Commission européenne
Justice

# Treizième rapport annuel
## du groupe de travail «Article 29» sur la protection des données


1830-6454

# Treizième 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 2009

---

Adopté le 14 juillet 2010

Ce groupe de travail a été institué en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la Direction C (Justice civile, droits fondamentaux et citoyenneté) de la direction générale Justice de la Commission européenne, Belgique, bureau LX-46 01/190.

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

# TABLE DES MATIÈRES

Présentation du président du groupe de travail «Article 29» sur la protection des données ..... 4

1. Questions examinées par le groupe de travail «Article 29» sur la protection des données à caractère personnel ..... 7
   - 1.1. Transfert de données vers les pays tiers ..... 8
   - 1.2. Communications électroniques internet et nouvelles technologies ..... 11
   - 1.3. Données à caractère personnel ..... 12
   - 1.4. Comptabilité, audit et matières financières ..... 13

2. Principaux développements dans les États membres ..... 15
   - Autriche ..... 16
   - Belgique ..... 18
   - Bulgarie ..... 23
   - Chypre ..... 26
   - République tchèque ..... 28
   - Danemark ..... 31
   - Estonie ..... 33
   - Finlande ..... 35
   - France ..... 39
   - Allemagne ..... 46
   - Grèce ..... 49
   - Hongrie ..... 56
   - Irlande ..... 58
   - Italie ..... 59
   - Lettonie ..... 67
   - Lituanie ..... 71
   - Luxembourg ..... 77
   - Malte ..... 79
   - Pays-bas ..... 81
   - Pologne ..... 85
   - Portugal ..... 88
   - Roumanie ..... 90
   - Slovaquie ..... 93
   - Slovénie ..... 98
   - Espagne ..... 103
   - Suède ..... 109
   - Royaume-Uni ..... 113

3. Union européenne et activités communautaires ..... 115
   - 3.1. Commission européenne ..... 116
   - 3.2. Cour de justice européenne ..... 117
   - 3.3. Contrôleur européen de la protection des données ..... 118

4. Principaux développements dans les pays de l'EEE ..... 123
   - Islande ..... 124
   - Liechtenstein ..... 126
   - Norvège ..... 129

5. Membres et observateurs du groupe de travail «Article 29» relatif à la protection des données ..... 131
   - Membres du groupe de travail «Article 29» relatif à la protection des données en 2009 ..... 132
   - Observateurs du groupe de travail «Article 29» relatif à la protection des données en 2009 ..... 137

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

En 2009, les nouvelles technologies évoluent à un rythme effréné et dans un monde sans frontières. Notre cadre juridique et nos pratiques doivent ainsi s'adapter à ces transformations profondes, et ce en maintenant un niveau élevé de protection des données.

Nous avons établi les fondements possibles d'une régulation mondiale de la protection des données lors de la 31e Conférence internationale des commissaires à la protection des données (Madrid, novembre 2009) en adoptant une résolution visant à établir des standards internationaux pour la protection de la vie privée et des données à caractère personnel. Il s'agit là d'un pas historique, car pour la première fois les autorités de protection des données sont parvenues à élaborer au niveau mondial un corpus de principes communs adaptés aux dernières évolutions technologiques.

Une réflexion sur les conséquences organiques et juridiques de ces choix s'impose et un important travail de sensibilisation des pouvoirs publics doit être rapidement engagé afin que ces derniers prennent des initiatives pour mettre en place un instrument juridique international ayant une valeur contraignante.

Dans le même temps, une réflexion au niveau européen sur l'adaptation des outils existants a été engagée. Parmi les initiatives lancées en 2009, j'aimerais mentionner plus particulièrement l'initiative de la Commission européenne, qui sous l'impulsion de son vice-président, Jacques Barrot, et du G29, a organisé une grande consultation publique visant à obtenir des contributions relatives aux nouveaux défis en matière de protection des données et à l'amélioration du cadre juridique de protection des données personnelles au sein de l'Union européenne.

Le groupe de l'Article 29 et le groupe Police-Justice ont ainsi mis à profit leur expérience et leur expertise pour livrer un avis majeur à la fois au niveau européen et pour la protection des données en général, notamment en prenant en compte l'impact de l'entrée en vigueur du Traité de Lisbonne au 1er décembre. Cet avis présente des propositions pour améliorer les outils et les pratiques existants. Citons entres autres la volonté de développer des mesures pratiques à l'attention de l'individu notamment par une meilleure lisibilité de ses droits et la mise en place de moyens d'action concrets à sa disposition pour les exercer. Il s'agit aussi d'élever la protection des données dans l'entreprise au rang des valeurs éthiques communes et partagées et de renforcer l'efficacité concrète des actions entreprises par les responsables de traitement pour démontrer leur conformité aux textes juridiques applicables.

Plus encore, une réflexion a été engagée sur l'indépendance et l'évolution du rôle et des pouvoirs des autorités de protection des données qui sont amenées à exercer un rôle de vigie en alertant au plus tôt les pouvoirs publics ou plus largement le grand public sur des questions qui pourront rapidement devenir des grands problèmes de société.

J'ai ainsi eu l'occasion de partager mon inquiétude dans mon courrier de fin de mandat adressé à mes homologues européens en février 2010. J'ai toujours considéré – et encore aujourd'hui – que le G29 doit jouer un rôle phare, sur la scène européenne et internationale, en matière de protection des données personnelles et de la vie privée. Mais j'ai été amené à constater qu'il était devenu, dans son fonctionnement actuel, lourdement handicapé par son absence de moyens financiers autonomes.

Le renforcement des moyens du G29 permettrait d'organiser davantage d'auditions, de recourir à davantage d'experts pour être à même de réagir face aux évolutions technologiques les plus récentes, et plus généralement d'entreprendre les actions nécessaires pour faire entendre sa voix sur des sujets essentiels. L'octroi d'un budget

propre au G29 ainsi que la mise en place d'un secrétariat spécifique, conditionneront l'efficacité, la visibilité et l'indépendance – et donc la crédibilité – du G29 dans les années à venir.

Le travail du G29 est également entravé par un manque cruel de moyens de fonctionnement et notamment de locaux. Il est également difficile de bénéficier pour chaque réunion des services d'interprétariat adaptés et permettant à tous les experts nationaux de participer aux travaux du G29. Par ailleurs, notre groupe devrait disposer d'outils de communication plus efficaces, notamment par la maîtrise d'un site Internet propre. L'amélioration des outils de communication serait assurément de nature à accroître la visibilité des travaux et des actions menées.

Il est ainsi devenu urgent d'octroyer aux autorités de protection des données et au groupe de l'Article 29 des moyens tant humains que financiers à la mesure de leurs missions.

**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/2009_en.htm

# 1.1. TRANSFERT DE DONNÉES VERS LES PAYS TIERS

## 1.1.1. Dossiers passagers / PNR

### Avis n° 8/2009 (WP 167) sur la protection des données relatives aux passagers, collectées et traitées par les comptoirs de vente hors taxes des aéroports et des ports

Le droit communautaire permet d'exonérer de droits d'accises les achats effectués par les passagers dans les comptoirs de vente hors taxes des aéroports et des ports, en soumettant toutefois lesdits achats à certaines conditions. Pour satisfaire à ces conditions, la plupart des comptoirs situés dans les États membres de l'Union européenne collectent et traitent des données, y compris des données relatives aux passagers, à l'occasion de l'achat d'articles.

Toutefois, les pratiques mises en œuvre par les comptoirs de vente hors taxes en ce qui concerne le traitement et la collecte de ces données relatives aux passagers varient considérablement d'un pays à l'autre à travers l'Union européenne. Les passagers ne reçoivent absolument aucune information quant à la collecte des données, y compris de leurs données à caractère personnel, à l'objectif de la collecte, à leurs droits et à l'utilisation de ces informations par des organismes publics lorsque lesdites données leur sont transférées.

En vertu de l'article 30 de la directive 95/46/CE, la Commission européenne a demandé au groupe de travail «Article 29» d'examiner cette question et de passer en revue les pratiques actuelles en matière de protection des données dans les États membres de l'Union européenne en vue de formuler, si nécessaire, des recommandations pour la mise en œuvre uniforme des principes généraux relatifs à la protection des données que les comptoirs de vente hors taxes des aéroports et des ports sont tenus de respecter.

Le présent avis analyse les aspects juridiques et pratiques de la collecte et du traitement des données relatives aux passagers dans les comptoirs de vente hors taxes, avec pour objectif de fournir des conseils aux vendeurs travaillant dans ces comptoirs ainsi qu'aux autorités douanières chargées de veiller à la mise en œuvre du droit communautaire afin d'obtenir une meilleure harmonisation de l'application des dispositions existantes.

## 1.1.2. Clauses contractuelles types

### Avis n° 3/2009 (WP 161) concernant le projet de décision de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants de données établis dans des pays tiers en vertu de la directive 95/46/CE (responsable du traitement de données vers sous-traitant de données)

Depuis plusieurs années, les entreprises et autorités de protection des données (APD) se fondent sur les clauses contractuelles types, adoptées par la Commission européenne le 27 décembre 2001[2], pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers, en vertu de la directive 95/46/CE (transfert du responsable du traitement de données vers un sous-traitant de données, régi par la décision 2002/16/CE).

