécial» portant sur un système destiné à signaler les soupçons d'actes illicites ou contraires à l'éthique (système de dénonciation) ainsi que des requêtes associées concernant l'approbation du transfert desdites données à des agents de traitement basés aux États-Unis. Le Bureau a également émis plusieurs avis relatif à l'interprétation à donner à la loi n° 482/2002 Coll. et aux opinions du groupe de travail «Article 29» à cet égard. Au cours de la période de référence, le Bureau a émis une décision négative concernant l'enregistrement spécial sur la base du traitement des données fournies par l'entremise du système de dénonciation, avant de revenir sur sa décision une fois tous les manquements identifiés éliminés. Concernant les systèmes de dénonciation, aucun transfert de données à destination de pays tiers n'a été autorisé par le Bureau. Après examen des demandes, le Bureau en est arrivé à la conclusion que ceux-ci ne comportaient pas les éléments nécessaires en vue d'une approbation. En effet, ces systèmes de dénonciation, très généraux, allaient bien au-delà du champ d'application de la loi n° 428/2002 Coll. Il convient de noter qu'il s'agissait exclusivement de systèmes développés à l'étranger, qui fonctionnaient déjà de longue date.

Coopération internationale

Des réunions bilatérales se sont tenues en vue de régler certains problèmes, de mettre une coopération sur pied ou d'échanger de bonnes pratiques. Y ont assisté le président du Bureau et les experts compétents.

Mai 2008: réunion bilatérale avec l'Office pour la protection des données à caractère personnel de la République tchèque, à l'initiative du Bureau slovaque, en Slovaquie. Cette réunion avait pour objet les situations qui donnent lieu à des échanges de meilleures pratiques en matière d'activités d'inspection:

- Utilisation des documents officiels dans la pratique: la carte d'identité et le passeport en tant que documents européens. Législation relative aux documents officiels; ampleur des données personnelles fournies dans les documents officiels.

- Traitement et divulgation de données personnelles issues des registres centraux (systèmes d'archivage) du ministère de la justice de la République slovaque en matière judiciaire (p. ex. Journal officiel des décisions judiciaires, collection de documents).
- Inspection sur le site des instances contrôlées (responsable/agent du traitement des données) sans nécessité de préavis. Coopération de différents organes et autorités de l'administration publique avec l'autorité de protection des données en République slovaque et tchèque.

Avril 2008: visite au Bureau de l'inspecteur général pour la protection des données de Varsovie (Pologne).
Cette visite avait pour but de se familiariser avec la structure organisationnelle et les activités de l'autorité polonaise de protection des données (GIODO). À cette occasion, les présidents des deux autorités ont accordé un entretien au quotidien «Rzeczpospolita».

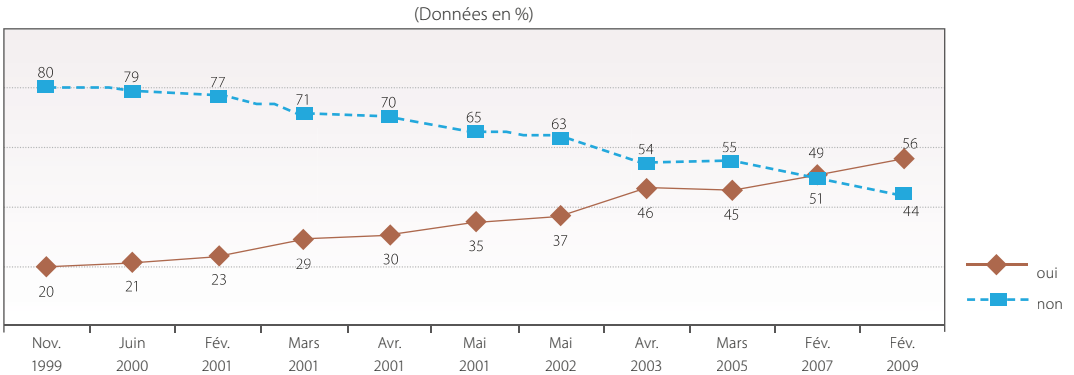
Avril 2008: visite à l'Office national pour la protection des données à caractère personnel de Bucarest (Roumanie).
Le programme de la visite était en lien avec une réunion bilatérale antérieure consacrée à la préparation de la Roumanie à son adhésion à l'espace Schengen, qui s'était tenue à Bratislava, et il a été étendu aux échanges de meilleures pratiques, notamment en relation avec les spécificités de l'autorité roumaine de protection des données en matière d'indépendance.

Sensibilisation de l'opinion publique à la protection des données personnelles
Depuis 1999, l'institut de sondage de l'Office statistique de la République tchèque a réalisé plusieurs enquêtes, à l'initiative de l'autorité de protection des données, sur des questions liées à la protection des données. La dernière en date remonte à février 2009.

Comme le montre ce graphique, ces deux dernières années, de février 2007 à février 2009, la sensibilisation de toutes les catégories de citoyens aux droits à la protection des données personnelles s'est accrue de 5 %. Dans l'ensemble, entre novembre 1999 et février 2009, c'est de 36 % qu'elle a augmenté.

Généralement, on peut affirmer que la sensibilisation la plus grande (supérieure à la moyenne slovaque) se manifeste chez les citoyens âgés entre 30 et 39 ans (68 %) et entre 40 et 49 ans (66 %), chez les répondants ayant un diplôme universitaire (87 %), chez les répondants qui ont terminé l'école secondaire (67 %), ainsi que chez les hommes d'affaires (70 %), les employés (74 %) et les personnes résidant dans des villes de plus de cent mille habitants (76 %).

Connaissez-vous vos droits relatifs à la protection des données personnelles résultant de la loi n° 482/2002 Coll. sur la protection des données à caractère personnel?



Slovénie

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

L'adoption de la loi sur la protection des données personnelles[20], de la loi sur le commissaire à l'information[21] et la mise en place du commissaire à l'information[22] en tant qu'autorité indépendante de protection des données a assuré la transposition complète de la directive 95/46/CE dans la législation slovène.

S'appuyant sur les dispositions spécifiques de l'article 48 de la LPDP, le commissaire à l'information a émis plusieurs avis *a priori* sur la législation en préparation, concernant la conformité de celle-ci à la protection des données personnelles. Les principaux textes examinés en 2008 concernaient les lois sur les cartes d'identité personnelles, les immigrants, le registre judiciaire, les communications électroniques ainsi que divers règlements relatifs à la santé publique et à l'assurance-maladie, à l'assistance juridique gratuite, etc.

Dans le cadre de sa mission, le commissaire a rencontré un problème en relation avec l'acquisition des données de localisation des téléphones portables dans les cas où la vie ou l'intégrité physique d'une personne sont en danger, sans rapport avec une procédure criminelle, et où la police a besoin d'obtenir ces données lors de la réception d'un appel d'urgence. À cet égard, le commissaire a suggéré que des amendements soient apportés à la loi sur les communications électroniques[23]. Selon les amendements proposés, dans la situation décrite ci-avant, la police aurait le droit de demander les données relatives à la dernière position connue du dispositif mobile d'une personne dont l'intégrité physique ou la vie sont en danger. Elle conserverait ces informations de manière permanente, et le commissaire vérifierait les modalités de leur conservation au moins une fois par an. Cet amendement constitue également une transposition adéquate de l'article 5 f de la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 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.

[20] Adoptée en 2004 et modifiée en 2007 (Journal officiel de la République de Slovénie, n° 94/2007, texte officiel consolidé), ci-après dénommée: LPDP.

[21] Journal officiel de la République de Slovénie, n° 113/2005.

[22] Entré en fonction le 1er janvier 2006.

[23] Journal officiel de la République de Slovénie, n° 13/2007.

B. Jurisprudence

En 2008, le commissaire à l'information a eu à traiter plusieurs cas dont les médias nationaux se sont largement fait l'écho.

Utilisation abusive des données de trafic relatives aux communications téléphoniques par le ministère des affaires étrangères

Le commissaire à l'information a émis une décision réglementaire dans une affaire ouverte à l'encontre du ministère des affaires étrangères, concernant la légalité du traitement de données personnelles au moyen de l'obtention d'un relevé des numéros de téléphone, tant des appels sortants qu'entrants, d'un réseau de téléphonie fixe. Ordre a été donné au ministère de détruire le CD sur lequel se trouvait la liste en question.

Aux fins d'une enquête réalisée en interne au ministère, et dans le but d'identifier l'employé qui avait transmis un courrier diplomatique au journaliste d'un quotidien, toutes les données de trafic avaient été collectées au cours d'une période donnée. Une base de données contenant environ 110 000 éléments d'information avait ainsi été créée.

Conformément à la loi sur les communications électroniques, les données de trafic se sont vu accorder une double protection, à savoir celle de la confidentialité de la correspondance et des autres moyens de communication, conformément à l'article 37 de la Constitution de la République de Slovénie (ci-après désignée «la constitution»), et celle conférée aux données personnelles en vertu de l'article 38 de la constitution. Les données de trafic étant considérées comme des données personnelles puisqu'elles ont trait à une personne physique identifiée ou identifiable, dans le cas d'une intervention illicite comme celle-ci, il existe une double violation des droits, affectant d'une part les employés du ministère et d'autre part leurs interlocuteurs (appelants ou appelés).

L'article 37, paragraphe 1, de la constitution garantit la confidentialité de la correspondance et des autres moyens de communication. Le paragraphe 2 du même article stipule que seule une loi peut prescrire la levée de cette protection et de l'inviolabilité de la vie privée sur la base d'une ordonnance émanant d'un tribunal, et ce pour une période donnée, lorsque cette procédure est nécessaire pour l'institution, dans le cadre d'une procédure pénale ou pour des raisons liées à la sûreté de l'État. La portée de la protection de la confidentialité des communications, telle que définie par l'article 37 de la constitution, découle de la nécessité de protéger la confidentialité des relations que noue une personne dans le cadre de ses communications, et non du type, du statut ou de l'appartenance du support ou du moyen de communication. Cette protection est garantie à toute personne, la constitution n'établissant pas à cet égard de distinction entre sphère privée et sphère officielle.

Le commissaire à l'information a statué que le ministère avait acquis et utilisé les données dans le but inadmissible d'examiner les données de trafic en vue d'établir quels étaient les employés qui avaient appelé le journal. Par ailleurs, le commissaire a conclu à une absence manifeste de proportionnalité, puisque l'acquisition des données susmentionnées n'a pas permis de trouver des preuves de fuites.

Office de protection de la concurrence

Le commissaire a décidé qu'il était interdit à l'Office de protection de la concurrence (OPC) de traiter les données personnelles contenues dans les copies de disques durs d'ordinateurs personnels obtenues lors d'une procédure visant à établir si les trois plus grands détaillants slovènes avaient été impliqués dans des actions concertées.

Au cours de l'inspection, le commissaire a déclaré que l'article 29 de la loi sur les distorsions de concurrence ne fournit pas une base juridique suffisante pour accéder à la correspondance électronique et aux données de trafic y afférentes. Compte tenu des dispositions strictes prévues par la constitution (article 37), la loi ne définit pas le traitement des courriers électroniques comme une forme d'enquête, et un accès à ceux-ci constitueraient donc une intrusion dans la confidentialité des communications prévues par la constitution. Le commissaire a ordonné à l'OCP d'empêcher tout accès aux fichiers électroniques ainsi acquis, qui contiennent également des données personnelles acquises de manière illicite et lui a accordé un délai de cinq jours pour transférer sur un autre support les informations susceptibles d'être utilisées dans la suite de l'enquête. Tout accès aux supports obtenus doit avoir lieu en présence du commissaire. Lors d'une révision judiciaire de la décision, le tribunal administratif a rejeté, dans l'attente d'un jugement définitif, une requête de l'OPC visant à obtenir l'autorisation d'examiner les données personnelles contenues sur les copies des disques durs et a ainsi confirmé la décision du commissaire. La Cour suprême a refusé à l'OPC toute protection juridictionnelle en tant qu'organe administratif dans la procédure de litige, les compétences et mandats des organes administratifs dans l'exécution de ses tâches administratives ne pouvant selon elle être considérés comme des droits ou des acquis soumis à la protection d'un tribunal en cas de litige.

Protection des données personnelles sensibles

Le commissaire a eu à traiter des cas graves de protection inappropriée de données personnelles sensibles. Ainsi, lors du transfert de supports de données (demandes d'examens en laboratoire) vers leur lieu de destruction, des cartons contenant lesdits supports sont tombés du camion et les supports se sont éparpillés sur la route. Le responsable du traitement des données – un centre de soins primaires – avait confié le transport et la destruction de fichiers contenant des données personnelles à un sous-traitant, agréé pour la collecte et le transport des déchets. Le centre de soins n'avait toutefois pas contractuellement défini les obligations de chacune des parties concernant le traitement des données, conformément à la LPDP. Il n'avait pas non plus fourni au sous-traitant d'instructions appropriées quant à la protection des données pendant leur transport et leur destruction, et n'avait pas supervisé l'exécution des procédures et mesures de protection des données personnelles par le sous-traitant. Le commissaire a mis à l'amende tant le responsable du traitement des données (centre de soins) que son agent (la société chargée du transport et de la destruction des données) pour avoir protégé les données personnelles de manière inadéquate et n'avoir pas respecté les dispositions légales en matière de sous-traitance du traitement des données personnelles.

Une autre affaire de protection insuffisante de données personnelles sensibles largement relayée par la presse a été mise au jour lors d'une inspection à l'Institut d'oncologie. Celle-ci a révélé que la documentation médicale (des dossiers médicaux contenant des données sur des patients décédés) était conservée dans une centaine de cartons ouverts, stockés dans un couloir sans la moindre protection. Par ailleurs, dans le même couloir facilement accessible se trouvaient deux armoires contenant des informations partielles sur des patients en cours de traitement. Le responsable du traitement des données qui aurait dû, conformément à la législation sur les données sensibles, assurer une protection adéquate de celles-ci s'est vu infliger une amende par le commissaire.

Le maire

Le maire d'une municipalité slovène a reçu une initiative de ses administrés relative à un appel au référendum portant sur la construction d'immeubles résidentiels sur le territoire de l'entité. Parmi les annexes jointes à cette initiative figurait une liste de plus de 400 signataires, avec les données personnelles qu'ils avaient fournies dans ce contexte. Le maire a remis une copie de l'initiative à l'avocat embauché par la société chargée de construire les immeubles en question. Celui-ci a, par la suite, utilisé cette liste dans un but autre que celui pour lequel les données avaient été collectées. En effet, il a informé les signataires de l'initiative qu'une action en dommages-intérêts avait été intentée à leur encontre et leur a demandé de retirer leur signature. Le maire et l'avocat ont été mis à l'amende pour traitement illicite de données personnelles.

Administration fiscale de la République de Slovénie

Le commissaire a aussi supervisé la protection des données personnelles assurée par les employés dans plusieurs registres de l'administration publique, notamment concernant les justifications d'accès au registre central des contribuables. Conformément à la LPDP, le responsable du traitement des données, en l'occurrence l'administration fiscale de la République de Slovénie, est tenu de permettre que soit établi quand des données personnelles ont été saisies dans le système d'archivage, utilisées ou traitées d'une quelconque autre manière. Le commissaire a donc pu examiner tous les accès à la base de données informatique des contribuables concernant 15 personnalités slovènes. L'administration fiscale a communiqué au commissaire une liste des employés qui avaient accédé aux données des 15 personnes susmentionnées sur une période de 8 mois en 2008. Chaque employé a été invité à justifier pourquoi il avait consulté les données, et il s'est avéré que seuls 47 des 200 employés concernés l'avaient fait de manière licite, c'est-à-dire en vue de mener à bien une procédure fiscale. Les autres employés n'avaient aucune raison valable d'accéder aux données. Le motif le plus souvent cité pour avoir consulté l'âge ou l'adresse de ces personnalités était la curiosité. Le commissaire a émis des avertissements à l'encontre des fonctionnaires qui avaient consulté les données sans base légale suffisante, afin de leur rappeler qu'il est interdit d'accéder à des données personnelles sans motif légal.

Contrôle de constitutionnalité

Sur la base de l'article 23a de loi relative à la Cour constitutionnelle autorisant le commissaire à l'information à amorcer une procédure de contrôle de constitutionnalité ou de légalité des textes réglementaires si une question se pose à cet égard dans le cadre de ses activités, deux nouvelles requêtes de contrôle de constitutionnalité portant sur certaines dispositions de la loi relative aux opérations bancaires et de la loi sur l'Agence de sécurité et de renseignement slovène ont été déposées en 2008. La première requête, concernant la disposition de la loi sur les opérations bancaires relative à l'instauration obligatoire d'un système d'information sur la solvabilité des clients ainsi que sur la communication obligatoire par les banques de ce type d'informations, a été retirée en mai 2008, suite à des négociations fructueuses avec le ministère des finances, qui a accepté d'amender la loi en vue d'y répertorier les données à stocker dans le système ainsi que la durée de conservation de celles-ci.

Concernant l'inspection de l'Agence de sécurité et de renseignement slovène, le commissaire a introduit une requête de contrôle de constitutionnalité portant sur la loi relative à cette institution, et plus particulièrement une révision des dispositions relatives au contrôle des télécommunications stratégiques, qui impliquent l'émergence de systèmes d'archivage des données personnelles. Le commissaire a demandé que la Cour constitutionnelle tranche concernant les écarts qui existent entre certaines dispositions de ladite loi et l'article

38 de la constitution (droit fondamental à la protection des données ou la confidentialité de ses informations). Le commissaire a également invité la Cour à déterminer si les dispositions de la loi étaient conformes à l'article 37 de la constitution, qui garantit la confidentialité des communications et définit les conditions et restrictions relatives aux violations de ce droit fondamental. La confidentialité des communications ne peut être suspendue que dans des conditions très strictes, pour l'institution, pour une procédure pénale ou pour des motifs relevant de la sûreté de l'État, dans des cas prescrits par la loi et sur la base d'une ordonnance du tribunal.

La Cour constitutionnelle a rejeté la demande du commissaire à l'information demandant un raisonnement formel, le requérant n'ayant pas démontré que la question du contrôle de constitutionnalité découlait de la procédure en cours. Elle a donc estimé que les conditions de procédure n'étaient pas remplies. La Cour constitutionnelle était d'avis que la loi relative à l'Agence de sécurité était suffisamment précise lorsqu'elle stipulait que l'écoute de communications internationales (la «surveillance stratégique de communications internationales») n'était autorisée que lorsque le numéro de téléphone et la personne n'étaient pas définis. Il convient également de souligner que, lors de l'inspection, le commissaire avait découvert que la surveillance visait un numéro de téléphone spécifique et donc une personne identifiable. Or, la loi ne l'autorise pas pour la surveillance stratégique de communications internationales, mais la question qui était posée en l'espèce était de savoir si la surveillance des communications internationales stratégiques pouvait être autorisée par le directeur de l'Agence, la loi précisant, conformément à la constitution, que seul un tribunal pouvait le faire. Cette question reste sans réponse. Le commissaire était d'avis que l'article permettant au directeur d'ordonner une telle surveillance était anticonstitutionnel.

C. Questions diverses importantes

Outre son rôle d'inspection et de répression, le commissaire a mené à bien diverses autres tâches relatives aux dispositions de la LPDP.

La réalisation de **mesures biométriques** n'étant autorisée qu'après réception de la décision du commissaire à l'information, 16 demandes seulement ont été reçues en 2008 (contre 40 en 2007). Proportionnellement, une baisse a été constatée dans le nombre de décisions émises (17 en 2008 contre 35 en 2007).

Une légère augmentation a été constatée dans le nombre de permis octroyés pour la **connexion de systèmes de classement**. En 2008, le commissaire à l'information a rendu 8 décisions (contre 7 en 2007) en la matière.

Dans le cadre de ses **activités d'inspection** (en décembre 2007, dix inspecteurs de la protection des données étaient au service du commissaire) en 2008, le commissaire à l'information a reçu 635 demandes et plaintes concernant des soupçons d'infraction à la loi sur la protection des données à caractère personnel (256 dans le secteur privé et 379 dans le secteur public). Une augmentation significative et constante (406 cas en 2007 et 231 en 2006) est observée par rapport aux années antérieures (76 % en 2007 et 56 % en 2008). Comme les années précédentes, la plupart des plaintes avaient trait à la divulgation de données personnelles (DP) à des utilisateurs non autorisés, à la collecte illicite ou excessive de DP, à une vidéosurveillance illégale, à une protection insuffisante des DP, à une publication illicite de DP, etc. En conséquence, une augmentation notable a été relevée dans le nombre de procédures ouvertes pour des infractions administratives: 279 cas en 2008 contre 133 en 2007 et 41 en 2006.

En 2008, le nombre de requêtes **d'opinions et de clarifications** écrites a atteint 853 unités. Bien que cela constitue une légère baisse par rapport aux 1 144 cas recensés en 2007, ces chiffres restent supérieurs aux 626 cas de 2006. Ce constat indique que le grand public est bien informé de son droit à la protection de la vie privée, grâce à une loi sur la protection des données à caractère personnel moderne. Le travail transparent du commissaire à l'information et les campagnes d'information intensives qu'il mène auprès de l'opinion publique n'y sont sans doute pas non plus étrangers.

Résultat de ces efforts, le commissaire jouit d'une bonne réputation, de la confiance de l'opinion et d'une grande publicité auprès de celle-ci, ce que montrent les sondages d'opinion réalisés dans le pays, de même que le rapport sur les conclusions de l'enquête Flash

Eurobaromètre relative à la protection des données de janvier 2008. Cette dernière révélait que la Slovénie figurait parmi les premiers pays européens en termes de sensibilisation des citoyens et des responsables du traitement des données à la protection des données et de connaissances de la réglementation légale et institutionnelle en la matière.

En décembre 2008, le commissaire à l'information a reçu le prix slovène Netko du meilleur site commercial et administratif dans la catégorie des institutions publiques.

Outre la publication sur son site internet d'avis non contraignants revêtant la forme d'explications écrites et l'édition de diverses brochures portant sur plusieurs questions liées la protection des données, le commissaire a, en 2008, commencé à rédiger des **orientations** sur des aspects spécifiques de la protection des données. Elles ont pour objectif de fournir des instructions et des informations pratiques courantes à l'intention des responsables du traitement des données, sous la forme d'une foire aux questions. Grâce aux réponses apportées et aux lignes directrices esquissées les responsables devraient être en mesure de se conformer aux dispositions statutaires de la loi sur la protection des données personnelles. L'année dernière, le commissaire a préparé et publié sur son site internet des orientations relatives à la protection des données personnelles dans les systèmes d'information hospitaliers, aux mesures biométriques, à la protection des données personnelles dans le contexte de l'emploi et à la vidéosurveillance.

À l'occasion de la seconde **Journée européenne de protection des données**, le commissaire a organisé une table ronde sur le thème d'une utilisation sûre de l'internet et d'autres technologies modernes. Ce débat était centré sur les jeunes utilisateurs et sur la protection des données personnelles dans ce contexte. Une brochure a été produite en vue d'informer les jeunes, les parents et les enseignants, puis publiée sur le site internet de l'école et largement distribuée dans toutes les écoles de Slovénie. Le commissaire à l'information a profité de cette opportunité pour présenter les prix des bonnes pratiques en matière de protection des données personnelles dans les secteurs public et privé.

Coopération internationale

Le commissaire a accueilli deux grandes réunions internationales en 2008. Ainsi, au printemps, il a organisé le **16e atelier de gestion de cas** consacré aux problèmes des mesures biométriques dans les secteurs public et privé, et à la protection des données sur l'internet. L'événement a eu lieu à Ljubljana. En septembre 2008, il a également organisé la **troisième conférence européenne des commissaires à l'information**, au cours de laquelle l'accent portait sur une mise en œuvre plus efficace, et surtout plus rapide, du droit d'accès aux informations publiques.

Dans le cadre de **l'évaluation de la Suisse dans le cadre de son adhésion à l'espace Schengen**, c'est le commissaire slovène à l'information qui a emmené l'équipe d'experts européens dans le domaine de la protection des données. L'évaluation s'est déroulée avec succès et un rapport final a été produit à l'automne.

Les représentants du commissaire ont activement participé à plusieurs **réunions et événements internationaux**, et notamment à la conférence de printemps des autorités européennes de contrôle de la protection des données, qui s'est tenue à Rome (en avril), à la 30e conférence internationale des commissaires à la protection des données sur le thème de la protection de la vie privée dans un monde sans frontière organisée à Strasbourg (octobre), au forum des autorités de protection des données des pays d'Europe centrale et orientale en Pologne, aux réunions du groupe de travail international sur la protection des données dans les télécommunications, etc.

Le commissaire à l'information a régulièrement été représenté au sein des **instances européennes** suivantes, actives dans le domaine de la protection des données à caractère personnel: groupe de travail «Article 29», organe de contrôle mixte d'Europol, autorité de supervision mixte de Schengen, autorité de supervision mixte des douanes et groupe de contrôle EURODAC dans le cadre de la coordination entre CEPD et les APD. Une coopération régulière avec le **Conseil de l'Europe** a également été instaurée, principalement dans le cadre du comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Espagne

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

Étant donné la tenue d'élections législatives en Espagne l'année dernière (les deux Chambres ont été dissoutes et réélues au terme des élections), le Parlement n'a voté aucun texte législatif relatif au secteur des télécommunications ou à la protection des données en vue de transposer la directive 95/46/CE.

B. Jurisprudence

Tribunal national

Au cours de l'année 2008, le tribunal national a rejeté un total de 166 appels à l'encontre de résolutions de l'Agence, qui ont été pleinement confirmées (72 %). Parmi ces jugements, 76 portaient sur des demandes de radiation du registre des baptêmes. 14 jugements considéraient les appels comme fondés sur certains points (6 %), et 48 sur tous les points (21 %), 22 d'entre eux concernant les registres des baptêmes, transmis après l'arrêt de la Cour suprême du 19 septembre 2008, sur lequel nous reviendrons ci-après. Dans un cas, le tribunal national a jugé un appel irrecevable. Les sentences suivantes méritent que l'on s'y arrête:

- Dans son jugement du 17 décembre 2008, le tribunal a estimé que la simple mention d'une période chômée ne constitue pas une information sanitaire et ne requiert pas le déploiement de mesures de sécurité strictes.
- Le jugement du 10 juillet 2008 précise le concept des sources accessibles au public, estimant que l'internet ne peut être dans son ensemble considéré comme un «média de masse».
- Les jugements des 26 février et 23 juillet, concernant l'appartenance publique ou privée des systèmes d'archivages d'associations professionnelles et de centres de santé publique, respectivement.
- Trois jugements datés du 1er octobre 2008 tranchent les appels liés au traitement des données de personnalités publiques par les médias de masse sociaux.

Cour suprême

Pour sa part, la Cour suprême a confirmé toutes les résolutions émises par l'Agence, à l'exception de celles liées aux registres des baptêmes de l'Église catholique.

Dans son arrêt du 19 septembre 2008, la Cour suprême a révoqué le jugement du tribunal national dans lequel celui-ci réaffirmait l'opinion défendue depuis 2004 par l'AEPD, selon laquelle les registres des baptêmes pouvaient être considérés comme des systèmes d'archivage, des jeux organisés de données personnelles, et que le principe de qualité des données en matière d'exactitude et d'actualisation leur était dès lors applicable.

S'appuyant sur ces critères, l'AEPD avait estimé qu'une plainte de citoyen devait conduire à une annotation en marge du registre, reflétant le droit de la personne concernée à l'effacement de ses données. Par ailleurs, dans son premier jugement, le tribunal national avait établi que les plaintes devaient être adressées par des personnes exerçant leur droit à la liberté de conscience, si elles étaient perturbées par le contenu du registre et souhaitaient marquer leur opposition au fait d'être considérées comme membres de l'Église catholique.

La Cour suprême a néanmoins conclu que le registre des baptêmes ne peut être tenu pour un système d'archivage comme mentionné ci-dessus, puisque «*les registres des baptêmes ne sont qu'une accumulation des données difficilement accessibles, dans lesquelles la recherche et l'identification sont mal aisées, du fait qu'elles ne sont pas classées par ordre alphabétique ni par date de naissance, mais uniquement par date de baptême*».

L'AEPD a introduit une requête devant la Cour constitutionnelle, avec le ministère public, considérant que l'interprétation du terme «système d'archivage» était susceptible de restreindre indûment le champ des règles de protection des données et ne tenait aucun compte de la portée du droit fondamental reconnu par la jurisprudence de la Cour constitutionnelle.

Dans neuf cas, elle a déclaré que les appels introduits à l'encontre des arrêts du tribunal national confirmant les résolutions de l'Agence, en relation avec le droit à la radiation des registres des baptêmes de l'Église catholique, étaient fondés.

Dans huit cas, elle a statué que l'appel introduit à l'encontre des jugements confirmant les résolutions de l'Agence était infondé.

Dans un cas, elle a déclaré irrecevable un appel visant des jugements confirmant les résolutions de l'Agence.

Résolutions de l'autorité espagnole de protection des données

La plus grande visibilité dont jouit l'AEPD parmi les citoyens a conduit à une forte hausse du nombre d'infractions signalées. En ce sens, les inspections préalables au lancement d'une procédure répressive ont augmenté de 45,4 %, et les résolutions procédurales amorcées ont pratiquement doublé (avec un accroissement de 94,1 %). Les secteurs dans lesquels la plupart des inspections ont été effectuées restent ceux des télécommunications, des institutions financières et de la vidéosurveillance. Ensemble, ces trois secteurs représentent 50,9 % de tous les contrôles.

Dans le cas des résolutions concernant des procédures répressives à l'encontre de sociétés privées, le haut du pavé est également occupé par les secteurs des télécommunications et des institutions financières, quoique leur nombre ait enregistré une hausse nettement supérieure à celle de l'année précédente (81,3 % contre 45 % et 104 % contre 58,8 %, respectivement). Toutefois, le secteur où l'augmentation a été la plus forte en termes de procédures répressives est celui de la vidéosurveillance (633,3 %), même si celles-ci ont conclu à une infraction dans 61,3 % des cas. Les résolutions faisant état d'une infraction à la LOPD par les administrations publiques ont cru de 19,7 %. De la même manière, les résolutions mettant un terme à la procédure se sont multipliées (113 %), de même que les rapports jugés irrecevables (138,3 %). Concernant les pénalités infligées, on a assisté à un accroissement des amendes punissant des infractions graves (551 contre 350). Le nombre de cas dans lesquels une baisse notable de la responsabilité des contrevenants a été constatée s'est élevé à 229, soit 42 % de l'ensemble des résolutions imposant une amende (contre 32 % en 2007) Parmi les principales inquiétudes que nourrissent les citoyens figure la réception d'appels non sollicités. Comme nous l'expliquerons plus tard, en conséquence de cela, l'AEPD a réalisé deux contrôles sectoriels *ex officio* portant sur les appels téléphoniques et SMS à destination de téléphones portables. Ce faisant, elle a constaté des lacunes dans les mécanismes permettant aux citoyens de s'opposer à la réception de tels appels et a mis en garde contre les risques associés à la souscription de services tarifés complémentaires (SMS Premium).