Bien que les clauses contractuelles types sur lesquelles porte la décision 2002/16/CE constituent une base solide pour le transfert de données à caractère personnel, la demande de «mise à jour» de celles-ci se fait de plus en plus pressante d'année en année. La volonté de «mettre à jour» les clauses contractuelles types de la décision 2002/16/CE est essentiellement motivée par l'avènement de l'«externalisation globale». De plus en plus d'entreprises transférant leurs données non seulement vers un sous-traitant (de premier niveau), mais également vers des «sous-sous-traitants» (que nous appellerons «sous-traitants de deuxième niveau»), voire vers des sous-traitants de troisième niveau ultérieurement, les clauses contractuelles types de la décision 2002/16/CE ne permettent pas de faire face à la complexité de ces transferts ultérieurs. Aussi la Commission européenne juge-t-elle nécessaire de modifier les clauses contractuelles types de la décision 2002/16/CE afin que les contrats soient davantage en phase avec la nouvelle

[2] JO L 6 du 10.1.2002, p.52. cf. avis du groupe de travail n° 7/2001 (WP 47), disponible à l'adresse suivante: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp47en.pdf

donne en matière d'accords commerciaux, et ce en adoptant une nouvelle décision fondée sur l'article 26, paragraphe 4, de la directive 95/46/CE.

### 1.1.3. Agence mondiale antidopage (AMA)

**Deuxième avis n° 4/2009 (WP 162) sur le standard international pour la protection des renseignements personnels de l'Agence mondiale antidopage (AMA), sur les dispositions du code de l'AMA s'y rapportant et sur d'autres questions relatives à la vie privée dans le cadre de la lutte contre le dopage dans le sport par l'AMA et les organisations (nationales) antidopage**

Dans son premier avis sur cette question[3], le groupe a examiné la compatibilité du projet de standard international pour la protection des renseignements personnels (ci-après «le standard pour la protection des renseignements personnels» ou «le standard») avec le niveau de protection minimal requis par la réglementation européenne en matière de protection des données. Bien qu'il ait exprimé son soutien en faveur de plusieurs aspects du standard, notamment la référence à la directive 95/46/CE, le groupe n'a pas conclu à la compatibilité de ce projet avec le niveau minimal de protection offert par la directive et a formulé certaines recommandations.

Le projet de standard a depuis été modifié et sa version révisée est entrée en vigueur le 1er janvier 2009. L'Agence mondiale antidopage (AMA) a fourni des informations complémentaires, en réponse aux précédentes demandes de clarification du groupe. Le groupe se félicite de l'intégration de certaines de ses remarques au standard pour la protection des renseignements personnels[4]. Il regrette néanmoins que ses autres remarques n'aient pas été prises en compte (voir point 3.2. ci-après).

La Convention internationale contre le dopage dans le sport adoptée par l'UNESCO en 2005, ratifiée par 25 des 27 États membres de l'UE, a été conclue pour soutenir les travaux de l'AMA au niveau international. Elle ne modifie en rien les droits et obligations des signataires qui découlent d'autres accords préalablement conclus (article 6 de la convention) et encourage la coopération entre les États dans des circonstances appropriées, toujours dans le respect du droit interne. Conformément au droit communautaire, toute disposition d'un accord international incompatible avec le droit communautaire est subordonnée à ce dernier. La convention de l'UNESCO ne fait aucune référence expresse aux droits fondamentaux en général ou aux droits en matière de protection des données en particulier.

Le groupe de travail ne saurait limiter ses remarques au seul standard pour la protection des renseignements personnels. En effet, celui-ci contenant de nombreuses références au code de l'AMA et à la base de données ADAMS (voir point 2.2.), il est nécessaire de l'examiner dans le contexte plus large de son application. Aussi, après avoir rappelé les principales caractéristiques du système élaboré par l'AMA (point 2), l'avis abordera-t-il de manière plus détaillée les questions suivantes: la localisation (point 3.1.), les remarques du premier avis qui n'ont pas été prises en compte (point 3.2.), les motifs de traitement (point 3.3.), le transfert des données vers la base de données ADAMS au Canada et d'autres pays en dehors de l'Union européenne (point 3.4.), les durées de conservation (point 3.5.) et les sanctions (point 3.6.).

[3] Avis n° 3/2008 du 1er août 2008 sur le projet de norme internationale de protection de la vie privée du code mondial antidopage (WP 156) http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp156_en.pdf

4 La définition modifiée de «traitement», de «données sensibles» (terme qui n'inclut plus les opinions politiques, religieuses ou philosophiques et l'adhésion à un syndicat, éléments dont la pertinence dans le cadre de la lutte contre le dopage a été mise en cause par le groupe de travail (point 3.2)) et la clarification apportée au point 6.2. Le groupe de travail a également constaté que l'article 6 a été reformulé et que désormais, en plus du consentement (désormais éclairé), il dispose que les «renseignements personnels» doivent être traités «lorsque la loi le prévoit expressément». Il a également observé d'autres modifications correspondant aux remarques qu'il avait formulées, dont la rédaction du commentaire sur l'article 9.2, la suppression des termes «manifestement abusives» à l'article 11.2 en ce qui concerne l'exercice du droit d'accès et la mention à l'article 11.5 du droit des participants de déposer une réclamation auprès d'une organisation antidopage internationale.

Dans l'Union, les responsables du traitement des données, tels que les organisations nationales antidopage (ONAD), les fédérations sportives nationales ou internationales et les comités olympiques, peuvent évaluer certaines des limites juridiques qui existent pour le traitement des données à caractère personnel des sportifs (et d'autres personnes concernées). Le groupe de travail souligne que les responsables du traitement dans l'Union sont tenus d'assurer un traitement des données à caractère personnel conforme au droit communautaire et à leur droit national et qu'ils ne doivent par conséquent pas tenir compte du code mondial antidopage et des standards internationaux lorsque ces derniers sont en contradiction avec ces droits. Le groupe de travail leur recommande de solliciter les conseils d'un juriste.

## 1.1.4. Caractère adéquat

### Avis n° 6/2009 (WP 165) sur le niveau de protection des données à caractère personnel assuré en Israël

Le 12 juillet 2007, la mission israélienne auprès de l'Union européenne a demandé à la Commission d'engager la procédure en vue de constater qu'Israël est un pays tiers assurant un niveau de protection adéquat au sens des articles 25 et 26 de la directive.

Afin d'apprécier le caractère adéquat du niveau de protection assuré en Israël, la Commission a chargé le Centre de recherche informatique et droit (ci-après dénommé le «CRID») de l'université de Namur d'élaborer un rapport détaillé évaluant le respect par le système réglementaire israélien des conditions posées à l'application de la réglementation en matière de protection des données à caractère personnel dans le document de travail «Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données», adopté le 24 juillet 1998 par le groupe de travail institué par l'article 29 de la directive (document WP 12).

Le rapport susmentionné et la réponse préliminaire des autorités israéliennes à celui-ci ont été examinés par le sous-groupe «Sphère de sécurité» lors d'une réunion qui s'est tenue le 18 mars 2009. Lors de cette réunion, le sous-groupe a demandé au groupe de travail son avis sur l'envoi par son président d'une lettre adressée aux autorités israéliennes qui, tout en donnant une appréciation positive du régime actuel de protection des données en Israël, insisterait sur les points nécessitant des éclaircissements supplémentaires.

Le 2 septembre 2009, par l'intermédiaire de l'Autorité israélienne chargée du droit, de l'information et des technologies (ci-après dénommée «ILITA»), les autorités israéliennes ont adressé au groupe de travail un rapport détaillé dans lequel elles répondaient aux questions soulevées dans la lettre précitée. Ce rapport a été analysé par les membres du sous-groupe et a également fait l'objet, le 16 septembre 2009, d'une réunion au cours de laquelle les membres du sous-groupe ont demandé aux autorités israéliennes, représentées par le responsable de l'ILITA et le directeur de son service juridique, de clarifier les points qui, après examen du rapport envoyé au sous-groupe, nécessitaient encore des explications.

Le sous-groupe a informé le groupe de travail, lors de sa réunion des 12 et 13 octobre 2009, des conclusions de la réunion du 16 septembre avec les autorités israéliennes et a proposé l'adoption du présent avis, dans les conditions qui y sont énoncées. Cette proposition a été approuvée par le groupe de travail lors de cette réunion.

### Avis n° 7/2009 (WP 166) sur le niveau de protection des données à caractère personnel dans la Principauté d'Andorre

Le 21 mai 2008, l'Ambassadeur de l'Andorre auprès de l'Union européenne a demandé à la Commission d'engager la procédure en vue de déclarer que la Principauté d'Andorre assure un niveau de protection adéquat au sens de l'article 25, paragraphe 6, de la directive 95/46/CE relative à la protection des données à caractère personnel.

Aux fins d'apprécier le caractère adéquat du niveau de protection des données en Andorre, la Commission a chargé le Centre de recherche informatique et droit (ci-après dénommé le «CRID») de l'Université de Namur de produire un rapport sur le sujet. Le CRID a élaboré un rapport détaillé, qui analyse le respect par le système réglementaire andorran des exigences concernant le droit matériel et la mise en œuvre des mécanismes de protection des données à caractère personnel, telles que définies dans le document de

travail «Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive de l'UE relative à la protection des données», adopté le 24 juillet 1998 par le groupe de travail (document WP12).

Le rapport a fait l'objet d'un débat du sous-groupe «Sphère de sécurité» lors de sa réunion du 18 mars 2009. Lors de cette réunion, le sous-groupe a demandé l'avis du groupe de travail concernant une lettre envoyée par son président aux autorités andorranes, qui, tout en donnant une appréciation positive du régime actuel de protection des données dans la Principauté, insisterait sur certains points susceptibles de nécessiter des éclaircissements supplémentaires.

Le 31 juillet 2009, les autorités andorranes, par l'intermédiaire de l'Agence andorrane de protection des données (APDA), ont adressé au groupe de travail «Article 29» un rapport circonstancié, dans lequel elles répondaient aux questions soulevées dans la lettre susvisée. Ce rapport a été analysé par le sous-groupe et a également fait l'objet d'une audition, le 16 septembre 2009, au cours de laquelle les membres du sous-groupe ont demandé aux autorités andorranes, représentées par le directeur de l'APDA, le responsable de son département «Inspection» et le responsable de son département juridique, des éclaircissements sur les points qui, à l'issue du précédent débat sur le rapport envoyé par le sous-groupe, nécessitaient encore des explications complémentaires.