Deux résolutions sont particulièrement dignes d'intérêt.

- Dans la résolution n° 00281/2007, l'AEPD a mis deux sociétés à l'amende pour avoir obtenu des informations personnelles relatives à un mineur au moyen d'un formulaire publié sur un site internet sans le consentement de ses parents et les avoir utilisées pour envoyer de la publicité concernant une carte de crédit, sans le consentement du tuteur légal de l'enfant.

  La société n'a pas fait preuve de la diligence requise pour empêcher le traitement de ces données compte tenu de la date de naissance de l'enfant. L'AEPD a déclaré deux infractions à la loi relative à la protection des données à l'encontre de l'entité. La première, qui portait sur la collecte des données d'un mineur sans l'accord de ses parents ou de son tuteur, constituait une infraction grave; la seconde, relative à la communication des données personnelles de l'enfant à une seconde entité en vue de mener une campagne publicitaire, est considérée comme très grave. Par ailleurs, l'Agence a estimé qu'en traitant les données dans le cadre de la campagne publicitaire sans l'autorisation du tuteur légal de l'enfant, la deuxième société s'était rendue coupable d'une infraction grave, en tant que responsable du traitement des données.

  Pour l'AEPD, et conformément à la réglementation applicable, il est nécessaire, pour les mineurs de moins de 14 ans, qui ne possèdent pas la maturité suffisante pour que l'on puisse garantir qu'ils donnent leur accord en connaissance de cause, d'obtenir le consentement des parents ou des tuteurs légaux. Par ailleurs, les informations appropriées pour ce faire doivent être fournies, avec une vérification de l'âge de l'enfant et, en cas de doute, l'entreprise doit s'abstenir de traiter les données.

- Dans sa résolution n° AP/00061/2007, l'AEPD a conclu à une infraction très grave à la LOPD, une administration publique n'ayant pas respecté le secret professionnel,

dans le cadre de la publication au Journal officiel d'une résolution contenant d'informations (noms, prénoms et numéros de carte d'identité compris) relatives aux bénéficiaires d'une aide destinée à soutenir des toxicomanes à décrocher. L'AEPD estime qu'il n'était pas nécessaire, pour respecter l'obligation légale «de transparence, d'objectivité et de concurrence», d'identifier les bénéficiaires de cette aide. En fait, il existait des solutions, telles que l'anonymisation ou la dissociation, pour que les personnes concernées ne soient pas identifiables. Pour l'AEPD, quoi que la publication de données dans les journaux officiels soit autorisée par la loi, il est nécessaire de réviser les critères présidant à l'incorporation des données dans les publications des organismes et institutions publics.

C. Questions diverses importantes

Au cours de l'année 2008, l'AEPD a concentré ses efforts sur les points suivants.

Faciliter le respect de la loi
L'un des meilleurs moyens de protéger les citoyens consiste à s'assurer que ceux qui exploitent leurs données savent comment les traiter, c'est-à-dire à faciliter le respect de la loi en redoublant d'efforts pour la faire mieux connaître du grand public et pour répondre aux doutes qui pourraient se faire jour. Traditionnellement, ces tâches étaient assumées par le département chargé de traiter les demandes des citoyens et par le service juridique.

Toutefois, 2008 s'est avéré être une année-charnière à cet égard, compte tenu de la politique volontariste menée dans le but d'accroître l'offre en informations, au moyen d'instruments tels que la publication de guides de vulgarisation sur les principes de base de la protection des données, rédigés dans un langage clair, simple et compréhensible. Telle était l'idée sous-jacente du «*Guide de la protection des données à destination des responsables de leur traitement*» et du «*Guide de la sécurité des données*», publiés en réponse à la multiplication des demandes d'informations à ce sujet. Par ailleurs, la mise en œuvre de la LOPD ayant renforcé la nécessité, pour l'Agence, de savoir quels étaient les critères applicables à celle-ci, l'AEPD a mis sur pied des «*ateliers ouverts*», qui ont remporté un vif succès en termes de présence (2 000 personnes) et de participation.

Ces incitants sont venus compléter les politiques de prévention traditionnelles basées sur les inspections sectorielles *ex officio*, telles que celles effectuées en 2008 en relation avec les «appels téléphoniques commerciaux et des messages textuels dans la téléphonie mobile». Ces inspections vont de paire avec la rédaction de rapports ou de déclarations relatifs aux nouveaux défis à relever dans le domaine de la protection des données, et plus particulièrement des services internet.

Ces guides sont disponibles aux adresses ci-dessous:
«*Guide de la protection des données à destination des responsables de leur traitement*»
https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_fiche-ros.pdf
«*Guide de la sécurité des données*»
https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

L'information comme élément-clé de la sensibilisation des citoyens
L'AEPD a fait une priorité de l'information des citoyens quant à leurs droits et à l'exercice de ceux-ci, et accorde une importance capitale à la mise en place d'instruments de prévention et de mesure de coercition en vue de garantir l'efficacité de ceux-ci.

Elle encourage ainsi les médias à jouer un rôle actif dans la diffusion de l'impact qu'a la protection des données personnelles sur la vie quotidienne des citoyens, surtout dans le contexte de la société de l'information, et veille à ce qu'ils assument ce rôle. Les efforts consentis à cet égard ont considérablement amélioré la qualité de l'information. La présence accrue de l'Agence et de la protection des données personnelles dans les médias est devenue une réalité: en 2008, le nombre d'entretiens et de demandes d'informations a doublé, passant à plus de 800 unités.

Du point de vue quantitatif, le service juridique a, en 2008, répondu à quelque 690 requêtes au total (soit 25 % de plus), dont 279 (40 %) lui ont été adressées

par des administrations publiques et 411 (60 %) par le secteur privé. 250 000 systèmes d'archivage ont été enregistrés auprès du registre général de la protection des données, qui a ainsi atteint un total de 1 267 579 unités (85 083 systèmes publics et 1 182 496 systèmes privés), soit une augmentation de 31 % par rapport à l'année précédente.

Il y a aussi eu une croissance significative dans le nombre de systèmes d'archivage publics enregistrés, de plus de 23 500 unités (hausse de 300 %). À ce stade, il convient de souligner que le Conseil général des pouvoirs judiciaires procède à l'enregistrement de tous les systèmes d'archivage liés aux organes judiciaires (11 965). Voilà une initiative qu'il convient de saluer, car elle jette des bases solides en vue d'encourager l'adaptation de la LOPD à l'administration judiciaire.

Attention spéciale aux mineurs d'âge

La protection des données personnelles des mineurs fait partie des matières auxquelles l'AEPD accorde une attention prioritaire. Divers efforts ont été consentis en vue de sensibiliser l'opinion publique à ces problèmes, dont la publication du «Guide relatif aux droits des garçons et des filles et aux devoirs des mères et des pères», un document contenant des recommandations de base en matière de protection des données, à destination du cercle familial et de l'école, présenté le 17 mai à l'occasion de la journée de l'internet.

L'Agence a également déclaré, à l'occasion de sa participation à la 30e conférence internationale des autorités de protection des données, que la formation à une utilisation élémentaire des outils informatiques, mettant en lumière leurs risques et leurs atouts, ne suffisait pas. Dans tous les cas, un défi urgent doit être relevé: le développement d'outils efficaces permettant de savoir si les utilisateurs des services internet sont des mineurs d'âge, ce pour quoi il convient d'obtenir l'aide de leurs parents.

Dans ce sens, l'AEPD a tranché un premier cas de traitement illégal des données d'un mineur sans vérification préalable de son âge. Une amende a été infligée à l'organisme concerné pour ce manque de diligence.

Le «Guide relatif aux droits des garçons et des filles et aux devoirs des mères et des pères» est disponible à l'adresse:
https://www.agpd.es/portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf

Internet vs. respect de la vie privée

Le web 2.0 a multiplié l'offre de nouveaux services mis à la disposition des internautes à grande échelle, et leur permettant d'interagir entre eux.

Il convient, à cet égard, de mentionner les réseaux sociaux, puissants canaux de communication et d'interaction rassemblant un grand nombre de jeunes utilisateurs, dont des mineurs d'âge, mais susceptibles de créer des risques pour la protection des données personnelles. Consciente de cela, l'AEPD s'est lancée dans une analyse des implications des réseaux sociaux en 2008 et, au terme de l'évaluation initiale, les points suivants sont devenus apparents:

- les informations relatives à la politique en matière de respect de la vie privée et aux conditions d'utilisation ne sont pas toujours très claires ni accessibles;
- il n'existe pas d'applications permettant de vérifier l'âge des mineurs qui tentent de se connecter au service;
- il est possible à des tiers, autres que les personnes considérées comme des «amis» ou des «contacts directs» par les utilisateurs, d'accéder à leurs profils.

Une mission urgente: vers des normes internationales en matière de respect de la vie privée

La diversité des systèmes de protection des données et de lutte contre le piratage, ou l'absence de tels systèmes, a conduit à divers problèmes qui pourraient être résolus par l'adoption de normes internationales (minimales) en vue de fournir des garanties quant aux flux de données opérés dans un monde globalisé.

L'AEPD a considéré que le temps était venu de mettre en œuvre des initiatives permettant d'enregistrer des progrès tangibles dans l'élaboration desdites normes. À l'occasion de la 30e Conférence internationale sur la protection des données et de la vie privée, une proposition conjointe dans ce sens a été présentée à l'autorité suisse, soulignant le besoin urgent de protéger la vie privée dans un monde sans frontières. Une proposition

a été adressée à l'autorité organisatrice de la Conférence internationale de 2009 concernant la création et la coordination d'un groupe de travail qui aurait pour mission de préparer et de soumettre une «*proposition conjointe de normes internationales pour la protection de la vie privée et des données personnelles*» lors de la séance à huis clos de la 31e conférence.

Cette proposition a recueilli l'approbation unanime de la Conférence, confiant ainsi à l'AEPD la tâche de former le groupe de travail et de mener à bien le projet consistant à développer une proposition de normes internationales en matière de protection de la vie privée dans le contexte du traitement des données personnelles. Le but ultime de ces travaux serait que le texte présenté à la Conférence de Madrid en novembre puisse être adopté par un vaste consensus et devenir un instrument international de protection de la vie privée et des données personnelles.

Coopération avec les agences de protection de données des communautés autonomes

En matière d'inspection, la coopération entre les agences de protection des données a progressé et s'améliore en termes d'analyse des mesures permettant de garantir l'efficacité des résolutions adoptées et de coordination des activités d'inspection lorsque celles-ci concernent les compétences de plusieurs agences. Par ailleurs, les agences ont échangé leurs critères en matière de vidéosurveillance, de publication des jugements sur le web et d'insertion d'informations personnelles dans les journaux officiels. Les agences partagent l'objectif prioritaire qui consiste à encourager l'éducation des mineurs d'âge et ont soutenu la candidature de l'AEPD à l'organisation de la 31e Conférence internationale de la protection des données et de la vie privée. Ce soutien est allé de paire avec un engagement à collaborer à la préparation d'un document contenant des normes communes pour la protection des données dans un monde globalisé.

Mise en œuvre: renforcement des mesures préventives

Plan sectoriel ex officio concernant la publicité par téléphone

L'AEPD a réalisé un plan sectoriel *ex officio* concernant la publicité par téléphone, dans le cadre duquel elle a analysé les pratiques des principaux opérateurs espagnols de téléphonie fixe et mobile ainsi que des entités proposant des services tarifés complémentaires (Premium) basé sur la réception de SMS ou des services d'abonnés.

D'une manière générale, l'AEPD a détecté des lacunes dans les systèmes de garantie permettant aux citoyens de ne pas être la cible d'appels publicitaires. Parmi les principales conclusions de l'analyse réalisée, l'AEPD a souligné les lacunes présentes dans les mécanismes mis à la disposition des citoyens afin que ceux-ci puissent, dans certains cas, empêcher et refuser la réception de communications commerciales par SMS et par téléphone sur leurs lignes fixes et mobiles, et elle a mis en garde contre les risques associés à la souscription de services tarifés complémentaires. Selon le rapport, les principales lacunes identifiées au cours de l'inspection sont les suivantes:

- Selon les données du plan sectoriel, 53 % des sociétés passées au crible consultent les annuaires téléphoniques pour sélectionner les destinataires de leurs campagnes via des appels passés sur des lignes fixes. À cet égard, l'attention de l'AEPD a été attirée sur le fait que seul 1 % des abonnés répertoriés dans les annuaires téléphoniques avaient demandé à ne pas recevoir d'appels commerciaux.
- Certaines pratiques déclarées par les opérateurs telles que l'utilisation de données relatives à des «personnes recommandées» ont déjà été sanctionnées par l'AEPD.
- L'AEPD a découvert que les appels aléatoires, sans identification de l'abonné correspondant au numéro, constituaient une méthode habituelle pour la conduite de campagnes s'appuyant sur la téléphonie mobile. Elle considère qu'il est urgent de légiférer en vue d'interdire cette pratique.
- Les émetteurs des messages sont tenus de fournir des informations claires, ainsi que des méthodes simples permettant de faire usage du droit à refuser la réception de tels messages.
- Les opérateurs doivent mettre en place des mécanismes de contrôle en vue de limiter l'afflux massif de SMS commerciaux de pays tiers n'observant pas la réglementation espagnole.

Concernant les services «premium», le plan sectoriel *ex officio* souligne que les clauses d'information contenues

dans la promotion de ces services contiennent très peu d'éléments, d'autant que des termes incomplets ou abrégés sont utilisés dans les messages envoyés sur les téléphones portables et que leur signal d'identification est difficile à lire. Les utilisateurs ne sont donc pas informés du coût des messages, de la procédure de désabonnement ni des données qui seront traitées, etc. Concernant ces services, l'AEPD met tout particulièrement en garde contre leur souscription par des mineurs, l'une des catégories de la population les plus vulnérables, ceux-ci étant plus faciles à tromper que les adultes.

Après avoir mené à bien le plan sectoriel, et suite aux lacunes identifiées, l'AEPD a préparé plusieurs **recommandations à l'intention des citoyens, de manière à les aider à faire valoir leurs droits, et à l'intention du secteur**, afin qu'il puisse améliorer ses pratiques.

L'intégralité du plan *ex officio* et les recommandations formulées sont disponibles à l'adresse:
https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/plan_sectorial_publicidad_telefonica_2008.pdf
https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_sms_llamadas_11_2008.pdf

Vidéosurveillance
En 2008, l'AEPD a ouvert une enquête *ex officio* concernant plusieurs sites internet qui diffusent des images en temps réel enregistrées par des caméras de sécurité installées dans des lieux publics afin de vérifier si le mot de passe requis pour accéder à ces images est correctement paramétré, comme l'exigent les réglementations en matière de protection des données.

Codes de conduite
L'autoréglementation au moyen de codes standard notifiés et enregistrés auprès du département de l'enregistrement constitue un instrument complémentaire en vue de faciliter le respect de la LOPD et de renforcer la sécurité juridique. Tout au long de l'année 2008, des initiatives d'autoréglementation ont été mises en œuvre dans le secteur de l'intermédiation en assurances privées, des assurances-groupes des employeurs actives dans le domaine des maladies professionnelles et des accidents du travail, de la pharmacovigilance et de la surveillance des essais cliniques, des firmes de sécurité et des cabinets d'avocats.

Principaux développements dans les pays tiers
activités de l'Espagne dans le cadre du réseau ibéro-américain de protection des données
La nécessité de relever de nouveaux défis internationaux a exigé un changement qualitatif dans l'activité du réseau ibéro-américain de protection des données, dont les grandes lignes sont les suivantes:
- renforcer la représentation institutionnelle des pays participants et optimiser leur efficacité;
- promouvoir l'organisation exécutive des représentants issus de pays latino-américains;
- ouvrir les réunions du réseau à des pays tiers n'appartenant pas à l'environnement ibéro-américain;
- favoriser l'échange de vues entre institutions politiques et compagnies privées;
- amorcer un dialogue ouvert entre les pays d'Amérique latine et la Commission européenne quant aux efforts visant à parvenir à une déclaration de pays adéquats garantissant la protection des données personnelles;
- intégrer le réseau ibéro-américain dans le processus de formulation de normes internationales en matière de protection des données.

La VI^{e} réunion ibéro-américaine relative à la protection des données, qui s'est tenue à *Carthagène des Indes* (Colombie) du 27 au 30 mai 2008, a jeté les bases requises pour réaliser ces objectifs. Les intervenants et institutions participantes représentaient tant des pays d'Amérique latine que les États-Unis, ainsi des multinationales étrangères. Le règlement du réseau a été actualisé. Désormais, l'AEPD se chargera du secrétariat du réseau et en assurera la présidence pour une période de deux ans, avec quatre membres remplissant des rôles spécifiques, assumés par l'Argentine, le Chili, le Mexique et le Portugal. À compter de mars 2009, le réseau ibéro-américain participera, en qualité d'observateur aux réunions biannuelles du Comité consultatif de la Convention 108 du Conseil de l'Europe.

L'Agence a continué à développer sa coopération bilatérale, laquelle a culminé dans la signature d'une lettre d'intention de coopération mutuelle entre l'Agence internationale pour le développement de la société de

l'information en Bolivie (ADSIB) et l'AEPD et du protocole d'accord entre la société pour la promotion de la production du Chili (CORFO) et l'AEPD.

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 l'adoption de la loi (1998:204) sur les données à caractère personnel (PDA, *Personal Data Act*), entrée en vigueur le 24 octobre 1998. La PDA est complétée par *l'ordonnance 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 régissent le traitement des données dans le cadre de certaines activités, soit en lieu et place de la PDA, soit en complément de celle-ci. La directive a également été prise en compte lors de l'élaboration de ces lois et ordonnances spécifiques.

La directive 2002/58/CE a été transposée en droit national par l'adoption de la loi (2003:389) relative aux communications électroniques (ECA, *Electronic Communications Act*), entrée en vigueur le 25 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 2004 de créer une commission sur 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, comme le mentionnait le rapport annuel de l'année dernière. Les membres de la commission ont aussi critiqué à plusieurs égards l'adoption d'une approche systématique et méthodique et ont répondu 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. La commission a présenté la deuxième et dernière partie de son rapport en janvier 2008. Elle y livre une analyse de la façon dont la protection de la vie privée doit être réglementée par la constitution, et y identifie d'autres mesures à prendre. L'un de ces propositions consiste à renforcer la protection de la vie privée dans la constitution. À cet égard, elle recommande une protection contre la surveillance exercée par les autorités publiques ainsi que contre le profilage de la situation des individus. À titre d'exemples d'infractions nécessitant un examen plus minutieux que ce n'est le cas actuellement, elle mentionne, entre autres, la surveillance secrète ainsi que la conservation des données de trafic.

Le rapport de l'année dernière mentionnait que *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* n'avait pas encore été transposée en droit national. C'est toujours le cas. Le gouvernement soumettra probablement un projet de loi à cet effet au Riksdag au mois de juin de cette année.

En juillet 2008, une nouvelle loi relative aux dossiers médicaux et aux soins de santé, la loi sur les données des patients, est entrée en vigueur. Celle-ci peut être considérée comme une réglementation unifiée des données personnelles dans les services de santé et de soins médicaux.

En juin 2008, le Riksdag a approuvé la proposition du gouvernement portant sur une nouvelle *loi de surveillance des signaux* pour les services de renseignement de la défense. Cette loi s'applique à toute surveillance des signaux exercée à des fins d'information de la défense. Elle prévoit diverses règles conçues pour protéger la vie privée des citoyens. Toutefois, le Riksdag exige des

mécanismes de contrôle supplémentaire, en vue, notamment, d'accroître la protection des particuliers. Le Conseil de l'inspection des données a été spécialement mandaté pour suivre les activités de l'Établissement radio de la défense nationale et fera rapport au gouvernement d'ici décembre 2010. La nouvelle législation est entrée en vigueur le 1er janvier 2009.

La troisième *directive européenne sur le blanchiment d'argent* a été transposée en droit national en 2008, et la nouvelle législation est entrée en vigueur le 15 mars 2009.

En décembre 2008, le gouvernement a soumis une proposition de loi visant à transposer la *directive européenne relative au respect des droits de propriété intellectuelle* (2004/48/CE) en droit national. Le Riksdag l'a approuvée, et cette loi entrera en vigueur le 1er avril 2009. L'une de ses caractéristiques principales réside dans le fait que les organisations chargées de protéger la propriété intellectuelle, si elles soupçonnent qu'une personne a été impliquée dans des partages de fichiers en réseau illégaux, peuvent s'adresser à un tribunal et demander que les fournisseurs d'accès internet divulguent des informations sur le propriétaire de l'adresse IP en question.

En décembre 2006, une commission d'enquête a été mise sur pied en vue d'abolir le monopole détenu par Apoteket AB (Coopérative nationale des pharmacies suédoises) dans la vente de produits pharmaceutiques et de permettre à d'autres opérateurs de vendre lesdits produits. Cette mission incluait aussi d'autres aspects, dont l'enregistrement des prescriptions. Le Conseil de l'inspection des données a été consulté et a rendu un avis, notamment sur les questions ayant trait aux bases de données. Le gouvernement a récemment déposé un projet au Riksdag en vue de la faire adopter une *loi sur les données des pharmacies*. Cette nouvelle loi devrait entrer en vigueur en juillet 2009.

En septembre 2008, le Conseil de l'inspection des données a rendu un avis sur les propositions d'amendements à la *loi sur les informations en matière de crédits*, lesquelles impliquent que, dorénavant, les exigences qui s'appliqueront aux informations de crédit sur l'internet seront identiques à celles des autres activités correspondantes. Ces propositions faisaient suite à un amendement à la *loi fondamentale sur l'expression* (une loi constitutionnelle) de 2003, qui permettait de divulguer des informations de crédit à tout un chacun sur des sites internet, sans avoir pour cela à respecter les règles strictes de la *loi sur les informations en matière de crédits*. Cette situation a donné lieu à des violations de la vie privée et à de nombreuses plaintes.

En février 2008, le gouvernement a mis sur pied une commission d'enquête chargée de passer en revue la législation en matière de vidéosurveillance. Cette mission incluait la réalisation d'une étude et l'analyse de l'application faite de la législation actuelle. Cette enquête examinera, entre autres, s'il y a lieu de prendre des mesures complémentaires en vue de renforcer la protection de la vie privée des citoyens eu égard à la vidéosurveillance.

B. Jurisprudence

Dans deux rapports annuels antérieurs, le Conseil de l'inspection des données a présenté des affaires portant sur les données biométriques en milieu scolaire. Les empreintes digitales des élèves étaient prélevées et traitées automatiquement en vue de vérifier l'accès à la cantine de l'école. En décembre 2008, la Cour administrative suprême a décidé que les écoles pouvaient utiliser les empreintes digitales des élèves pour vérifier s'ils avaient ou non payé leurs repas. Toutefois, les élèves doivent donner leur consentement, et il doit exister une solution de rechange pour ceux qui ne souhaitent pas que l'on utilise leurs empreintes.

Dans une décision de 2007, le Conseil de l'inspection des données statuait que l'Union suédoise des ouvriers de la construction devait cesser de traiter les données relatives aux salaires des ouvriers qui n'étaient pas membres de ce syndicat. Un appel a été introduit à l'encontre de cette décision devant le tribunal administratif du comté qui, en décembre 2008, l'a rejeté et a confirmé la décision du Conseil. L'Union des ouvriers du bâtiment s'est alors pourvue devant la Cour administrative d'appel, où l'affaire est toujours en instance.

Au cours de la période 2006-2008, le Conseil de l'inspection des données a effectué des contrôles concernant

les nouveaux systèmes de billetterie des compagnies de transport utilisant des cartes à puce qui laissent des traces électroniques (systèmes basés sur les techniques RFID). Lorsque le passager utilise son billet électronique, les données suivantes sont enregistrées: numéro de la carte, date, heure et arrêt/station. Si le détenteur de la carte l'a fait enregistrer auprès de la compagnie de transport, le numéro de la carte est associé au numéro d'identification personnelle du passager, à son nom et à son adresse. De ce fait, les traces électroniques de la carte peuvent être mises en relation avec une certaine personne. Le Conseil de l'inspection des données a décidé que lesdites traces ne pourraient être conservées que pendant 60 jours, après quoi elles ne devraient plus permettre une identification du passager. L'une des compagnies concernées a fait appel de la décision du Conseil devant le tribunal administratif du comté qui, en janvier 2009, a rejeté la décision du Conseil et a renvoyé l'affaire.

En 2007, le Conseil de l'inspection des données s'est penché sur la manière dont les sociétés et coopératives de logement traitent les données personnelles dans les systèmes de clés électroniques. La clé électronique est associée à un certain appartement et laisse souvent des données dans un journal des passages concernant l'heure et l'endroit où le résident a utilisé la clé. L'inspection a révélé que ces données n'étaient pas traitées correctement. Le Conseil a dès lors émis des lignes directrices quant à l'utilisation des clés électroniques dans les sociétés et coopératives de logement. Le Conseil suit une approche très restrictive en matière d'utilisation des données à des fins autres que l'ouverture des portes et la réservation de la buanderie. En juillet 2008, le Conseil s'est prononcé dans le cas d'une société de logement où, entre autres choses, les données de la clé électronique étaient utilisées pour voir qui avait utilisé la buanderie. Le Conseil a ordonné à la société en question de cesser d'utiliser ses fichiers journaux dans ce but. Un appel a été introduit à l'encontre de cette décision devant le tribunal administratif du comté, qui a confirmé la décision du Conseil. En 2009, la société s'est pourvue devant la Cour administrative d'appel.

En 2008, le Conseil de l'inspection des données a envoyé un questionnaire web aux écoles, dans le but, notamment, de savoir si, et dans quelle mesure, celles-ci avaient recours à la vidéosurveillance dans leurs locaux. Il en est ressorti que l'usage de la vidéosurveillance avait augmenté de 150 % en comparaison avec 2005, époque à laquelle une étude analogue avait été réalisée. Le Conseil de l'inspection des données a inspecté sept écoles et découvert que la vidéosurveillance des élèves en journée était, à de nombreux égards, contraire à la loi sur les données personnelles. Les inspections ont également révélé qu'il y avait des lacunes considérables dans la connaissance de la législation sur la protection des données, raison pour laquelle le Conseil a réalisé une liste de contrôle en vue d'aider les écoles à déterminer quand la vidéosurveillance est acceptable. Des appels ont été introduits à l'encontre des décisions du Conseil du 1er octobre 2008 devant le tribunal administratif du comté, où ils sont toujours en instance.

C. Questions diverses importantes

Documents imprimés

Tous les documents imprimés du Conseil de l'inspection des données peuvent être téléchargés gratuitement sur son site internet. *Magazin Dlrekt* est un périodique proposant des reportages, des actualités et des commentaires en relation avec les centres d'intérêt du Conseil de l'inspection des données. Quatre numéros ont été publiés en 2008.

Comme l'indiquait le rapport de l'année dernière, 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. Le Conseil a ainsi rédigé un manuel d'orientation à l'intention des municipalités et, en 2008, deux jeux d'orientations; l'un pour les autorités gouvernementales, *Services publics en ligne et loi relative aux données à caractère personnel*, et l'autre pour toutes les autorités publiques, *Sécurité informatique et services en ligne des autorités publiques*.

Nous avons également produit un rapport, *Respect de la vie privée année 2008*, qui contient un aperçu complet des nouvelles lois, décisions et techniques publiées au cours de l'année en relation avec la protection de la vie privée.

Un second rapport concernant l'attitude des jeunes, surtout vis-à-vis de l'internet, a été publié en 2008, et le

rapport *Jeunes et respect de la vie privée* a été présenté lors de la 30e Conférence internationale sur la protection des données qui s'est tenue à Strasbourg.

Accords sectoriels
Au cours de l'année 2008, à l'initiative du Conseil de l'inspection des données, le secteur de l'immobilier s'est attelé à la rédaction d'un accord sectoriel (code de conduite) visant à réglementer l'utilisation de la vidéo-surveillance dans les immeubles à appartements. Cette initiative a été prise suite à la multiplication des plaintes concernant ces systèmes. L'accord sectoriel devrait être terminé en juin 2009.

Atelier nordique de traitement des cas
En mai 2008, le Conseil de l'inspection des données a accueilli l'annuel *atelier nordique de traitement des cas*, rassemblant des participants venus du Danemark, des Îles Féroé, de Finlande, d'Islande, de Norvège et de Suède.

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, 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, 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

Un arrêt rendu en 2008 par la Cour européenne des droits de l'homme dans l'affaire S. et Marper contre Royaume-Uni déclarait que la conservation «générale et indifférenciée» d'échantillons cellulaires et de profils ADN de personnes soupçonnées d'avoir commis des infractions mais non condamnées, était disproportionnée et ne traduisait pas un juste équilibre entre les droits des individus et les intérêts de l'État.

Suite à cet arrêt, le gouvernement britannique s'est engagé à publier un livre blanc sur la collecte et l'utilisation d'informations médico-légales en 2009.

L'arrêt Marper est d'une importance capitale pour le bureau, et ses implications iront bien au-delà de la seule conservation des profils ADN et empreintes digitales. En effet, il constitue un soutien de poids à l'approche que nous suivons concernant plusieurs aspects de la confidentialité des informations à caractère personnel.

Le bureau possède désormais un statut d'observateur à toutes les réunions du *National DNA Database Strategy Board*.

C. Questions diverses importantes

Nous avons commémoré la Journée européenne de la protection des données de janvier dernier en lançant notre nouveau code de bonnes pratiques en matière de caméras de surveillance au Parlement.

Nous avons pris des mesures de coercition à l'encontre de plusieurs organisations, dont Carphone Warehouse (CPW) et Marks & Spencer (M&S). L'enquête sur CPW faisait suite à des plaintes liées à la manière dont les informations à caractère personnel y étaient conservées et traitées, et celle sur M&S a été ouverte après le vol d'un ordinateur portable contenant les données, non chiffrées, de 26 000 collaborateurs.

Nous avons poursuivi 17 organisations, dont un bureau de recouvrement de créances de Manchester, pour avoir littéralement bombardé des particuliers et entreprises de télécopies non sollicitées, ainsi qu'un notaire et un comptable pour non-notification en tant que responsables du traitement des données.

Le 25 juin, quatre rapports ont été publiés sur la manipulation des informations à caractère personnel. Le bureau a publié sa réponse à ceux-ci en novembre.