Le sous-groupe a informé le groupe de travail, lors de sa réunion des 12 et 13 octobre 2009, des conclusions de l'audition et a proposé l'adoption du présent avis, sous réserve des conditions qu'il énonce. Cette proposition a été approuvée par le groupe de travail lors de cette réunion.

### 1.1.5. Procédure d'échange d'informations avant le procès («pre-trial discovery»)

**Document de travail n° 1/2009 (WP 158) sur la procédure d'échange d'informations avant le procès («pre-trial discovery») dans le cadre de procédures civiles transfrontalières**

Le présent document de travail indique aux responsables du traitement des données soumis au droit communautaire comment traiter les demandes de transfert de données à caractère personnel vers un autre État en vue de leur utilisation dans une procédure civile. Le groupe de travail a rédigé le présent document parce qu'il craint qu'en raison, notamment, de la diversité des approches de la procédure civile dans les États membres, la directive 95/46/CE ne soit pas toujours appliquée de manière uniforme.

Dans la première partie du document, le groupe de travail donne un aperçu des différences d'approche des procédures civiles, et en particulier de la procédure d'échange d'informations avant le procès («pre-trial discovery»), entre les juridictions de «common law» comme celles des États-Unis et du Royaume-Uni et les juridictions de tradition civiliste.

Il décrit ensuite les lignes directrices destinées aux responsables du traitement des données lorsqu'ils tentent de concilier les exigences de la procédure judiciaire à l'étranger avec les obligations fixées par la directive 95/46/CE en matière de protection des données.

## 1.2. COMMUNICATIONS ÉLECTRONIQUES, INTERNET ET NOUVELLES TECHNOLOGIES

**Avis n° 1/2009 (WP 159) concernant les propositions modifiant la directive 2002/58/CE sur 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 (ci-après «la proposition») modifiant la directive 2002/58/CE concernant le traitement des données à caractère personnel dans le **secteur des communications** électroniques (directive «vie privée et communications électroniques») et la directive 2002/21/CE (directive-cadre). La proposition a finalement été adoptée par le Parlement européen et le Conseil le 25 novembre 2009.

Le groupe de travail a déjà adopté deux avis sur les propositions modifiant le cadre réglementaire européen pour les réseaux et services de communications électroniques (l'avis n° 8/2006 adopté le 26 septembre 2006[5] et l'avis n° 2/2008 adopté le 15 mai 2008[6]).

Tout en se réjouissant qu'il ait été tenu compte de certaines de ses recommandations précédentes, le groupe de travail tient à souligner certains aspects essentiels des questions soulevées à la suite de la première lecture au Parlement et au Conseil.

### Avis n° 5/2009 (WP 163) sur les réseaux sociaux en ligne

Le présent avis se concentre sur la façon dont le fonctionnement des sites de réseautage social (SRS) peut répondre aux exigences de la législation de l'UE en matière de protection des données. Il a principalement pour objectif de donner des indications aux fournisseurs de SRS quant aux mesures à mettre en place afin de garantir le respect du droit communautaire.

Cet avis souligne que les fournisseurs de SRS et, dans de nombreux cas, les fournisseurs tiers sont responsables du traitement des données, avec les responsabilités que cela implique envers les utilisateurs de SRS. L'avis observe que bon nombre d'utilisateurs évoluent dans une sphère purement personnelle et qu'ils contactent des personnes pour gérer leurs affaires personnelles, familiales ou domestiques. L'avis estime que «l'exemption domestique» s'applique dans ces cas, qui ne sont donc pas régis par les réglementations relatives aux responsables de traitement des données. L'avis précise également dans quelles circonstances les activités d'un utilisateur de SRS ne sont pas couvertes par «l'exemption domestique». La diffusion et l'utilisation d'informations disponibles sur les SRS à des fins secondaires, non recherchées, sont une préoccupation majeure du groupe de travail «Article 29». L'avis recommande une sécurité robuste et des paramètres par défaut permettant de respecter la vie privée comme point de départ idéal pour tous les services offerts. La principale source de préoccupation semble être l'accès aux informations relatives au profil. L'avis aborde également des thèmes tels que le traitement de données ou d'images sensibles, la publicité ou le marketing direct sur les SRS ainsi que les problèmes de conservation des données.

Les recommandations essentielles portent sur les obligations des fournisseurs de SRS de se conformer à la directive relative à la protection des données et sur le maintien et le renforcement des droits des utilisateurs. L'engagement primordial des fournisseurs de SRS devrait être de donner aux utilisateurs dès leur inscription des informations sur leur identité et avancer toutes les raisons pour lesquelles les données à caractère personnel sont traitées. Une attention particulière devrait également être accordée au traitement des données à caractère personnel des mineurs. Selon l'avis, les utilisateurs ne devraient pas mettre en ligne des photos ou des informations concernant d'autres personnes sans le consentement de celles-ci. De plus, l'avis considère que les SRS sont également tenus de conseiller leurs utilisateurs en ce qui concerne les droits au respect de la vie privée d'autrui.

## 1.3. DONNÉES À CARACTÈRE PERSONNEL

### Avis n° 2/2009 (WP160) 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.

Ce document doit être envisagé dans le contexte de l'initiative générale de la Commission européenne décrite dans sa communication «Vers une stratégie européenne sur les droits de l'enfant». En contribuant à cet objectif général, il cherche à renforcer le droit fondamental des enfants à la protection des données à caractère personnel. Ce sujet n'est pas totalement nouveau pour

[5] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf

[6] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf

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 n° 3/2003), sur l'utilisation des données de localisation (avis n° 5/2005) et sur les visas et les éléments d'identification biométrique (avis n° 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 (partie II) et en les illustrant par des références aux données scolaires (partie III).

Le domaine des données scolaires a été retenu parce qu'il s'agit de 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.

### L'avenir de la protection de la vie privée: contribution conjointe (WP 168) à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel

Le 9 juillet 2009, la Commission a lancé une consultation sur la révision du cadre juridique du droit fondamental à la protection des données à caractère personnel. Dans le cadre de sa consultation, la Commission a appelé à la communication d'avis sur les nouveaux défis de la protection des données à caractère personnel, notamment au regard des nouvelles technologies et de la mondialisation. Elle entend ainsi recueillir des éléments de réflexion pour déterminer si le cadre juridique actuel répond à ces défis et quelles mesures devraient être prises à l'avenir pour relever les défis identifiés. Le présent avis expose la réponse conjointe à cette consultation du groupe de travail «Article 29» (ci-après dénommé «groupe de travail 29») et du groupe de travail «Police et justice».

Le message central de cette contribution est que les principes essentiels de la protection des données, tels qu'entérinés dans la directive 95/45/CE, restent valables. Il est possible d'améliorer le niveau de protection des données dans l'UE grâce à une meilleure application des principes actuels de protection des données dans la pratique. Cela ne signifie pas pour autant qu'aucun changement législatif n'est nécessaire. Au contraire, il est utile de saisir cette occasion pour:

- préciser les modalités d'application de certaines règles et principes clés en matière de protection des données (tels que le consentement et la transparence);
- moderniser le cadre actuel, par l'ajout de nouveaux principes (tels que la «prise en compte du respect de la vie privée dès la conception» et la «responsabilité»);
- renforcer l'efficacité du système par la modernisation des dispositions de la directive 95/46/CE (par exemple en limitant la charge administrative);
- intégrer les principes fondamentaux de la protection des données dans un cadre juridique global, qui s'applique également à la coopération policière et judiciaire en matière pénale.

## 1.4. COMPTABILITÉ, AUDIT ET MATIÈRES FINANCIÈRES

### Contribution du groupe de travail «Article 29» (WP 164) à la consultation publique de la DG MARKT concernant le rapport du groupe d'experts sur les historiques de crédit

Le groupe de travail «Article 29» se félicite de l'occasion que lui a donnée la Commission européenne de commenter le rapport du groupe d'experts sur les historiques de crédit (GEHC), soumis à consultation publique. Le groupe de travail «Article 29» note que la Commission européenne a chargé le GEHC de rechercher les moyens d'optimiser la circulation des données sur les crédits à la consommation au sein de l'UE. Le groupe de travail prend acte qu'en exécutant son mandat, le GEHC a également tenu compte du droit au respect de la vie privée et d'autres considérations liées à la protection des consommateurs. À cet égard, le groupe de travail note avec satisfaction que le GEHC a décidé de ne recommander ni la création d'une base de données de crédit centralisée au niveau européen ni l'alignement de tous les États membres sur un modèle, existant ou à créer, de données de crédit.