Revue du traitement des données
Une revue des procédures de traitement des données au sein des instances gouvernementales a été initiée par le Premier ministre en réponse à la perte des données personnelles de plus de 25 millions de citoyens par le HMRC (*Her Majesty's Revenue and Customs*) en 2007. Cette revue a été menée par sir Gus O'Donnell, des Services du gouvernement. Dans ses conclusions, il recommandait notamment à tous les départements du gouvernement central d'avoir recours à des évaluations d'impact sur la confidentialité.

Revue de la sécurité des informations au HMRC
Le chancelier de l'échiquier a confié à Kieran Poynter, directeur de PricewaterhouseCoopers, la réalisation d'une enquête portant sur la perte de données à caractère personnel au HMRC et d'une analyse détaillée des processus et systèmes liés au traitement des données au HMRC.

Rapport d'enquête indépendant de l'IPCC (Independent Police Complaints Commission) sur la perte des données relative aux allocations familiales

L'IPCC, en vertu des compétences qui lui sont conférées par la loi de 2002 sur les services de police, a mené sa propre enquête sur la série d'événements qui ont conduit à la perte de données au HMRC, afin de vérifier si des membres du personnel du HMRC avaient eu un comportement criminel ou avaient commis des infractions disciplinaires.

Rapport sur la perte de données à caractère personnel au ministère de la défense

Le 9 janvier 2008, un ordinateur portable de la marine royale contenant des données non chiffrées sur plus de 600 000 personnes a été volé. Le secrétaire d'État à la défense a chargé sir Edmund Burton de mener l'enquête afin d'établir les circonstances et événements exacts qui ont conduit à la perte de ces données personnelles par le ministère de la défense, d'examiner l'adéquation des mesures prises pour éviter qu'un tel incident se reproduise et, plus généralement, des politiques, pratiques et processus de gestion du ministère de la défense en matière de protection des données à caractère personnel.

Le rapport sur le partage des données, réalisé par Richard Thomas et Mark Walport, à la demande du Premier ministre, a été publié le 11 juillet. Celui-ci émet une série de recommandations visant à transformer la culture personnelle et organisationnelle des personnes chargées de collecter, de gérer et de partager l'information. Nous avons répondu à la consultation menée dans le cadre de cette revue.

Nous avons lancé notre stratégie de protection des données lors de la conférence des préposés à la sécurité des données, qui s'est tenue à Manchester en mars, et diffusé notre rapport sur l'intégration des principes de protection des données dès la phase de conception lors de notre conférence de novembre à Manchester. Ce dernier invite les organisations à améliorer, par des gestes simples, leurs mesures organisationnelles et technologiques en vue mieux protéger les informations personnelles. Il a pour but d'aider les organisations à adopter de nouvelles techniques d'intégration des principes de protection des données dès la phase de conception. En outre, il souligne la nécessité de s'assurer que les organisations apportent le soin requis à la protection de la vie privée, et ce dès la phase de conception de leurs nouveaux systèmes d'information.

En 2007, le commissaire a répondu à 47 consultations (nombre identique à celui de 2007).

En 2008, le commissaire a témoigné devant les commissions parlementaires suivantes:

- Commission de l'intérieur de la Chambre des Communes: rapport «A Surveillance Society?».
- Commission de l'intérieur de la Chambre des Communes: enquête sur la société de la surveillance.
- Commission parlementaire spéciale sur la Constitution de la Chambre des Lords: 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 parlementaire spéciale sur l'Union européenne de la Chambre des Lords, sous-commission de l'intérieur: enquête sur la décision-cadre relative aux dossiers passagers.
- Commission parlementaire spéciale sur l'Union européenne de la Chambre des Lords: enquête sur Europol.
- Commission des sciences et de la technologie de la Chambre des Lords: médecine génomique – implications de la génération et du stockage de données sur le génome pour la sécurité et la confidentialité des données à caractère personnel.
- Commission des projets de loi d'intérêt public de la Chambre des Communes: lecture en commission de la loi antiterrorisme.

Le bureau a également fourni des preuves écrites dans le cadre du rapport sur le partage de l'information de Thomas/Walport et a rencontré l'équipe chargée de celle-ci.

Fin 2008, nous avions reçu 340 notifications de manquements aux règles de sécurité et développé un guide destiné aux organisations afin que celles-ci sachent comment gérer les infractions aux règles de sécurité impliquant des données à caractère personnel.

Chapitre 3
Union européenne et activités communautaires

3.1. COMMISSION EUROPÉENNE

Décision 2008/49/CE de la Commission européenne du 12 décembre 2007 relative à la protection des données à caractère personnel dans le cadre de la mise en œuvre du Système d'information du marché intérieur (IMI)[24]

La Commission a décidé de compléter sa décision en adoptant des dispositions relatives à la protection des données à caractère personnel dans le contexte de l'IMI. La Commission et les États membres étant appelés à assumer diverses responsabilités et obligations en la matière dans le cadre de leurs tâches et fonctions au sein de l'IMI, cette décision définit leurs fonctions, responsabilités et droits d'accès respectifs, comme le suggérait l'avis du groupe de travail «Article 29» relatif à la problématique de la protection des données dans le cadre du Système d'information du marché intérieur (IMI).[25]

Recommandation de la Commission du 2 juillet 2008 sur l'interopérabilité transfrontalière des systèmes de dossiers informatisés de santé[26]

Cette recommandation adressée aux États membres fournit un ensemble d'orientations pour le développement et le déploiement de systèmes de dossiers informatisés de santé interopérables autorisant l'échange de données de patients au sein de la Communauté dans la mesure où des impératifs médicaux ou sanitaires l'exigent. Ces systèmes doivent permettre aux prestataires de soins de santé de veiller à ce que le patient reçoive des soins plus efficaces, grâce à un accès rapide et sécurisé, si nécessaire, à des informations fondamentales, et potentiellement vitales, sur la santé de la personne concernée, dans le respect des droits fondamentaux du patient au respect de sa vie privée et à la protection de ses données.

[24] JO L 013 du 16.01.2008, p. 18-23.

[25] Avis 01911/07/EN, DT 140.

[26] JO L 190 du 18.7.2008, p. 37-43.

3.2. COUR DE JUSTICE EUROPÉENNE

Arrêt de la Cour (grande chambre) du 29 janvier 2008 – Productores de Música de España (Promusicae) contre Telefónica de España SAU (Affaire C-275/06)[27]

Dispositif de l'arrêt:

Les directives 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique, dans le commerce intérieur («directive sur le commerce électronique»), 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, et 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 (directive vie privée et communications électroniques), n'imposent pas aux États membres de prévoir, dans une situation telle que celle de l'affaire au principal, l'obligation de communiquer des données à caractère personnel en vue d'assurer la protection effective du droit d'auteur dans le cadre d'une procédure civile. Toutefois, le droit communautaire exige desdits États que, lors de la transposition de ces directives, ils veillent à se fonder sur une interprétation de celles-ci qui permette d'assurer un juste équilibre entre les différents droits fondamentaux protégés par l'ordre juridique communautaire. Ensuite, lors de la mise en œuvre des mesures de transposition desdites directives, il incombe aux autorités et aux juridictions des États membres non seulement d'interpréter leur droit national d'une manière conforme à ces mêmes directives, mais également de ne pas se fonder sur une interprétation de celles-ci qui entrerait en conflit avec lesdits droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité.

[27] JO C 64 du 08.03.2008, p. 9.

Arrêt de la Cour (grande chambre) du 16 décembre 2008 – Heinz Huber contre Bundesrepublik Deutschland (Affaire C-524/06)[28]

Dispositif de l'arrêt:

1. Un système de traitement de données à caractère personnel relatives aux citoyens de l'Union non-ressortissants de l'État membre concerné tel que celui mis en place par la loi sur le registre central des étrangers (*Gesetz über das Ausländerzentralregister*) du 2 septembre 1994, telle que modifiée par la loi du 21 juin 2005, et ayant pour objectif le soutien des autorités nationales en charge de l'application de la réglementation sur le droit de séjour ne répond à l'exigence de nécessité prévue à l'article 7, sous point e), 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, interprété à la lumière de l'interdiction de toute discrimination exercée en raison de la nationalité, que:

- s'il contient uniquement les données nécessaires à l'application par lesdites autorités de cette réglementation, et
- si son caractère centralisé permet une application plus efficace de cette réglementation en ce qui concerne le droit de séjour des citoyens de l'Union non-ressortissants de cet État membre.

Il appartient à la juridiction de renvoi de vérifier ces éléments en l'espèce au principal.

En tout état de cause, ne sauraient être considérés comme nécessaires au sens de l'article 7, sous point e), de la directive 95/46 la conservation et le traitement de données à caractère personnel nominatives dans le cadre d'un registre tel que le registre central des étrangers à des fins statistiques.

2. Il convient d'interpréter l'article 12, paragraphe 1, CE en ce sens qu'il s'oppose à l'instauration par un État membre d'un système de traitement de données à caractère personnel spécifique aux citoyens de l'Union non-ressortissants de cet État membre dans l'objectif de lutter contre la criminalité.

Arrêt du tribunal de première instance du 8 novembre 2007 – The Bavarian Lager Co. Ltd contre Commission (Affaire T-194/04)[29]

Le tribunal de première instance des Communautés européennes (troisième chambre) a annulé une décision de la Commission du 18 mars 2004, portant rejet d'une demande d'accès au procès-verbal complet d'une réunion. Il a estimé qu'une demande adressée à la Commission des Communautés européennes visant à accéder à des données personnelles figurant dans un document de la Commission ne peut être refusée au motif de la protection de la vie privée et de l'intégrité des personnes concernées que si cette divulgation est susceptible de porter concrètement et effectivement atteinte à la protection de la vie privée et de l'intégrité desdites personnes, et que le demandeur n'était pas tenu de prouver que ladite divulgation était nécessaire. La Commission a interjeté appel.

3.3. CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Introduction

La mission du contrôleur européen de la protection des données (CEPD) consiste à veiller à ce que les libertés et droits fondamentaux des personnes physiques, et notamment leur vie privée, soient respectés par les institutions et organes fondamentaux dans le cadre du traitement des données à caractère personnel.

Conformément aux dispositions du règlement (CE) n° 45/2001[30] («le règlement»), les principes activités du CEPD sont les suivantes:

- contrôler le traitement des données à caractère personnel par les institutions et organes communautaires

[28] JO C 44 du 21.02.2009, p. 5.

[29] JO C 315 du 22.12.2007, p. 33.

[30] Règlement (CE) n° 45/2001 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).

et vérifier que les dispositions du règlement sont respectées (supervision);
- conseiller les institutions et organes communautaires sur toutes les questions ayant trait au traitement des données personnelles, et notamment émettre des avis sur les propositions de nouvelles législations et suivre les nouveaux développements ayant une incidence sur la protection des données personnelles (consultation);
- coopérer avec les autorités de contrôle nationale et avec les organismes de contrôle du «troisième pilier» de l'UE afin de renforcer la cohérence dans la protection des données à caractère personnel (coopération).

Supervision

Le travail de supervision consiste à fournir des avis et à assister les délégués à la protection des données en soumettant les traitements à risque à des contrôles préalables, à mener des enquêtes, notamment sur site, et à traiter les réclamations.

En 2008, le **contrôle préalable** est resté la principale activité du CEPD dans le cadre de sa mission de supervision. Il a ainsi publié plus de 100 avis de contrôle préalable – du jamais vu ! – portant essentiellement sur les points suivants: traitement des données relatives à la santé, recrutement de personnel et sélection des candidats, évaluation du personnel, accréditation des journalistes, systèmes de gestion des identités, contrôles d'accès et enquêtes de sécurité.

Si la plupart des institutions et organes ont bien progressé dans le respect des règles et principes en vigueur en matière de protection des données, la supervision met désormais l'accent sur la vérification de la mise en œuvre des recommandations émises suite au contrôle préalable et sur l'amélioration du degré de conformité au sein des agences. Dans ce contexte, le CEPD a développé plus avant sa **politique d'inspection** et a réalisé une première série de contrôles sur site dans différents organes et institutions, en vue de mesurer le respect des consignes dans la pratique.

En 2008, le nombre total de **réclamations** a continué à augmenter. Si les cas recevables étaient moins nombreux qu'auparavant, la complexité s'est par contre renforcée. Les cas déclarés recevables portaient notamment sur l'accès aux données, le traitement de données sensibles, le droit de rectification et l'obligation de fournir des informations.

Le CEPD a également continué à fournir des conseils sur les **mesures administratives** que les institutions et organes communautaires envisagent de prendre en ce qui concerne le traitement des données à caractère personnel. Plusieurs questions importantes ont été soulevées, notamment concernant les transferts de dossiers médicaux aux juridictions nationales, l'accès aux documents publics contenant des données personnelles, la mise en œuvre des dispositions du règlement (CE) n° 45/2001 et les plaintes traitées par le médiateur européen.

Le CEPD a continué à 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.

Consultation

Le CEPD a continué à renforcer son rôle consultatif et a été amené à émettre des avis sur un nombre croissant de propositions législatives. Il a élargi le champ de ses interventions à divers domaines politiques, ainsi qu'à tous les stades de la procédure législative.

En 2008, le CEPD a rendu 14 avis sur des propositions de législation et initiatives européennes. La majorité d'entre elles restent liées à la thématique **de la liberté, de la sécurité et de la justice**. À cet égard, l'adoption d'une **décision cadre pour la protection des données** dans le domaine de la coopération policière et judiciaire en matière pénale a constitué un événement majeur. Tout au long des négociations, ce texte a été l'un des points focaux de l'attention du CEPD, qui a émis trois opinions ainsi que des commentaires à son endroit.

La proposition visant à modifier le règlement relatif à **l'accès public aux documents** détenus par les institutions européennes, ainsi qu'à réviser la **directive vie**

privée et communications électroniques a aussi fait l'objet d'une attention toute particulière de la part du CEPD. Les questions relatives aux **dossiers passagers** ont également joué un rôle de premier plan dans les activités consultatives du CEPD, notamment eu égard au suivi de la proposition européenne en la matière.

Le CEPD s'est aussi concentré sur **l'échange d'informations**. Il a ainsi adopté des opinions sur les systèmes d'échange d'informations proposés dans le cadre du Système d'informations du marché intérieur (IMI), d'Eurojust, de la sécurité routière, de la protection des enfants qui surfent sur l'internet, du Système européen d'information sur les casiers judiciaires (ECRIS), du groupe de contact à haut niveau UE-US sur la protection et le partage des données et de la stratégie européenne e-Justice. Des commentaires préliminaires ont également été publiés quant au train de mesures de l'Union européenne sur la gestion des frontières. Les avis du CEPD mettaient en lumière la nécessité que de tels échanges d'informations fassent l'objet d'une évaluation minutieuse, assortie de garanties spécifiques en matière de protection des données.

Le recours à de **nouvelles technologies** a également été abordé à plusieurs occasions (p. ex. dans le cadre de l'ECRIS et de la stratégie européenne e-Justice). Le CEPD en a appelé plusieurs fois à la prise en compte, le plus tôt possible, des questions relatives à la protection des données. Il a également souligné que les outils technologiques ne devaient pas seulement servir à assurer l'échange d'informations, mais également à renforcer les droits des personnes concernées.

La **qualité des données** est un autre thème important. Un haut degré d'exactitude des données est nécessaire afin de prévenir toute ambiguïté concernant le contenu des informations traitées. Il est impératif que cette exactitude fasse l'objet d'un contrôle régulier et adéquat. Sans compter que des données de grande qualité ne constituent pas seulement une garantie fondamentale pour les personnes concernées, mais permettent aussi à ceux qui les traitent de les utiliser plus efficacement.

Plusieurs perspectives de changements constituant les **priorités** à venir du CEPD ont été identifiées. Parmi celles-ci figurent de nouvelles **tendances technologiques** soulevant des inquiétudes critiques en matière de protection des données et de respect de la vie privée, telles que le développement de systèmes informatiques en nuages[31] et des technologies de séquençage de l'ADN.

Concernant les nouveaux développements en matière de **politique** et de **législation**, les principaux problèmes auxquels le CEPD entend consacrer de l'attention sont les suivants:

- réflexion sur les améliorations à apporter à la **décision relative au cadre de protection des données** en vue de renforcer la protection fournie par le nouvel instrument du troisième pilier;
- **l'avenir de la directive relative à la protection des données**;
- le programme pluriannuel de la Commission dans le domaine de la liberté, de la sécurité et de la justice appelé «**programme de Stockholm**»;
- **les grandes tendances dans le maintien de l'ordre** et dans les activités législatives en relation avec la lutte contre le terrorisme et le crime organisé;
- la révision du règlement sur **l'accès public aux documents**;
- les nouvelles initiatives destinées à améliorer les **soins de santé transfrontaliers** en relation avec l'utilisation des technologies de l'information.

Coopération

La principale plateforme de coopération entre les autorités de protection des données en Europe est le **groupe de travail «Article 29»**. Le CEPD participe aux activités du groupe, qui joue un rôle crucial dans l'application uniforme de la directive relative à la protection des données.

Le CEPD et le groupe de travail ont coopéré en vue d'instaurer une bonne synergie sur divers sujets, mais surtout dans le contexte de la mise en œuvre de la directive relative à la protection des données et des défis soulevés par les nouvelles technologies. Le CEPD

[31] L'information en nuages fait référence à l'utilisation d'une technologie informatique basée sur l'internet («nuage») pour divers services. Il s'agit d'un style d'informatique fournissant des ressources évolutives de manière dynamique et souvent virtualisables sous la forme d'un service via l'internet.

a fermement soutenu les initiatives prises en vue de faciliter les flux de données internationaux.

Le groupe de travail a adopté des opinions sur des propositions législatives qui, dans certains cas, ont également fait l'objet d'avis du CEPD (p. ex. révision de la directive vie privée et communications électroniques). Si la consultation du CEPD est un élément contraignant du processus législatif de l'Union européenne, les contributions du groupe de travail sont elles aussi très utiles, d'autant qu'elles peuvent contenir des points d'attention spécifiques à un pays donné. Le CEPD se félicite donc toujours de ces apports, qui s'inscrivent dans la même philosophie que ces propres avis.

L'une des principales tâches de coopération du CEPD concerne **Eurodac**, où les responsabilités en matière de contrôle de la protection des données sont partagées entre les autorités nationales de protection des données et le CEPD. Le groupe de coordination de la supervision d'Eurodac, composé d'autorités nationales de protection des données et du CEPD, s'est réuni deux fois en 2008 et s'est concentré sur la mise en œuvre du programme de travail adopté par le groupe en décembre 2007. Trois sujets du programme avaient été sélectionnés en vue d'un examen plus approfondi suivi d'un rapport, à savoir: informations des personnes concernées, les enfants et Eurodac et DubliNet[32]. Dans le même temps, le cadre dans lequel opère le groupe a également retenu l'attention: la Commission européenne a entrepris une révision du règlement de Dublin et du règlement Eurodac, dans le contexte des mesures d'asile en général.

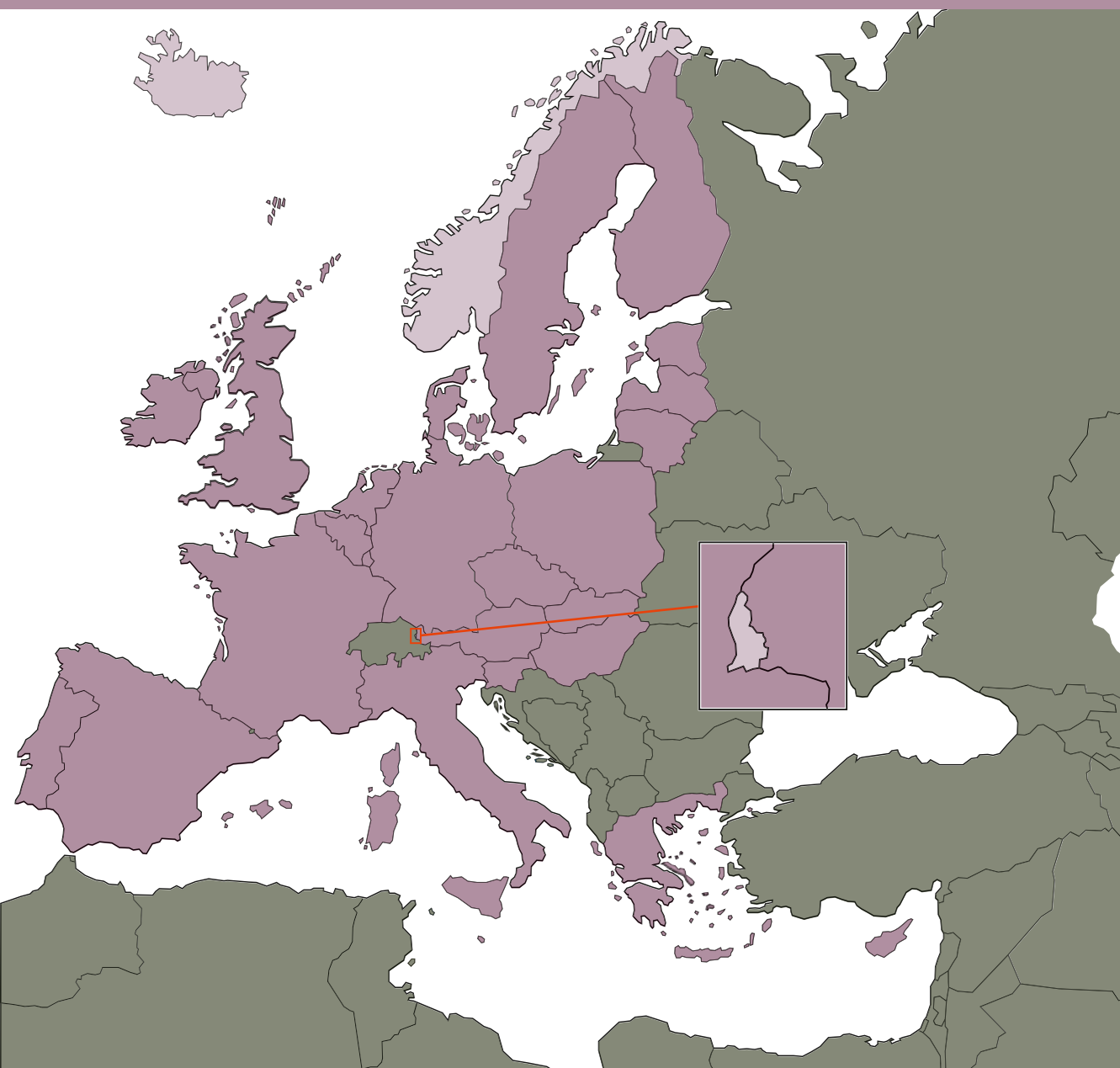
La nécessité d'une étroite coopération entre le CEPD et les autres autorités de protection des données sur les **questions relatives au troisième pilier**, à savoir la coopération policière et judiciaire, est devenue manifeste ces dernières années, suite à la multiplication des initiatives de collecte et d'échange de données personnelles au niveau européen et international.

Le CEPD s'efforce de garantir un niveau de protection des données élevé et cohérent dans les travaux des organes de contrôle de la protection de données (organes de contrôle conjoints pour Schengen, Europol, Eurojust et le Système d'information douanier) établis sous le troisième pilier de l'Union européenne. Le CEPD coopère également avec les autorités nationales de protection des données en contribuant activement aux réunions tenues par le groupe de travail sur les questions policières et judiciaires.

La coopération au sein des **forums internationaux** s'est poursuivie, notamment dans le cadre de la Conférence internationale des commissaires à la protection des données et de la vie privée, organisée à Strasbourg, et de l'«initiative de Londres», destinée à sensibiliser l'opinion publique à la protection des données et à renforcer celle-ci. Suite aux événements analogues organisés en 2005 et 2007, un troisième atelier sur la protection des données au sein des organisations internationales est actuellement à l'étude.

[32] DubliNet est le réseau électronique sécurisé de canaux de transmission reliant les autorités nationales en charge des demandes d'asile. Généralement, un «résultat positif» dans le système Eurodac déclenche un échange de données concernant le demandeur d'asile. Cet échange passe par DubliNet.

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 2008, plusieurs textes législatifs et règles administratives 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° 88/2008 relative à la procédure pénale. Cette loi contient plusieurs dispositions ayant une incidence sur la vie privée des citoyens, des défendeurs bien sûr, mais aussi, par exemple, des témoins. Parmi ces dispositions figurent celles de l'article 16 relatif à l'accès aux documents de procédure. Non seulement l'article 16 accorde ce droit au défendeur et à son conseil, mais également au public. Tant les dépositions à charge qu'à décharge sont accessibles au public. Toutefois, certaines parties de ces documents contenant des informations sur des affaires privées, financières ou commerciales ne seront pas révélées, pour autant que cette confidentialité soit équitable et raisonnable, à moins que la partie concernée accepte que ces informations soient communiquées. Les jugements et autres décisions judiciaires seront transmis au public sur demande, mais, dans des cas spécifiques, certaines informations devront être supprimées desdits documents, par exemple lorsque des intérêts privés l'exigent. Toutefois, comme le montre l'article 17, les jugements et décisions judiciaires ne sont pas toujours transmis sur demande. Les tribunaux peuvent aussi les publier, par exemple sur leurs sites internet, moyennant la suppression des données qui ne peuvent pas être rendues publiques.

2. Loi n° 97/2008 modifiant la loi sur les produits médicinaux n° 93/1994. En 2003, de nouvelles dispositions ont été ajoutées à la loi n° 93/1994, cf. loi n° 89/2003, portant sur la création d'une base de données centrale des prescriptions médicales placée sous la responsabilité de la direction nationale de la santé. Les dispositions relatives à cette base de données sont inscrites à l'article 27 de la loi n° 93/1994. Selon ces dispositions, la direction nationale de la santé a accès à la base de données afin de mener à bien son rôle de surveillance des assuétudes, des narcotiques et des produits médicinaux, ses activités générales de contrôle des prescriptions médicales et le suivi des développements en matière de produits médicinaux. L'Agence islandaise de pharmacovigilance ainsi que l'institution d'assurance-maladie peuvent également y accéder, moyennant le respect de certains critères. À l'origine, les données permettant une identification personnelle devaient être supprimées dans un délai de trois ans à compter de leur saisie dans la base de données. Toutefois, la loi n° 97/2008 a porté cette période à 30 ans.

3. Loi n° 112/2008 relative à l'assurance-maladie. Cette loi prévoyait la création d'une nouvelle institution publique, à savoir l'Institution d'assurance-maladie. Celle-ci a pour mission de négocier le règlement des soins de santé au moyen de fonds publics dédiés avec les institutions de soins de santé et les prestataires de soins de santé indépendants. Selon l'article 46 de la loi, les professionnels de la santé responsables de la conservation des dossiers de patients sont tenus de fournir à l'Institution d'assurance-maladie un accès aux données et documents nécessaires afin qu'elle puisse mener à bien sa mission. Toutefois, les employés de l'Institution ne peuvent consulter les fichiers que sur le site où ils sont conservés et uniquement les parties des documents nécessaires à l'administration des contrats de soins.

4. Loi n° 142/2008 relative à l'investigation des événements et des causes qui ont mené à la faillite des banques islandaises en 2008, et des événements connexes. Cette loi crée une commission d'enquête spéciale placée sous les auspices du Parlement islandais. Celle-ci reviendra sur la crise financière qui s'est produite à l'automne 2008 en Islande et présentera ses conclusions en la matière. Conformément à l'article 14 de la loi, la commission notifiera tout soupçon d'agissements criminels au ministère public. Par ailleurs, la commission, si elle juge vraisemblable qu'un fonctionnaire ait failli à ses obligations, en informera le directeur de l'Institution et le ministère concerné. Selon le paragraphe 1, article 6, de la loi, toutes les personnes physiques, institutions et personnes morales sont tenues de fournir tous documents, informations et explications que la commission d'enquête jugera nécessaires.

Les membres de la commission et les enquêteurs sont tenus au secret professionnel concernant les informations confidentielles portées à la connaissance de la commission, conformément à l'article 4, paragraphe 3, de la loi. La commission peut toutefois fournir des informations et des documents à des groupes de travail et experts si cela s'avère nécessaire. En outre, la commission peut également fournir des informations si celles-ci sont requises dans le cadre d'un échange mutuel d'informations ou de la coopération avec des instances étrangères chargées d'enquêtes dans des conditions analogues à celles de la commission. Le destinataire des informations sera aussi tenu à un devoir de réserve. Toutefois, conformément à l'article 4, paragraphe 4, les dispositions ci-dessus n'excluent pas la publication, par la commission, d'informations qu'elle juge nécessaires en vue de fonder ses conclusions, même si lesdites informations seraient confidentielles dans d'autres circonstances. Les informations relatives aux affaires privées de personnes physiques, y compris à leurs affaires financières, ne seront publiées que si l'intérêt public lié à leur divulgation contrebalance les intérêts particuliers de la personne en question.

En vertu de l'article 17, paragraphe 2, de la loi, les dispositions des articles 18 à 21 de la loi relative à la protection des données n° 77/2000, à savoir les dispositions relatives aux droits d'accès et aux informations à fournir à la personne concernée, ne s'appliquent pas aux activités de la commission. Toutefois, l'article 17, paragraphe 3, prévoit que les personnes faisant l'objet d'une enquête de la commission bénéficieront, au terme de celle-ci, des droits prévus par les dispositions précitées de la loi sur la protection des données si une procédure pénale n'est pas ouverte à leur encontre. Le droit d'accès sera alors régi par les dispositions de la loi de procédure *ad hoc*.

5. Loi n° 160/2008 relative à un centre de service et de connaissances pour les déficients visuels, malvoyants et non-voyants. En vertu de l'article 6 de la loi, le centre de service et de connaissances tiendra un registre sur toutes les personnes déficientes visuelles, malvoyantes et non voyantes en vue d'améliorer le service qui leur est fourni, de garantir la qualité de ce service, de superviser la fourniture du service et de réaliser des recherches scientifiques et statistiques. Le traitement des données personnelles à cet égard s'effectuera conformément à la loi relative à la protection des données.

6. Loi n°164/2008 modifiant la loi relative à l'impôt sur le revenu n° 90/2003. Son article 6 a ajouté une nouvelle disposition à la loi relative à l'impôt sur le revenu, stipulant que les banques et autres institutions financières conservant des dépôts informeront, de leur propre initiative, le commissaire national aux impôts des sommes et intérêts concernant les dépôts à la fin de chaque année.