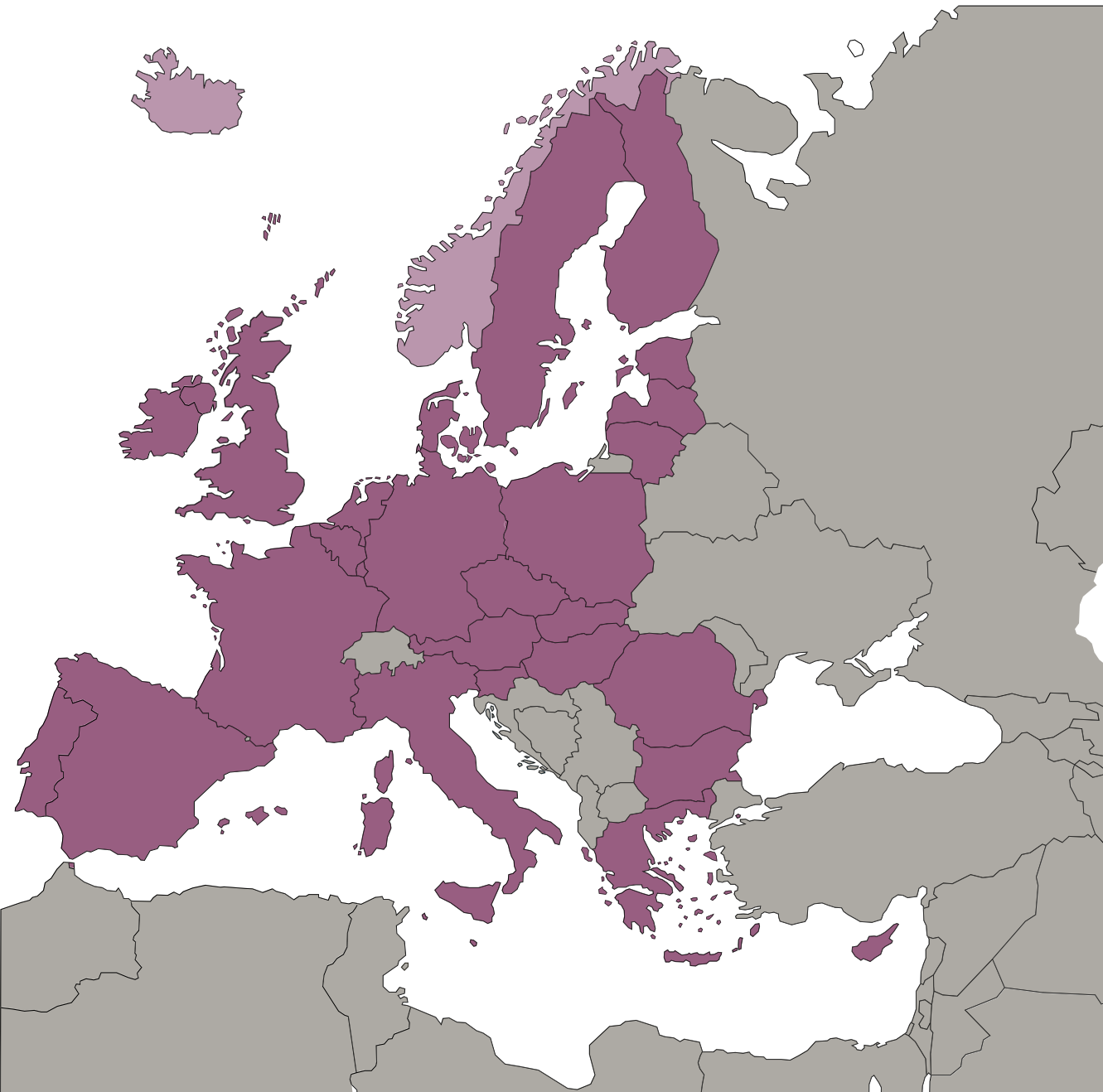
Le groupe de travail «Article 29» a souligné dans son avis que l'approche retenue par les autorités chargées de la protection des données de l'UE/de l'EEE est fondée sur la directive relative à la protection des données à caractère personnel (95/46/CE), ainsi que sur les législations nationales transposant cette directive dans l'ordre juridique des États membres. Le rapport du GEHC aborde des questions importantes, comme l'harmonisation des réglementations, l'organisation d'une table ronde et la coopération entre les autorités chargées de la protection des données. Le groupe de travail «Article 29» invite donc le groupe d'experts à adopter une position ferme et claire et à obtenir des engagements formels de toutes les parties concernées sur les sujets qui requièrent d'adopter des mesures réglementaires.

Les recommandations émises par le groupe d'experts dans son rapport reflètent principalement les préoccupations du secteur financier, étant donné que la majorité des membres de ce groupe représentent des institutions financières. Les membres du groupe de travail estiment donc que la présente contribution, ainsi que les observations des représentants des consommateurs sur le rapport du groupe d'experts, devraient également être prises en considération.

Le rapport appelle à une libéralisation plus poussée du traitement des profils de crédit privés. Dans la plupart des États membres, la tendance est de considérer ce traitement comme une forme de «mise sur liste noire» ou de fichage. La référence actuelle aux «législations locales sur la protection des données» (*local data protection laws*) n'est pas suffisante, en particulier du fait que bon nombre d'États membres n'ont pas (encore) adopté de dispositions détaillées et équilibrées concernant la protection des données à caractère personnel en matière de crédit. En outre, le rapport du groupe d'experts est améliorable en ce qui concerne les garanties précises et spécifiques à fournir par rapport aux règles en matière de protection des données.

# Chapitre 2

## Principaux développements dans les États membres



## Autriche

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

Le Parlement autrichien s'est ressaisi du projet de modification de la loi autrichienne sur la protection des données décrit dans le rapport 2008 et l'a adopté fin 2009 en tant qu'**amendement 2010 à la loi sur la protection des données personnelles**[7]. Ce nouveau projet de loi[8] ne reprend qu'une partie des thématiques abordées dans l'avant-projet de 2008. Les principales nouveautés concernent la réglementation de la vidéosurveillance, l'instauration d'une obligation d'information en cas de violation grave de la confidentialité des données et la simplification du processus de notification de l'utilisation qui est faite des données, par le passage à une procédure en ligne. En revanche, la proposition initiale de rendre juridiquement obligatoire le recours à des préposés à la protection des données n'a pas été retenue.

La commission autrichienne pour la protection des données fera rapport sur les détails de la nouvelle loi et ses répercussions dans le courant de l'année prochaine, eu égard au fait que celle-ci n'est entrée en vigueur que le 1er janvier 2010.

Un nouveau projet de loi visant à transposer la directive 2006/24/CE (**conservation des données**) dans le droit autrichien a été soumis pour avis fin 2009[9]. La commission autrichienne pour la protection des données a pris position et a souligné, une fois encore,[10] que dans le cas d'une telle restriction du droit fondamental à la protection des données personnelles, il convenait de définir, de manière précise et limitative, l'objectif poursuivi par le traitement des données, ce qui exige que l'on circonscrive clairement le concept d'«infraction grave».

Au cours de la période de référence, parmi les plaintes enregistrées, nombreuses étaient celles qui concernaient **l'évaluation de la solvabilité**, raison pour laquelle la commission pour la protection des données a réitéré à plusieurs reprises sa demande d'établir un cadre juridique concernant l'obtention, la fourniture et la réutilisation d'informations en matière de solvabilité, suite à quoi le ministère fédéral compétent s'est vu chargé de présenter un projet de loi en ce sens avant la fin de l'année 2010.

La commission pour la protection des données a également souligné la nécessité d'une intervention urgente du législateur dans un autre domaine : celui de l'échange de données entre prestataires de soins de santé (p. ex. établissements hospitaliers) et compagnies d'assurance-maladie privées. La commission pour la protection de la vie privée a, en collaboration avec les représentants des intéressés (assurés, assureurs, établissements de soins, professions médicales), réalisé une analyse approfondie de la situation et mis celle-ci à la disposition du ministère compétent en vue de l'élaboration d'un nouveau projet de loi.

### B. Jurisprudence

L'existence d'un droit à des **renseignements** sur les données collectées dans le cadre d'une **vidéosurveillance** a été réfutée dans le cas où

- la durée de conservation normale des enregistrements était de 48 heures,
- aucun événement justifiant de visionner lesdits enregistrements ne s'était produit, et
- il était pratiquement certain que d'autres personnes étaient concernées par l'enregistrement et qu'elles l'auraient donc aussi été par le visionnage des images.

Cette décision a été motivée par le fait que les droits de tiers - en l'occurrence, ceux des autres personnes filmées - à la protection de leurs données personnelles primaient, en l'espèce, sur l'intérêt pour le demandeur d'obtenir des renseignements, eu égard au fait que les données en question étaient de toute façon appelées à être effacées à très brève échéance, sans que personne n'en ait eu connaissance, puisqu'aucun événement ne justifiant que lesdites images soient visionnées (acte de vandalisme, agression, etc.) ne s'était produit[11].

[7] http://www.parlament.gv.at/PG/DE/XXIV/I/I_00472/pmh.shtml

[8] Le projet et tous les avis y afférents sont disponibles sur le site du Parlement autrichien, à l'adresse: http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00062/pmh.shtml

[9] http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00117/pmh.shtml

[10] http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00117_I3/imfname_178831.pdf

[11] http://www.ris.bka.gv.at/Dokumente/Dsk/DSKTE_20081205_K121385_0007-DSK_2008_00/DSKTE_20081205_K121385_0007-DSK_2008_00.pdf

Par ailleurs, la Cour constitutionnelle a dans l'intervalle confirmé que **la conservation de documents de procédure (judiciaire)** au-delà de la durée de la procédure est également autorisée lorsque le suspect est acquitté ou lorsqu'un terme est mis à la procédure. Et ce, en dépit du fait qu'il n'existe, outre le principe selon lequel les données ne peuvent être conservées qu'aussi longtemps qu'elles sont utilisées, aucune disposition juridique spécifique concernant la durée de conservation autorisée pour les documents de procédure. La raison essentielle de les conserver au terme de la procédure réside dans la possibilité de prouver que la personne a été acquittée ou que la procédure a été abandonnée, mais aussi dans la possibilité de vérifier la régularité de ladite procédure. Or, cette solution provisoire ne permet pas de remédier au risque d'une éventuelle utilisation abusive des données, en les employant à des fins autres que le but initial de l'enquête. Il faut pour cela des restrictions d'accès bien définies et sûres, qui soient également efficaces au niveau technique et organisationnel[12].

### C. Questions diverses importantes

**Vote électronique.** Du 18 au 22 mai, les étudiants autrichiens ont pu élire leurs représentants par vote électronique, au moyen de leur carte d'identité[13]. Le système de vote prévoyait un chiffrement strictement séparé des données d'identité du votant et du contenu de son vote. Ce n'est que lors du comptage des voix que les données d'identité des votants ont été déchiffrées au moyen de la clé privée du prestataire de services. Dans le cadre de cette procédure, toute voix émanant d'une personne qui n'avait pas le droit de voter a été supprimée de l'urne électronique. Les données d'identité ont ensuite été effacées du jeu de données. Les données de contenu (votes), toujours chiffrées (au moyen de la clé de la commission électorale), ont alors été mélangées et déchiffrées au moyen de la clé privée, puis comptabilisées par deux membres de la commission électorale. À aucun moment de la procédure, des noms n'ont été utilisés en guise de données d'identification. Seul un code personnel spécifique défini par la commission pour la protection des données sur la base du registre des votants l'a été. Ces codes ont été comparés aux codes personnels des étudiants dont les cartes d'identité ont été utilisées, afin de vérifier si les électeurs avaient bien le droit de vote.

[12] http://www.ris.bka.gv.at/Dokumente/Dsk/DSKTE_20090121_K121390_0001-DSK_2009_00/DSKTE_20090121_K121390_0001-DSK_2009_00.pdf

[13] http://www.oeh-wahl.gv.at

# Belgique

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

**Commission de contrôle flamande pour l'échange électronique de données administratives**

La Commission de contrôle flamande pour l'échange électronique de données administratives (*Vlaamse toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer* – ci-après dénommée la «Commission de contrôle» ou «CCF») autorise l'échange électronique de données à caractère personnel entre tous les départements de l'administration flamande, les provinces, les villes et les municipalités. En outre, elle conseille, sur demande ou de sa propre initiative, le Parlement flamand, le gouvernement flamand et d'autres autorités et parties prenantes. Dans certains cas, un responsable de la sécurité ne peut être désigné qu'après l'avis positif de la Commission de contrôle. La CCF soumet un rapport annuel au Parlement flamand. Les membres de la CCF ont été désignés par le Parlement lors de la réunion du 17 décembre 2009. La CCF a été instituée en vertu du décret flamand du 18 juillet 2008 *relatif à l'échange électronique de données administratives* (le «décret e-gov»). Le président de la CCF et deux de ses membres ont été désignés par la Commission de la protection de la vie privée (ci-après dénommée «la Commission» ou «la Commission belge»), tandis que trois autres membres ont été désignés par le Parlement flamand, assisté par un comité consultatif d'experts.

**Développements relatifs à la législation sur la surveillance par caméra (avis n° 24/2009 et 40/2008)**

Depuis l'entrée en vigueur de la loi *réglant l'installation et l'utilisation de caméras de surveillance* (ci-après dénommée la «loi caméras») le 10 juin 2007, la Commission a reçu plus de 6000 déclarations. Cette loi repose sur un principe important, à savoir que ce n'est pas chaque caméra qui doit faire l'objet d'une déclaration, mais plutôt chaque site sous surveillance. À la suite d'une série de problèmes pratiques rencontrés par les services de police en utilisant des caméras de surveillance mobiles, la Commission a été invitée en 2009 par la commission de l'Intérieur du Sénat à participer à l'évaluation de la loi «caméras». Cette activité parlementaire a accouché de la loi du 12 novembre 2009 *visant à modifier la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance* (Moniteur belge du 18 décembre 2009). Grâce à cette loi amendée, il suffit désormais de demander l'avis du conseil communal en question, qui, à son tour, doit consulter le chef de corps de la zone de police locale, tandis qu'il s'imposait également auparavant d'obtenir l'avis de ce dernier. La version modifiée de la loi «caméras» contient par ailleurs un nouveau chapitre établissant que les caméras de surveillance mobiles ne peuvent être utilisées par les services de police que dans le cadre de grands rassemblements et pour des missions non permanentes exclusivement, dont la durée d'exécution est limitée. Les caméras peuvent être utilisées soit dans des lieux ouverts (pendant une manifestation, par exemple), soit dans des lieux fermés accessibles au public (festival de rock, notamment).

L'arrêté royal du 21 août 2009 *portant modification de l'arrêté royal du 10 février 2008 définissant la manière de signaler l'existence d'une surveillance par caméra* (Moniteur belge du 25 septembre 2009) a également modifié les règles existantes concernant les dimensions des pictogrammes obligatoires signalant l'existence d'une surveillance par caméra.

## B. Jurisprudence

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

## C. Questions diverses importantes[14]

**Secteur public**

***Source authentique des données relatives aux véhicules (avis n° 06/2009)***

En 2009, la Commission a rendu un avis positif concernant l'avant-projet de loi *portant création de la source authentique des données relatives aux véhicules*, qui a pour but principal de réaliser la traçabilité des véhicules (via les propriétaires enregistrés qui y sont liés). Deux précédents rapports annuels de la Commission montrent que les deux avant-projets précédents avaient reçu un avis négatif (avis 42/2006 et 23/2008). Le nouvel

[14] Tous les avis, recommandations et autorisations de la Commission sont disponibles sur son site officiel à l'adresse: http://www.privacycommission.be.

avant-projet de loi intègre pratiquement toutes les observations de la Commission, ainsi que des améliorations substantielles, dont la désignation claire d'un responsable du traitement des données à caractère personnel et l'annexion d'une liste détaillée de finalités pour lesquelles les données de la source authentique peuvent être utilisées. Une liste de (catégories de) destinataires potentiels des données a été décrite de manière générale et la compétence d'autorisation du Comité sectoriel pour l'Autorité fédérale (institué au sein de la Commission et partiellement composé de membres de la Commission) a été reconnue. De plus, un vaste ensemble de compétences d'avis a été confié au même comité. Cependant, la Commission pointe aussi quelques possibilités d'amélioration. Ainsi, elle recommande de préciser explicitement dans l'avant-projet que les données des plaques d'immatriculation (de l'actuel registre des véhicules) feront partie de la source authentique. Elle recommande également de décrire plus en détail la manière dont le service de gestion pour le secteur[15] et toutes les sources de données (p. ex. les centres d'inspection automobile et les constructeurs) doivent se conformer à l'obligation d'informer les personnes concernées, ainsi que les mesures concrètes à prévoir pour désigner effectivement un responsable de la sécurité de l'information. La Commission recommande encore que chaque service ou source ayant accès aux données dénonce à la personne concernée, au comité sectoriel et au service de gestion les abus dont il aurait connaissance en matière de sécurité. Nouvelle en Belgique, cette obligation de dénoncer une fuite en matière de sécurité (ce qu'on appelle une «security breach notification») existe déjà dans les pays anglophones et sera également intégrée (en partie) à la modification prévue de la directive 2002/58/CE sur le commerce électronique.

***Autorisation unique pour l'accès au répertoire des marques d'immatriculation (Délibération AF n° 12/2009)***
Par le passé, la confusion régnait pour les gestionnaires privés de parking public quant à savoir comment collecter les rétributions, taxes ou redevances de stationnement; en témoignent différentes condamnations prononcées dans ce contexte. C'est pourquoi la Commission belge et le Comité sectoriel pour l'Autorité fédérale (supervisant la communication électronique de données à caractère personnel au sein de l'Autorité fédérale) ont toujours refusé d'accorder aux gestionnaires privés de parking l'accès à l'identité du titulaire du numéro de la marque d'immatriculation dans le répertoire de la DIV[16] (avis n° 37/2003 et délibération AF n° 02/2007). Une modification législative (loi du 22 décembre 2008 *portant des dispositions diverses*, titre 4, chapitre 2, Moniteur belge du 29 décembre 2008) a clarifié la situation et permet aux villes et communes, à leurs concessionnaires et aux régies autonomes communales de demander l'identité du titulaire du numéro de la marque d'immatriculation à la DIV. Il s'agit là d'une autorisation «unique», c'est-à-dire que dans l'autorisation, le Comité sectoriel décrit les conditions (strictes) que doivent respecter la DIV et les catégories de personnes ayant accès aux données, et ces dernières doivent signer une déclaration d'engagement aux termes de laquelle ils s'engagent à respecter ces conditions.

À des fins de plus grande transparence, toutes les autorisations uniques des Comités sectoriels de la Commission ainsi que les listes des personnes ayant accès aux données sont publiées (en français et en néerlandais) sur le site de la Commission, sous la rubrique «Décisions».

***Le traitement des données à caractère personnel dans le cadre de la politique antidopage (avis n° 30/2009)***
En 2009, à la demande du ministre compétent, la Commission a émis un avis relatif à un projet de standard international pour la protection de la vie privée et des renseignements personnels, élaboré par l'AMA (Agence mondiale antidopage). Ce standard international contient un minimum de règles communes qui doivent être respectées dans le cadre du traitement des renseignements personnels sur la base du Code mondial antidopage. La Commission a constaté que le standard international déroge à certaines garanties ancrées dans la législation belge pour la protection de la vie privée et a formulé quelques remarques concernant, par exemple, les motifs possibles de traitement de données à caractère personnel sensibles, le devoir d'informer les personnes concernées, les mesures de

[15] La Direction générale Mobilité et Sécurité routière du Service public fédéral belge Mobilité et Transports.

[16] Direction pour l'Immatriculation des Véhicules – le bureau fédéral belge chargé de l'immatriculation des véhicules et de leurs conducteurs.

sécurité et responsabilités, la durée de conservation des données à caractère personnel et l'exercice des droits des personnes concernées (droit d'accès, droit de rectification et droit d'opposition). La Commission a également souligné que les normes minimales décrites dans le standard international ne peuvent porter préjudice à la législation belge en matière de protection de la vie privée, qui est plus stricte.