7. Règles relatives à l'obligation de notifier ou d'obtenir un permis pour le traitement de données personnelles, n° 712/2004. Ces règles, adoptées par l'autorité de protection des données conformément aux articles 31 et 33 de la loi relative à la protection des données, remplacent la règle n° 698/2004. Le changement le plus significatif réside dans le fait que le traitement des données personnelles dans la recherche génétique n'est plus soumis à autorisation, pour autant que les personnes concernées aient consenti au traitement. Le traitement doit néanmoins être notifié à l'autorité de protection des données. Comme décrit au point 8 ci-dessous, l'autorité de protection des données a adopté des règles concernant le traitement des données personnelles dans la recherche génétique.

8. Règle n° 1100/2008 sur le traitement des données personnelles dans la recherche génétique. Comme décrit au point 7 ci-dessus, le traitement de données personnelles dans la recherche génétique n'est plus soumis à autorisation de l'APD si la personne concernée consent au traitement. Dans ce cas, les dispositions de la règle n° 1100/2008 doivent toujours être observées. Celles-ci remplacent celles relatives à l'autorisation des projets de recherche individuels. Selon ces règles, le consentement des personnes concernées doit répondre à certaines exigences. Ces personnes doivent par exemple être informées de la date de la suppression des données ou du caractère permanent de leur conservation à des fins de recherche. Elles doivent savoir s'il est prévu de contacter des parents en vue de leur demander de participer au projet de recherche et si elles sont susceptibles de recevoir des informations quant à leur génotype, si elles le souhaitent. Les règles contiennent également des dispositions relatives, par exemple, à

l'encodage des données personnelles. Celles-ci stipulent qu'aucun agent de traitement de données génétiques ne peut avoir accès aux données permettant d'identifier les personnes concernées et que les personnes qui se livrent à la recherche génétique doivent notifier à l'APD le traitement de données personnelles dans chaque projet de recherche et envoyer une description des mesures de sécurité prises à cet égard à l'Autorité. Si les mêmes mesures de sécurité sont utilisées dans plusieurs projets de recherche, une description commune pour tous ces projets suffit.

B. Jurisprudence

Le 3 octobre 2008, la Cour suprême d'Islande a émis un jugement relatif au pouvoir du commissaire national aux impôts à demander des informations financières sur des personnes physiques. Le commissaire avait demandé des données à des compagnies de cartes de crédit sur toutes les transactions effectuées à l'aide de cartes de crédit émises et facturées à l'étranger, dans les cas où le retrait total dépassait un certain montant. Cette demande se fondait sur l'article 94 de la loi relative aux impôts sur le revenu n° 90/2003, stipulant que tout le monde est tenu de fournir aux autorités fiscales les informations et documents nécessaires que celles-ci demandent.

Une compagnie de cartes de crédit a refusé de fournir les informations demandées. Conformément à l'article 94 de la loi précitée, le commissaire national aux impôts a alors demandé une décision du tribunal concernant l'obligation de la société à lui fournir lesdites informations. Le tribunal d'arrondissement de Reykjavik a conclu que la compagnie était tenue de le faire. La compagnie a fait appel de cette décision devant la Cour suprême. La Cour a estimé, entre autres, que la demande d'information du commissaire national aux impôts ne dépassait pas les limites fixées à l'article 7, paragraphe 1, alinéas 2 et 3, de la loi relative à la protection des données, stipulant que les données personnelles doivent être obtenues dans un but spécifique, explicite et pertinent et ne pas subir d'autres traitements à des fins incompatibles. Elles précisent en outre que les données personnelles concernées doivent être adéquates, pertinentes et ne pas être excessives en relation avec l'objet du traitement. En conséquence, la Cour suprême a conclu que la compagnie en question était tenue de fournir les informations demandées par le commissaire national aux impôts.

C. Questions diverses importantes

Comme mentionné dans la description des développements législatifs de 2008 présentée ci-dessus, la loi sur les produits médicinaux n° 93/1994 a été modifiée de manière à étendre la période de conservation des données personnelles dans la base de données centrale des prescriptions de trois à trente ans. Il s'agit là de l'une des principales questions relatives à la protection des données de 2008. L'autorité de protection des données a émis un avis sur la proposition de loi portant cette modification, estimant que cette extension de la période de conservation était disproportionnée.

Autre grand sujet de discussion: l'adoption de la règle n° 1100/2008 de l'autorité de protection des données relative au traitement des données personnelles dans la recherche génétique. Voir à cet égard la description fournie dans les développements législatifs de 2008.

Le 6 octobre 2008, l'autorité de protection des données a émis un avis à l'intention de la Confédération des employeurs islandais quant au fait de savoir s'il était légal pour les entreprises de traiter des données personnelles en relation avec un système de recouvrement à l'amiable. En vertu de ce système, une personne soupçonnée de vol ou de tentative de vol de marchandises ne serait pas dénoncée à la police si elle payait une certaine somme à l'entreprise concernée. La personne signerait un accord à cet effet, consentant à ce que ses données personnelles soient saisies dans une base de données gérée par une firme de sécurité donnée.

L'autorité de protection des données a considéré qu'il n'était pas certain que ce type d'accord soit légal. Par ailleurs, ce système supposerait que des entreprises privées se substituent à l'État, en décidant d'une mesure répressive punissant un comportement illicite. L'autorité de protection des données a donc estimé qu'il était peu probable que le traitement de données personnelles dans le cadre de ce type de système soit légal. En conséquence de quoi ce système n'a pas été mis en œuvre.

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 (CPD) consiste à rendre un avis sur les projets de loi et décrets pertinents pour la protection des données et à vérifier leur compatibilité avec les dispositions de la directive 95/46/CE. En 2008, le CPD a ainsi rendu un avis sur 20 projets de loi. Il convient tout particulièrement de mettre en lumière, du fait de leur importance particulière en la matière, les deux révisions partielles de la loi sur la protection des données (ou DSG, pour *Datenschutzgesetz*) du Liechtenstein, de même qu'un projet collectif concernant le traitement des données nécessitant une protection particulière, sur lequel nous reviendrons plus en détail ci-après.

La *première révision partielle de la DSG* doit être vue dans le contexte d'une adhésion aux accords de Schengen et de Dublin, qui mettent notamment l'accent sur la protection des données. Les amendements apportés portaient principalement sur la structure et l'organisation de l'unité de protection des données (ou SDS, pour *Stabsstelle für Datenschutz*). Jusque là, la SDS était intégrée à l'administration du Liechtenstein et dépendait du ministère de la justice. Elle était donc davantage considérée comme un département de ce ministère que comme une institution à part entière. De ce fait, la SDS ne répondait pas au critère qui veut que l'autorité de contrôle de la protection des données exerce «en toute indépendance les missions dont [elle est investie]», comme stipulé par la directive 95/46/CE sur la protection des données[33]. Pour garantir cette totale indépendance, le contrôleur de la protection des données devait devenir complètement autonome sur le plan institutionnel, personnel et financier. Une adaptation de la DSG était donc nécessaire en vue de se préparer au mieux à l'évaluation de l'accord Schengen/Dublin. La DSG a donc été modifiée de manière à rebaptiser le SDS «Office pour la protection des données» (ou DSS, *Datenschutzstelle*) et d'en faire une institution complètement indépendante ne rendant désormais plus compte qu'au parlement. Le CPD n'est plus désigné par le gouvernement, mais bien élu par le parlement. Il bénéficie en outre d'une indépendance personnelle et financière ainsi que d'un droit de recours propre. Ces amendements très significatifs sont entrés en vigueur le 1er janvier 2009.

Une *deuxième révision partielle de la DSG* a été engagée afin, d'une part, de mettre en œuvre les dispositions du protocole additionnel à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et, d'autre part, de transposer de manière plus fidèle à la lettre la directive sur la protection des données. Outre quelques modifications rédactionnelles mineures, reposant principalement sur l'expérience collectée au cours des cinq dernières années, de nouvelles procédures de certification en matière de protection des données vont être introduites. Celles-ci permettront de distinguer certains processus métiers, structures d'organisation mais aussi produits informatiques en leur décernant un label de qualité en matière de protection des données (ce label étant encore à créer). Ces procédures contribueront ainsi à davantage responsabiliser les détenteurs de jeux de données et, assurément, à promouvoir la protection des données. L'adaptation à la directive 95/46/CE des prescriptions en matière de transfert des données à l'étranger poursuit le même objectif. L'obligation de notification qui existait jusque là pour certaines divulgations de données à l'étranger doit disparaître au profit d'un devoir de diligence général des détenteurs de jeux de données. Une autre nouveauté est la mise en place d'une base juridique pour la surveillance vidéo dans l'espace public, après que la Commission sur la protection des données a recommandé instamment la création d'une telle base dans sa décision d'avril 2008[34]. La mise en œuvre d'une surveillance vidéo dans l'espace public est ainsi désormais conditionnée à l'autorisation préalable de l'Office pour la protection des données. Cette révision partielle entrera en vigueur le 1er juillet 2009.

Depuis l'arrivée à échéance, le 31 juillet 2007 déjà, de la période de transition prévue à l'*article 44, paragraphe 3, de la DSG*, il est strictement interdit de procéder au traitement de jeux de données et de profils personnels en dehors des cas expressément prévus par la loi. La

[33] Cf. art. 28 de la directive 95/46/CE («en toute indépendance»).

[34] Cf. ci-dessous, B.

création des bases juridiques encore inexistantes mais requises pour le traitement de données à caractère personnel nécessitant une protection particulière sera réglée *via* un *projet de loi collectif*.

B. Jurisprudence

La *décision de la Commission sur la protection des données de la principauté du Liechtenstein* (ou DSK, pour *Datenschutzkommission) du 7 avril 2008* sur la surveillance vidéo dans la zone piétonne de Vaduz constitue une décision de principe qui reflète les exigences constitutionnelles qui s'imposent à l'État en matière d'ingérence dans la vie privée[35].

Les faits:
Sur décision du conseil municipal du 29 août 2006, la Ville de Vaduz a installé des caméras de sécurité dans la zone piétonne de Vaduz. 16 caméras surveillaient ainsi en permanence l'ensemble du secteur. Cette décision de la ville de Vaduz se fondait sur l'article 52, paragraphe 4, de la loi sur les municipalités[36].

Suite à une plainte déposée auprès de la SDS[37], le contrôleur avait, dès 2007, recommandé à la Ville de réduire la surveillance vidéo dans la zone piétonne, car on ne pouvait pas partir du principe qu'il s'agissait là d'une ingérence proportionnée dans la sphère privée. Il disait douter par ailleurs que l'article 52, paragraphe 4, de la loi sur les municipalités puisse constituer une base juridique suffisante. La Ville n'ayant pas donné suite à ses recommandations, le contrôleur a porté l'affaire devant la commission afin que celle-ci tranche.

Les motifs de la décision:
La surveillance vidéo complète de la zone piétonne constitue une atteinte considérable au droit à la vie privée[38] et aux libertés individuelles[39] des passants, garantis par la Constitution. La surveillance vidéo complète d'un espace public constitue une atteinte considérable aux droits fondamentaux à la vie privée et à la liberté individuelle du simple fait qu'il s'agit d'une mesure exercée sans discernement à l'encontre de toutes les personnes qui pénètrent dans l'espace concerné, indépendamment des soupçons qui pourraient peser sur elles, et sans que cette mesure soit motivée par un comportement répréhensible concret ou soit provoquée par leur comportement des personnes filmées[40].

La commission estime que la restriction d'un droit fondamental n'est possible que lorsqu'elle repose sur une base légale, qu'elle est dans l'intérêt public, qu'elle est proportionnée et qu'elle ne vide pas de leur substance les droits protégés. Ce sont les principes reconnus par la Convention européenne des droits de l'homme.

La commission estime donc que la clause générale de l'article 52, paragraphe 4, de la loi sur les municipalités ne constitue pas une base juridique suffisante, car la surveillance vidéo intégrale d'un espace public constitue une ingérence majeure dans la sphère privée et une atteinte considérable au droit fondamental de la liberté individuelle et nécessite dès lors une autorisation légale spécifique. Plus l'atteinte aux libertés fondamentales est importante, plus les conditions qui la justifient doivent être claires. Constatant le rôle de plus en plus grand jouée par la surveillance vidéo au Liechtenstein et l'absence d'un système d'autorisation légale spécifique en la matière, la commission a donc recommandé, dans sa décision, la mise en place d'un cadre juridique concernant la surveillance vidéo[41].

Si l'intérêt public poursuivi par la Ville d'assurer le calme, la sécurité et le maintien de l'ordre et d'empêcher des délits concrets, tels des actes de vandalisme et des dégradations, est incontestable, il n'en reste pas moins que le principe de proportionnalité[42] repose sur l'idée selon laquelle une atteinte à une liberté fondamentale

[35] Le texte intégral de la décision peut être consulté à l'adresse suivante: http://www.llv.li/entscheidung_der_datenschutzkommission_zur_videoueberwachung_in_der_fussgaengerzone_in__vaduz.pdf

[36] L'article 52, paragraphe 4, de la loi sur les municipalités dispose que le maire de la municipalité dirige la police locale et veille au maintien du calme, de la sécurité et de l'ordre public. Il stipule en outre que celui-ci est habilité à prendre toutes ordonnances requises à cet effet et à instaurer des amendes sur la base des dispositions légales et policières en vigueur.

[37] Cf. rapport 2007.

[38] Art. 32, paragraphe 1, de la constitution du Liechtenstein.

[39] Art. 8 de l'EMRK.

[40] Cf. arrêt de la Cour constitutionnelle allemande du 23 février 2007, Az. 1 BvR 2368/06.

[41] Cf. ci-dessus, point A, deuxième révision partielle de la DSG.

[42] Cf. art. 4 de la DSG.

ne peut pas aller plus loin que ce qu'exige l'intérêt public. La mesure de l'autorité publique doit être adéquate pour réaliser l'objectif poursuivi dans l'intérêt public. Elle doit par ailleurs être nécessaire au regard de l'objectif poursuivi, ce qui signifie qu'elle doit cesser si une mesure équivalente mais moins stricte permet d'obtenir le résultat visé. Par ailleurs, l'intervention ne peut pas dépasser la mesure du nécessaire en termes matériels, géographiques et temporels.

Outre les principes de l'adéquation et de la nécessité, la mesure doit être proportionnelle, ce qui signifie qu'elle doit garantir un équilibre raisonnable entre l'objectif ou le but poursuivi et l'atteinte aux libertés qu'elle nécessite.

Soucieux de vérifier la proportionnalité de la mesure, le contrôleur de la protection des données avait déjà adressé, avant de porter le dossier devant la commission, diverses questions à la Ville de Vaduz. Il lui avait ainsi demandé si des mesures moins strictes avaient été examinées, si l'objectif poursuivi ne pouvait pas être atteint en plaçant ponctuellement des caméras à des «points chauds» ciblés, combien de cas de dégradations avaient été enregistrés avant et après l'installation des caméras de sécurité et dans combien de cas les enregistrements vidéo avaient servi à élucider une affaire et avaient contribué à l'identification de l'auteur des faits, etc. La Ville n'a toutefois pu apporter que des réponses insuffisantes à ces questions, y compris dans le cadre de la procédure lancée par la commission.

La commission sur la protection des données a donc confirmé, dans sa décision, la recommandation du contrôleur de la protection des données, selon laquelle la surveillance intégrale et constante de la zone devait être réduite au strict nécessaire, tant dans le temps que dans l'espace. Il s'agit en particulier de se demander si une surveillance vidéo appliquée 24 heures sur 24, sept jours par semaine, est vraiment nécessaire et si la surveillance ne pourrait pas être limitée à certains jours et à certaines heures. Par ailleurs, il convient de vérifier si la surveillance ponctuelle et ciblée de certains objets d'utilité publique ne suffirait pas.

C. Questions diverses importantes

Outre les préparatifs intensifs à l'adhésion du Liechtenstein aux accords de Schengen et de Dublin, l'Office pour la protection des données s'est également concentré sur le secteur des télécommunications et du travail. Dans ce dernier cas, il a souvent été amené à se pencher sur les questions de surveillance des travailleurs sur leur lieu de travail et sur le traitement réservé aux courriers électroniques et à l'utilisation de l'internet sur le lieu de travail. Pour la première fois depuis l'entrée en vigueur du droit d'accès indirect, inscrit à l'article 34 *nonies* de la loi sur les services de police[43], le contrôleur a dû examiner concrètement, sur demande, si des données personnelles d'intéressés avaient été utilisées par la police dans le cadre de missions ayant trait à la sûreté de l'État ou dans le cadre d'enquêtes visant la prévention de délits et si, le cas échéant, cette utilisation était légale.

Au cours de l'année de référence, on a noté un nombre important de demandes d'information quant à la légalité de divulgations de données dans les contextes les plus divers. Citons, à titre d'exemples: la publication des prénoms usuels des personnes décédées (protection de la vie privée *post mortem*); la légalité d'une divulgation de données à l'étranger; la publication de notes sur l'internet; la divulgation de données à la suite de la levée du secret d'assurance; et la divulgation d'adresses de citoyens par les municipalités.

Le public est principalement informé par le biais du site internet de la SDS, sur lequel sont publiés en permanence des renseignements sur des sujets d'actualité et/ou d'intérêt. Le nombre de visiteurs en constante augmentation témoigne de l'importance de ce site en tant qu'outil d'information: le site a enregistré 234 646 accès (8 355 visiteurs uniques) au cours de l'année de référence, soit quatre fois plus que l'année précédente.[44]

[43] L'article 34 *nonies*, paragraphe 1, de la loi sur les services de police dispose que toute personne peut exiger de l'Office pour la protection des données que celui-ci vérifie si la police nationale a respecté la loi dans le traitement de ses données dans le cadre de missions ayant trait à la sûreté de l'État (article 2, paragraphe 2) ou à la prévention de délits [article 2, paragraphe 1, point d)]. L'Office pour la protection des données communique alors à la partie requérante, selon une formule toujours identique, qu'aucune donnée la concernant n'a été traitée de manière illégale ou, en présence d'éventuelles irrégularités, qu'elle a introduit une recommandation visant à remédier à celles-ci. Cette disposition est entrée en vigueur en 2007. Cf. rapport annuel de 2007.

[44] En 2007, le nombre d'accès était de 54 679, pour 7 158 visiteurs uniques.

Les principaux thèmes abordés au cours de l'année de référence ont été: l'obligation de notification des transferts de données à l'étranger, la protection des données relatives aux enfants, les conclusions de la 30ème conférence internationale sur la protection des données, les réseaux sociaux et les communiqués de presse à l'occasion de la 2ème Journée européenne de la protection des données. Le site internet permet également, outre ces actualités, de consulter les instructions du contrôleur, ou «directives», relatives à l'interprétation et à l'application de la loi sur la protection des données. En 2008, les *directives sur les droits des personnes* concernées ont été remaniées en profondeur et actualisées, tout comme les *directives sur le traitement de la publicité non sollicitées, et plus particulièrement du spam.* Par ailleurs, des *directives relatives au traitement des données à caractère personnel dans le domaine privé* ont été élaborées. À l'occasion de la 2ème Journée européenne de la protection des données, le contrôleur de la protection des données a publié une brochure contenant ces dernières directives, qu'il a distribuée à un grand nombre de multinationales, de compagnies d'assurances et de bureaux de recouvrement au Liechtenstein. Par ailleurs, un questionnaire leur a également été remis, d'une part afin de voir comme les entreprises traitent la question de la protection des données et d'autre part en vue d'intensifier la collaboration.

Norvège

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

En mai 2008, le Storting (Parlement norvégien) a amendé la loi sur les systèmes d'archivage de données sanitaires personnelles, de manière à interdire les accès illégitimes aux dossiers de patients. Conformément à la section 13a de la loi sur les systèmes d'archivage de données sanitaires personnelles, «il est interdit de consulter, rechercher, s'approprier, utiliser ou posséder des informations sanitaires traitées en vertu de cette loi, à moins que les soins du patient, ou l'administration desdits soins, ne l'exigent ou que ces opérations soient spécifiquement autorisées par des lois ou réglementations». Toute infraction à cette disposition peut être passible d'amende ou d'une peine d'emprisonnement jusqu'à 3 mois. Ces règles sont entrées en vigueur et sont appliquées par l'Inspection des données.

En décembre 2008, le Storting a adopté plusieurs amendements à la loi relative aux données à caractère personnel. Une nouvelle disposition autorisant la prescription de règlements a été incluse à la section 3 de la loi. Cet amendement était nécessaire en vue de fournir un poids légal aux règlements planifiés sur l'accès aux courriers électroniques des employés.

Dans le même temps, une modification apportée à la section 46 de la loi a autorisé l'Inspection des données à imposer des pénalités de non-conformité pour infraction à la loi relative aux données à caractère personnel. L'Inspection des données était déjà en mesure d'imposer des amendes coercitives pour les infractions actuelles. Ce nouveau type de pénalités peut être infligé en cas d'infractions passées.

Par ailleurs, une nouvelle section 47a a été adoptée, en vertu de laquelle l'Inspection des données peut faire appel à l'Agence nationale de recouvrement pour faire appliquer les pénalités de non-conformité et les amendes coercitives qu'elle a imposées. Par le passé, l'Inspection des données n'a jamais fait usage de son autorité pour imposer des amendes coercitives, parce que les ressources nécessaires au recouvrement de telles amendes n'étaient pas disponibles.

Ces amendements légaux sont entrés en vigueur le 1er janvier 2009.

En juin 2008, le Storting a adopté des amendements à la loi relative au Système d'information Schengen (loi SIS). Ceux-ci avaient été rendus nécessaires par l'adoption, par le Conseil de l'UE, de deux règlements en décembre 2006 et d'une décision en juin 2007, qui, ensemble, formaient la base légale du Système d'information Schengen (SIS II) de deuxième génération. Ces actes législatifs ont été transposés en droit national au moyen d'amendements ad hoc apportés à la loi SIS. D'autres amendements ont été votés suite aux observations formulées lors du suivi de l'évaluation Schengen de la Norvège en 2005-2006. Enfin, d'autres encore étaient nécessaires parce que la Norvège a choisi d'effectuer des recherches directes dans le SIS II central lorsque celui-ci sera opérationnel. En conséquence, l'Inspection des données est tenue de vérifier, sur demande de la personne concernée, si les données la concernant qui figurent dans le SIS sont correctes, si les règles d'accès ont été observées et si les informations ont été enregistrées et utilisées conformément à la loi SIS. Si les informations ont été saisies par une autre partie à la Convention, ce contrôle doit s'effectuer en consultation avec l'organe de contrôle de celle-ci. Ces amendements ne sont pas encore entrés en vigueur.

La nouvelle loi sur la liberté d'information, de même que les règlements y afférents (adoptés en 2007), qui devaient entrer en vigueur le 1er juillet 2008, ont été reportés au 1er janvier 2009. La nouvelle loi était mentionnée dans le rapport annuel de 2007. Il s'ensuit que les organes publics qui archivent des courriers électroniques devront mettre ces enregistrements à disposition sur l'internet dès que le système électronique public correspondant sera finalisé. Les noms de personnes ne pourront faire l'objet de recherches dans ce système que pendant 12 mois. En outre, la loi permet également la publication de documents publics sur l'internet. Toutefois, les règlements prévoient que certaines données ne pourront jamais y être postées. C'est le cas des informations soumises à une obligation de confidentialité, des données personnelles sensibles, des numéros d'identité

nationaux, des numéros d'identité personnels et des numéros associés à une fonction spécifique ainsi que des informations relatives au salaire et autres rémunérations de personnes physiques, à l'exception des informations concernant les salaires et rémunérations des cadres supérieurs du secteur public et des cadres supérieurs et administrateurs d'entités juridiques indépendantes.

Le Storting a adopté une nouvelle loi sur la recherche médicale. Celle-ci était mentionnée dans le rapport annuel de 2007 auquel nous renvoyons pour plus de détails. Aucune date n'a encore été fixée pour son entrée en vigueur.

B Jurisprudence

Aucune.

C. Questions diverses importantes

Répartition peu claire des responsabilités et contrôle interne inadéquat
La loi relative aux données à caractère personnel prévoit que la responsabilité du traitement des données personnelles incombe à un contrôleur. En 2008, les activités de contrôle ont révélé une répartition peu claire des responsabilités pour un certain nombre de bases de données et registres de données personnelles. Les inspections effectuées ont aussi montré que les routines de contrôle internes étaient souvent insatisfaisantes et qu'il était fait appel à des agents du traitement des données même si aucun accord adéquat n'a été conclu avec eux.

L'intensification des échanges entre bases de données affaiblit la protection des données
Le nombre d'agences partageant des données personnelles d'autres services et agences du gouvernement ou disposant d'un accès à celles-ci a tendance à augmenter. L'objectif de ce partage consiste souvent à renforcer l'efficacité des procédures. En 2008, ce phénomène était particulièrement manifeste dans les secteurs de la justice et de la santé ainsi que dans la proposition d'une nouvelle loi concernant le registre de la population.

Les systèmes employés dans le secteur de la justice sont développés méthodiquement en vue de permettre davantage d'échanges au niveau de la base de données. Du point de vue de l'Inspection des données, cette évolution signifie que des exigences strictes doivent être définies dans la réglementation légale des registres de police. L'Inspection des données est consciente du fait que le ministère de la justice travaillait à un projet de législation en 2008. Elle a dès lors formulé des suggestions d'amendements spécifiques qu'elle jugeait nécessaires concernant la nouvelle loi sur les registres de police, par exemple l'amélioration des garanties fondamentales, et notamment des modalités adéquates pour la suppression/le tri des données, le contrôle d'accès et l'obligation de confidentialité.

Usage plus répandu de fausses caméras de vidéosurveillance
L'Inspection des données est de plus en plus souvent contactée par des personnes qui estiment que leur vie privée est violée par des caméras de surveillance qui, après examen plus approfondi, s'avèrent être des leurres. L'utilisation de fausses caméras pose un problème de principe délicat. Dans de nombreux cas, elles sont positionnées de manière telle qu'elles représenteraient une surveillance illicite si elles étaient réelles.

Or, même s'il ne s'agit pas de vraies caméras, le sentiment d'être surveillé est lui bien réel. Dans le pire des cas, ces caméras en plastique inoffensives peuvent avoir un grand impact sur la perception qu'a une personne de sa vie quotidienne. Toutefois, aucun traitement de données personnelles n'ayant effectivement lieu, l'utilisation de ces caméras n'est pas couverte par la loi relative aux données à caractère personnel.

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 2008

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 internet: http://www.dsk.gv.at/	M. Willem Debeuckelaere Commission de la protection de la vie privée 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 internet: 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 2 915 3501 Fax: +359 2 915 3525 E-mail: kzld@government.bg kzld@cpdp.bg Site internet: http://www.cdpd.bg	M^me^ Goulla Frangou Commissaire à la protection des données à caractère personnel (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str. Athanasia Court, 2nd floor - CY - 1082 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 internet: 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 internet: 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 internet: http://www.datatilsynet.dk

Estonie	**Finlande**
M. Urmas Kukk M. Viljar Peep 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 internet: 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 internet: http://www.tietosuoja.fi
France	**Allemagne**
M. Alex Türk Président 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 internet: http://www.cnil.fr	M. Peter Schaar 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 internet: 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 Site internet: http://www.datenschutz-berlin.de

Grèce	**Hongrie**
M. Christos Yeraris Autorité hellénique pour la protection des données à caractère personnel (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1-3, avenue Kifisias 115 23 GR – Athènes Tél: +30 210 6475608 Fax: +30 210 6475789 E-mail: christosyeraris@dpa.gr Site internet: http://www.dpa.gr	M. András Jóri Commissaire parlementaire 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 internet: 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 internet: 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@garanteprivacy.it Site internet: http://www.garanteprivacy.it
Lettonie	**Lituanie**
M^{me} Signe Plumina Inspection nationale des données (Datu valsts inspekcija) Blaumana str. 11/13 – 15, Riga, LV-1011, Latvia Tél: +371 6722 31 31 Fax: +371 6722 35 56 E-mail: signe.plumina@dvi.gov.lv, info@dvi.gov.lv Site internet: http://www.dvi.gov.lv	M. Algirdas Kunčinas Inspection de protection des données (Valstybinė duomenų apsaugos inspekcija) A.Juozapaviciaus str. 6 / Slucko str. 2, LT-01102 Vilnius Tél: +370 5 279 14 45 Fax: + 370 5 261 94 94 E-mail: ada@ada.lt Site internet: http://www.ada.lt

Luxembourg	**Malte**
M. Gérard Lommel Commission nationale pour la Protection des Données - CNPD 41, avenue de la Gare - L - 1611 Luxembourg Tél: +352 26 10 60 -1 Fax: +352 26 10 60 – 29 E-mail: info@cnpd.lu Site internet: http://www.cnpd.lu	M. Joseph Ebejer Commissaire à la protection des données Bureau du Commissaire à la protection des données (Office of the Data Protection Commissioner) 2, Airways House High Street Sliema SLM 1549 MALTE Tél: +356 2328 7100 Fax: +356 23287198 E-mail: joseph.ebejer@gov.mt Site internet: 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 internet: 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 internet: 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 internet: 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 internet: 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 internet: 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 internet: 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 internet: 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 internet: http://www.datainspektionen.se
Royaume-Uni	**Contrôleur européen de protection des données**
M. Richard Thomas Bureau du commissaire à l'information Wycliffe House Water Lane, Wilmslow, SK9 5AF GB Tél: +44 1625 545700 Fax: +44 1625 524510 E-mail: Veuillez compléter le formulaire sur notre site internet Site internet: 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 internet: http://www.edps.europa.eu

OBSERVATEURS DU GROUPE DE TRAVAIL «ARTICLE 29» RELATIF À LA PROTECTION DES DONNÉES EN 2008

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 internet: 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 internet: http://www.datatilsynet.no
Liechtenstein	**République de Croatie**
M. Philipp Mittelberger Commissaire chargé de la protection des données Bureau de protection des données (Datenschutzstelle, DSS) Kirchstrasse 8, Postfach 684 – FL -9490 Vaduz Tél: +423 236 6090 Fax: +423 236 6099 E-mail: info@dss.llv.li Site internet: http://www.dss.llv.li	M. Franjo Lacko Directeur M^me^ 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 internet: 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 internet: www.dzlp.mk , info@dzlp.gov.mk	

Secrétariat du groupe de travail «Article 29»

M[me] Niovi Ringou
Chef d'unité faisant fonction
Unité de protection des données
Direction générale Justice, liberté et sécurité
Commission européenne
Bureau: LX46 1/02 - BE - 1049 Brussels
Tél: +32 2 295 12 87
Fax: +32 2 299 8094
E-mail: Niovi.Ringou@ec.europa.eu
Site internet: http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm

NE-AC-10-002-FR-C
10.2758/22388

COMMISSION
EUROPÉENNE

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 978-92-79-13758-7