En réponse à une demande d'information, la Commission a également remis un avis sur la réglementation flamande concernant le programme antidopage, et plus précisément sur l'obligation de communiquer les données de localisation des sportifs dans le cadre des contrôles antidopage hors compétition. Le décret flamand du 13 juillet 2007 *relatif à la pratique du sport dans le respect des impératifs de santé et d'éthique* et l'arrêté du gouvernement flamand du 28 juin 2008 le mettant en œuvre ne définissent pas quelles données de localisation doivent être communiquées par les athlètes de haut niveau. Ils font par contre référence au Code mondial antidopage, ce qui fait actuellement l'objet d'un recours devant le Conseil d'État. La Commission a néanmoins indiqué qu'exiger des données de localisation correspondant à quatre heures par jour est proportionné. Elle a émis des observations quant au statut des athlètes d'élite. Enfin, la Commission a formulé une série de remarques concernant les durées maximales de conservation des données et le devoir d'informer les personnes concernées.

*Base de données pour l'Office wallon de la formation professionnelle et de l'emploi (avis n° 18/2009)*

En 2009, la Commission a émis un avis positif sur le système «Jobpass» de l'Office wallon de la formation professionnelle et de l'emploi (ci-après «le Forem»). Le Forem est un organisme d'intérêt public wallon qui accomplit des missions en partenariat, conformément au contrat de gestion conclu entre le gouvernement wallon et le comité de gestion du Forem. D'une part, le système Jobpass délivre aux demandeurs d'emploi une carte à puce et, d'autre part, il met en œuvre une nouvelle base de données. L'objectif de la base de données et de la carte à puce est de faciliter pour le Forem et ses partenaires (p. ex. les centres de formation, qui ont uniquement accès aux renseignements nécessaires à l'exercice de leurs missions) l'identification des demandeurs d'emploi et l'échange d'informations à leur sujet. Le système facilite également l'échange de certaines informations avec l'Office national de l'emploi (via la Banque carrefour de la sécurité sociale) et aide les demandeurs d'emploi à apporter la preuve des démarches qu'ils effectuent pour trouver un emploi: grâce à sa carte à puce, le demandeur d'emploi peut enregistrer ses passages dans un organisme du Forem et de ses partenaires sans devoir passer par un conseiller. La Commission était d'avis que ces opérations de traitement des données étaient adéquates, pertinentes et non excessives. Elle a toutefois interdit la mention du numéro de registre national (qui figurait sur la partie sécurisée de la carte à puce) puisque le Comité sectoriel du registre national n'en avait pas donné l'autorisation.

**Secteur privé**

*Marketing direct (recommandation n° 04/2009)*

Au terme de la consultation de toutes les LVP européennes et sur la base de différentes demandes et plaintes reçues ces dernières années, la Commission a publié en 2008 une note juridique exprimant sa position par rapport aux pratiques de marketing direct. Soucieuse de proposer une analyse équilibrée, la Commission a ensuite entamé un dialogue avec les parties prenantes issues du monde des entreprises, des associations de consommateurs et du secteur universitaire afin de mieux cerner leurs intérêts, leurs priorités et leurs codes de conduite, le cas échéant. Enfin, la Commission, qui souhaitait entendre l'avis des citoyens, a publié une enquête publique sur son site internet. Ces efforts ont abouti à la recommandation n° 04/2009 sur le marketing direct et la protection des données à caractère personnel. Dans ce document, la Commission donne interprétation de la loi sur la vie privée en matière de marketing direct, recommande un certain nombre de méthodes en tant que meilleures pratiques (qui répondent à un traitement loyal et transparent des données à caractère personnel, que ces méthodes soient ou non requises par la loi) et formule à l'égard du législateur plusieurs améliorations souhaitables des dispositions existantes.

*Consentement*

La Commission est d'avis que le consentement libre, spécifique et informé de la personne concernée peut servir de base à la justification du marketing direct et le recommande par ailleurs à titre de meilleure pratique.

La recommandation fixe des conditions et énumère une série de cas dans lesquels le consentement de la personne concernée est indispensable (p.ex. en principe toujours lorsque le marketing direct est pratiqué par le biais de messages personnalisés par courrier électronique, fax ou système automatisé d'appel) ou plutôt inévitable (p.ex. commerce d'adresses et profilage).

*Intérêt légitime*
Bien que le maintien d'un équilibre soit loin d'être évident (en particulier pour le commerce d'adresses et de profils), la Commission reconnaît que ce principe est un fondement du traitement de données à caractère personnel dans le cas du marketing direct. La recommandation stipule le moment auquel l'équilibre des intérêts est évalué, les critères au moyen desquels l'équilibre est considéré et la manière dont l'équilibre des intérêts est sauvegardé. Si l'équilibre est rompu, le traitement doit être complètement interrompu.

*Délai de conservation*
Outre le devoir de rectifier les données inexactes, la Commission recommande aussi un délai de conservation pour les données à caractère personnel.

*Information*
La Commission souligne l'importance d'une information correcte, en particulier lorsque les données ne sont pas collectées directement auprès de la personne concernée. Dans ce cas, la Commission recommande fortement au responsable du traitement de communiquer de manière proactive la provenance des données à la personne concernée. Les acteurs du marketing direct ne peuvent invoquer une dispense de l'obligation d'information par la justification que celle-ci se révèle impossible ou implique des efforts disproportionnés, notamment parce que l'objet central du marketing direct est précisément le fait de rentrer en contact avec les personnes concernées.

*Opposition*
Enfin, la Commission mentionne que la personne concernée est libre d'utiliser son droit d'opposition sans la moindre justification. Cette opposition suffit à mettre fin au traitement des données. Elle établit encore que le droit d'opposition ne peut pas être entravé par des conditions que l'on y associe.

*Recommandation aux bailleurs et agents immobiliers relative au traitement des données des candidats locataires (recommandation n° 01/2009)*
Ces dernières années, des demandes d'informations ont été régulièrement introduites auprès du secrétariat de la Commission par des citoyens qui s'interrogent sur les contrats de bail et les données à caractère personnel que les propriétaires de biens offerts en location ou les agents immobiliers sont en droit de demander. Dans sa recommandation, la Commission stipule les données qui peuvent ou ne peuvent pas être demandées.

La Commission considère que des données telles que le nom, le prénom, l'adresse, le droit de séjour légal en Belgique et la date de naissance sont nécessaires à la conclusion d'un contrat de bail, mais qu'il est disproportionné de demander l'origine ethnique, le lieu de naissance et le numéro de registre national des candidats locataires. Quant à l'état civil, le numéro de téléphone et le numéro de plaque d'immatriculation, ils peuvent être pertinents ou pas selon les cas. Il est interdit, par exemple, de collecter le numéro de plaque d'immatriculation du locataire, sauf dans l'hypothèse où la location comprendrait une zone d'emplacement de parking dont l'accès ou le contrôle exige une reconnaissance du véhicule. À l'inverse, l'état civil n'est pas pertinent dans le cas d'un locataire qui sera le seul occupant du bien loué.

Les bailleurs doivent être en mesure de vérifier si les locataires sont suffisamment solvables pour s'acquitter du loyer mensuel. Il suffit pour cela de connaître leurs revenus réguliers, il est inutile de s'enquérir de leur situation financière globale. Cela signifie que s'il est justifié pour le candidat locataire d'avoir à montrer sa fiche de salaire (dont il pourra avoir rayé, s'il le préfère, l'identité de son employeur, sa profession et d'autres données sans intérêt), la remise d'une copie au bailleur ne se justifie pas, car il s'agit d'en tirer une simple appréciation de la solvabilité du candidat locataire. Il est cependant admis qu'un agent immobiliser conserve la preuve de la vérification des revenus des candidats locataires en réalisant une copie de la fiche de salaire. La consultation des données de la Centrale belge des crédits aux particuliers est réservée aux prêteurs et assimilés dans l'exercice de leurs missions.

Les bailleurs peuvent se renseigner sur les personnes qui occuperont le bien mis en location, par exemple le nombre d'occupants et leur âge approximatif. La loi sur la vie privée interdit de demander un extrait du casier judiciaire. Par ailleurs, la Commission n'autorise le traitement de données relatives à la santé qu'à la double condition que le locataire ait donné son consentement écrit, rétractable à tout moment, et que la donnée en question soit pertinente. Par exemple, un candidat locataire handicapé pourra être amené, pour obtenir la location d'un appartement adapté à ses besoins, à décrire son état de santé.

**Nouvelles technologies**

*Rétention de données (avis n° 20/2009)*

Dans le cadre de la transposition en droit belge de la directive européenne 2006/24/CE sur la conservation de données, la Commission a été priée d'émettre un avis relatif à un avant-projet de loi et à un projet d'arrêté royal relatif à l'obligation de collaboration. La directive a pour objectif d'harmoniser les obligations des fournisseurs de services en matière de conservation de certaines données, en vue de garantir la disponibilité pour les services autorisés de ces données à des fins de recherche, de détection et de poursuite d'infractions graves. La Commission a déjà remis deux avis négatifs dans ce contexte. En 2009 cependant, les avant-projets modifiés ont reçu un avis favorable, pour autant qu'il soit tenu compte des remarques formulées. Ainsi, la durée de conservation des données doit être réduite de 24 à 12 mois et cette disposition doit être stipulée dans l'avant-projet de loi. Le Parlement doit évaluer l'avant-projet de loi et le projet d'arrêté royal et le ministre compétent doit soumettre un rapport annuel au Parlement. Enfin, le rôle du service NTSU-CTIF[17], désigné pour accéder directement aux bases de données, doit être plus clairement défini. Plus concrètement, il convient de clarifier sa place dans la structure organisationnelle et le niveau de sécurité requis.

*Identification par radiofréquence (avis n° 27/2009)*

Cet avis, émis d'initiative, traite de l'utilisation des «tags» d'identification par radiofréquence RFID en vue du traitement de données à caractère personnel. Cette technologie permet de stocker et de lire à distance des informations contenues dans des puces implantées dans des objets ou des êtres vivants. La Commission fait la distinction entre deux situations dans lesquelles il peut être question d'un traitement de données à caractère personnel: d'une part le croisement de données personnelles avec un tag; d'autre part, le placement de données à caractère personnel sur un tag. Dans son avis, la Commission énumère les principes de la loi relative à la protection de la vie privée dont doit tenir compte le responsable du traitement. Ainsi, ce dernier doit veiller à la légitimité et à la proportionnalité du traitement envisagé. Si un traitement de données à caractère personnel est en principe possible lorsque les personnes concernées ont donné leur consentement, l'intérêt du responsable du traitement doit être confronté au droit à la protection de la vie privée des personnes concernées, par exemple au moyen d'une analyse de risque. La personne concernée doit également être suffisamment informée via une politique en matière de vie privée compréhensible, qui doit contenir au moins l'identité et l'adresse du responsable du traitement, le but du traitement, les données traitées (éventuellement si la localisation des tags sera ou non suivie), une synthèse de l'évaluation d'impact sur la vie privée et une analyse de risque. Enfin, la Commission souligne l'importance de mesures de sécurité techniques et organisationnelles adéquates.

[17] Le système central d'interception technique du service de police intégrée.



## Bulgarie

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

1. Lors de sa première réunion en 2009, la Commission pour la protection des données personnelles a adopté de nouvelles règles portant sur l'activité de la Commission pour la protection des données personnelles, lesquelles ont été promulguées dans le Journal officiel bulgare du 2 février 2009, abrogeant les règles portant sur l'activité de la Commission en vigueur depuis mars 2007.

   La nécessité d'élaborer et d'adopter les règles 2009 se justifiait par les nouvelles priorités adoptées par la Commission pour la protection des données personnelles en sa qualité d'autorité de contrôle indépendante en matière de traitement de données à caractère personnel. Cet acte juridique poursuit l'objectif de synchroniser l'activité des cellules administratives de la Commission en exerçant un contrôle général sur le respect de la loi sur la protection des données à caractère personnel et le traitement des données à caractère personnel. Grâce aux nouvelles dispositions, la Commission jouit d'une plus grande flexibilité pour adopter ses décisions, d'où une efficacité accrue de son fonctionnement global.

   Ces règles mettent en exergue les pouvoirs de la Commission spécifiés dans la loi sur la protection des données à caractère personnel et les mesures afférentes prises par la Commission. L'administration de la Commission a subi des changements structurels, lesquels ont consolidé les cellules assistant la Commission dans une activité particulière et, partant, l'activité d'expertise, au bénéfice de meilleurs résultats dans la mise en œuvre des pouvoirs de la Commission définis dans la législation.

2. La CPDP a préparé un avant-projet modifiant et complétant la loi sur la protection des données à caractère personnel (LPDP) et a organisé, en février 2009, des débats publics réunissant le président et les membres de la Commission de la sécurité interne et de l'ordre public à l'Assemblée nationale, des représentants d'organisations non gouvernementales, des cercles universitaires et des médias. Cependant, en raison des élections parlementaires de juin 2009, l'avant-projet de loi n'a pas été approuvé par la 40e Assemblée nationale. Le travail s'est poursuivi et les recommandations issues de la consultation publique ont été prises en considération.

3. Les représentants de la CPDP ont participé aux travaux du groupe de travail interdépartemental pour la préparation d'un avant-projet de loi modifiant et complétant la loi relative aux communications électroniques. Les modifications envisagées stipulent que la Commission pour la protection des données personnelles agira en qualité d'autorité de contrôle sur l'activité des entreprises fournissant des services et/ou réseaux de communications électroniques accessibles au public, afin de garantir le respect des règles de protection et de sécurité des données stockées conformément à l'art. 7 de la directive 2006/24/CE. La désignation de la Commission en tant qu'autorité de contrôle est conforme à l'obligation selon laquelle, en vertu de l'art. 9 de la directive 2006/24/CE, chaque État membre désigne une autorité publique qui est chargée de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de l'article 7 pour ce qui concerne la sécurité des données conservées. La directive 2006/24/CE stipule explicitement que cette autorité peut être la même que celle visée à l'article 28 de la directive 95/46/CE, à savoir la Commission pour la protection des données personnelles en Bulgarie.

4. En novembre 2009, le Conseil des ministres a adopté le Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, et a soumis au Parlement une proposition à ratifier. Ce qu'a fait le Parlement, et le Protocole a été promulgué au Journal officiel du 6 janvier 2010. La CPDP est l'autorité de contrôle en vertu de l'article premier, paragraphe 1, du Protocole additionnel.

### B. Jurisprudence importante

Le traitement de plaintes de personnes faisant état de violations spécifiques de leurs droits constitue une part

significative des activités de la Commission. Après analyse, il s'avère que les plaintes déposées à l'encontre des services répressifs centraux concernent principalement la communication de données à caractère personnel à des tiers ou la diffusion de telles données à l'insu de la personne concernée ou sans son consentement.

Un nombre conséquent de plaintes concerne également le refus d'accès aux données à caractère personnel, ainsi que la communication de données à caractère personnel à des tiers. La Commission pour la protection des données personnelles a formulé des instructions obligatoires relatives à l'accès aux données à caractère personnel, conformément aux demandes des plaignants, jugées fondées.

En 2009, la Commission pour la protection des données personnelles a été saisie de nouveaux cas relatifs à la diffusion de données à caractère personnel sur internet. Il a été établi que les données personnelles d'une certaine catégorie d'utilisateurs sont publiées sur des forums à des fins de support, dans le cadre de documents spécialisés, rapports, cours universitaires et analyses. Outre les violations de la loi relative au droit d'auteur et aux droits voisins, la Commission pour la protection des données personnelles considère que la diffusion de données à caractère personnel contredit le principe de proportionnalité et celui de la limitation des finalités du traitement des données personnelles en vertu de l'article 2, paragraphe 2, alinéas 2 et 3, de la loi sur la protection des données à caractère personnel.

En 2009, la Commission a rendu un avis concernant les demandes soumises tant par les responsables de traitement des données au titre de l'article 3 de la LPDP que par des particuliers soucieux du respect de leurs droits légaux. Des réponses ont été apportées aux questions relatives à la publication des données à caractère personnel de propriétaires, de représentants et de membres d'organes collectifs d'entreprises commerciales dans le registre du commerce, géré par l'agence bulgare chargée de l'enregistrement. En vertu de l'article 11 de la loi relative au registre de commerce, le registre est public. Tout un chacun est habilité à y accéder librement, de même qu'à la reproduction électronique des documents sur la base de laquelle des entrées, effacements et annonces ont été réalisés, ainsi qu'à la reproduction électronique des dossiers d'entrepreneurs réenregistrés. L'agence autorise également le libre accès aux demandes contenues dans le système d'information du registre de commerce, aux documents annexés et aux refus notifiés. Des renseignements tels que l'adresse du siège social, l'adresse d'exploitation et les représentants de l'entreprise, deviennent publics dès l'inscription de l'entreprise dans le registre. L'ordonnance n° 1 sur la gestion, la conservation et l'accès au registre de commerce spécifie les formulaires types des demandes d'enregistrement et indique explicitement les circonstances requérant un enregistrement, lesquelles doivent figurer dans les demandes d'enregistrement, d'effacement ou de publication. L'ordonnance régit les obligations légales en vertu desquelles l'agence chargée de l'enregistrement traite en toute légalité les données à caractère personnel d'une certaine catégorie d'individus.

La Commission a reçu des demandes concernant des cas où, au moment de procéder au paiement par carte de débit ou de crédit (les dénommés «instruments de paiement électronique», IPE), les employés de divers points de vente demandent aux clients de présenter leur pièce d'identité (carte d'identité) dans le but de contrôler leur identité. En vertu de l'article 31, paragraphe 5, de la loi relative aux systèmes de paiement, instruments de paiement électronique et transfert d'argent, le vendeur peut demander une pièce d'identité s'il peut raisonnablement douter de l'identité du détenteur de l'IPE.

Concernant l'application de l'article 64 de la loi relative au système judiciaire concernant la publicité et la transparence des activités et décisions des tribunaux et au sujet de la protection des droits individuels dans le cadre du traitement des données à caractère personnel, la Commission a rendu un avis recommandant d'entourer la création et la conservation d'un registre public des décisions de justice de certaines mesures visant à empêcher l'identification des individus. Outre l'emploi d'initiales au lieu du nom complet des personnes et la suppression des adresses et numéros privés, il s'impose également de supprimer toutes les indications liées à des caractéristiques physiques, physiologiques, génétiques, mentales, psychologiques, économiques, culturelles et sociales ou tout autre facteur pouvant contribuer à identifier l'individu en dépit de l'utilisation des initiales.

## C. Questions diverses importantes

Le 30 avril 2009, lors d'une session extraordinaire, la Commission pour la protection des données personnelles a intégré, dans le registre des responsables du traitement des données personnelles et dans les registres conservés par leurs soins, tous les responsables du traitement des données personnelles non enregistrés ayant introduit une demande entre 2003 et 2008. 193 351 responsables ont ainsi reçu un numéro d'identification. Dans ce contexte, la Commission a également fixé un délai dans lequel les responsables du traitement des données personnelles doivent mettre à jour les données soumises afin de proposer une base de données actualisée. L'obligation de mise à jour des circonstances dans les registres est une obligation permanente en vertu de la loi sur la protection des données à caractère personnel. Cette loi prévoit des sanctions en cas de traitement de données personnelles non enregistré et de mise à jour incomplète des informations figurant sur le formulaire d'enregistrement, qui doit être introduit dans le registre. La décision de la Commission de mettre à jour les informations jusqu'au 15 février 2010 vise à garantir la fiabilité des informations reprises dans le registre public, généralement accessible sur le site internet de l'institution. Les responsables du traitement des données personnelles peuvent actualiser leurs informations sur internet (même sans signature électronique), par voie postale ou directement avec la réception de la Commission.

# Chypre

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

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

(II) Lois modifiées

(III) Lois promulguées

## B. Jurisprudence importante

Suite à une question soumise par le chef de police au service juridique de la République de Chypre concernant la légalité d'une réglementation prévoyant la collecte des empreintes digitales d'étudiants provenant de pays tiers à leur arrivée à Chypre, le procureur général a conclu dans son avis que cette pratique ne semble pas être légale et a suggéré que le commissaire responsable de la protection des données personnelles examine la question plus en détail.

Après examen de tous les règlements législatifs pertinents en vigueur, le commissaire a rendu une décision concluant que cette réglementation spécifique ne constitue/fournit pas une base légale pour collecter les empreintes susmentionnées. Par la suite, une procédure imposant des sanctions administratives à la police a été lancée puis stoppée, le chef de la police ayant entretemps procédé, de sa propre initiative, à la destruction de la base de données des empreintes, conformément à l'avis et à la décision susmentionnés.

Suite à des articles parus dans la presse et à plusieurs appels téléphoniques de citoyens reçus par notre bureau concernant la pratique de l'autorité municipale des contractuels consistant à photographier les véhicules en stationnement interdit dont les propriétaires s'étaient vu infliger une amende, notre bureau a déclaré, en correspondance avec l'autorité municipale, que cette pratique enfreignait la législation en matière de protection des données.

Bien que l'autorité municipale ait mis fin à cette pratique, conformément à la position exprimée ci-dessus, elle a ensuite interjeté appel auprès de la Cour suprême. L'affaire est en instance.

## C. Questions diverses importantes

Suite à une proposition soumise par le commissaire en octobre 2009, le Conseil des ministres a adopté une décision obligeant tous les ministères et départements/services gouvernementaux à désigner des responsables de la protection des données, qui seront ultérieurement formés par les services de la Commission aux questions de protection des données internes.

Suite à plusieurs plaintes déposées auprès de nos services en 2003, le commissaire a remis un avis concluant que la pratique de la Garde nationale consistant à indiquer sur les documents de renvoi/suspension provisoire des soldats les raisons médicales (physiques ou mentales) ayant conduit à leur renvoi ou à la suspension provisoire de leurs obligations de service constituait une violation de la législation sur la protection des données.

La Garde nationale a mis fin à cette pratique conformément à l'avis précité. Cependant, en 2009, le ministre de la défense a publié un décret ordonnant à la Garde nationale de réinstaurer cette ancienne pratique, au motif que la délivrance des documents de renvoi/suspension provisoire de service est un acte administratif, qui oblige le corps administratif, en l'occurrence la Garde nationale, à communiquer par écrit aux soldats les raisons sous-tendant la décision de renvoi/suspension. Le commissaire étudie l'affaire avant de rendre sa décision.

L'association des banques chypriotes (ACB) a informé le commissaire de son intention de développer et mettre en place le système/base de données «ARTEMIS», qui serait exploité par une organisation privée placée sous l'autorité de l'ACB, en vue de permettre aux banques membres de l'ACB de partager les informations relatives aux débiteurs défaillants et d'évaluer le degré de solvabilité de clients potentiels.

L'ACB a soumis à notre service l'avant-projet du règlement interne de l'organisation en vue de la mise en place et de l'exploitation de ce système/base de données, qui

a été finalisé et adopté dans le respect des commentaires/recommandations du commissaire. Ce règlement est entré en vigueur et le système est opérationnel depuis novembre 2009.

Une compagnie privée qui envisage de lancer un service similaire à *Google Street View* a sollicité l'avis de nos services sur le sujet. Le service proposé implique de photographier l'ensemble des rues publiques de Chypre et de créer une carte virtuelle qui sera mise à la disposition des visiteurs sur internet. Ce service pourrait notamment être utilisé par les autorités municipales pour identifier les tronçons nécessitant des travaux routiers.

Compte tenu des documents pertinents adoptés par le groupe de travail «Article 29», nos services ont informé l'entreprise qu'en plus d'autres garanties, les photographies devront être floutées de manière à empêcher l'exposition des plaques d'immatriculation des véhicules et des visages humains. En outre, le service devra offrir aux personnes concernées un moyen aisé de déposer plainte concernant les données personnelles susceptibles d'être exposées. Nous examinons actuellement le service proposé.

## République tchèque

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

La réglementation générale en matière de protection des données à caractère personnel est la loi n° 101/2000 Coll. relative à la protection des données à caractère personnel et à la modification de certains actes connexes, entrée en vigueur le 1er juin 2000. L'Office pour la protection des données à caractère personnel («OPDP» ou «l'Office»), créé sur la base des dispositions de cette loi, est doté de pouvoirs importants. Organe indépendant, 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 commerciales 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».

La procédure de modification 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 en 2008.

Depuis le 1er avril 2009, date à laquelle la loi n° 52/2009 Coll. a intégré les définitions de nouvelles infractions à la loi sur la protection des données à caractère personnel, l'Office est tenu de poursuivre en justice toute violation de l'interdiction de publier des données à caractère personnel stipulée par d'autres réglementations légales. Cet amendement accompagnait la «loi muselière», une modification du Code pénal qui a fait suite à la publication répétée d'un grand nombre de données à caractère personnel issues de procédures pénales, la plupart du temps dans des quotidiens populaires et concernant des mineurs. L'Office a jugé positif que l'amendement dénonce plus particulièrement les dangers d'une publication sans restriction et d'une divulgation «en vrac» de données personnelles (y compris la publication dans les médias et sur internet). Malheureusement, le débat public entourant ce changement dans la procédure pénale, ou plutôt la campagne critique concentrée par la plupart des médias sur la suppression présumée de la liberté d'expression, a souvent oublié l'objectif initial de l'amendement, à savoir protéger la vie privée des personnes lésées dans des délits (les victimes).

La loi n° 111/2009 Coll. sur les registres de base impose à l'Office d'établir, au sein du tout nouveau système eGovernment, des identificateurs «source» et «agenda» des personnes physiques et d'organiser le transfert des identificateurs «agenda» des personnes physiques dans les agendas électroniques individuels. Les nouveaux identificateurs doivent, entre autres, réduire le risque de traitement non autorisé des données personnelles de citoyens conservées dans des registres de l'administration publique. L'Office a accepté cette compétence à la condition que la création et le transfert des identificateurs tendent à garantir une sécurité maximale et que l'ensemble du processus de génération des identificateurs soit strictement séparé de tout traitement effectif de données à caractère personnel par les autorités. Parallèlement, il ne peut en aucun cas être porté préjudice au contrôle actuel exercé par l'Office sur le traitement des données à caractère personnel au sein des registres existants de l'administration publique et des nouveaux registres de base proposés.

### B. Jurisprudence importante

En 2009, les travaux législatifs de l'Office ont traité de lois spécifiques ayant une incidence sur la protection de la vie privée et des données personnelles (le gouvernement doit impérativement consulter l'Office durant la procédure législative). Une attention particulière a été prêtée à la préparation de la nouvelle codification du droit civil, au travail sur les nouveaux registres électroniques de l'administration publique et aux réglementations liées aux registres de soins de santé. Les commentaires et objections de l'Office ont été partiellement suivis.

## C. Questions diverses importantes

Lors de l'application de la législation nationale et, par extension, de la législation de l'Union ou de la Communauté européenne, le ***travail de contrôle et de vérification***, y compris les inspections sur site, continue de jouer un rôle capital. Conformément à l'article 31 de la loi sur la protection des données à caractère personnel, les activités de contrôle de l'Office sont menées soit sur la base d'un plan d'activités de contrôle, soit sur la base de plaintes. Le plan d'activités de contrôle est élaboré de concert par le président et les inspecteurs de l'Office; il est contraignant et son exécution est régulièrement évaluée par le comité des inspecteurs, qui fait office de comité consultatif conjoint pour le président et les inspecteurs. La plupart des contrôles, y compris les inspections sur site, liés à des violations de la loi sur la protection des données à caractère personnel, ont été menés sur la base de plaintes et de requêtes d'individus (90 %), le reste des activités de contrôle résultant du plan de contrôle (8 %) et des instructions du président de l'Office (2 %). Notons cependant que ces deux dernières catégories d'inspections recouvrent généralement des procédures de contrôle plus complexes.

Le plan d'activités de contrôle pour 2009 était centré sur les thèmes suivants:
*Les systèmes d'information de l'administration publique* – le traitement de données à caractère personnel était un sujet fréquent de demandes de renseignement et de consultation (les contrôles s'intéressaient aux registres de la population).
*Les systèmes d'information multinationaux* – les contrôles étaient généralement initiés par les autorités de contrôle conjointes SIS et EURODAC et par d'autres initiatives de l'Union (c.-à-d. les données de trafic dans les systèmes de transport).
*Le traitement de données à caractère personnel dans le cadre de systèmes de surveillance par caméra* – l'autorité tchèque de protection des données (APD) applique les principes de base de la protection des données à caractère personnel tels que publiés dans la position officielle de l'APD.
*Les systèmes d'information dans la sphère de la justice* – l'APD tchèque s'est attelée au traitement de données personnelles dans le cadre d'activités incluant des sanctions administratives.

Lorsque le contrôle révélait une violation de la loi sur la protection des données personnelles, les parties en tort ont fait l'objet de poursuites administratives eu égard au traitement (illégal?) des données à caractère personnel. Dans ces cas, des amendes ont été imposées. Les parties jugées coupables peuvent interjeter appel de la décision auprès du président de l'Office.

Données statistiques relatives aux plaintes traitées en 2009:

| | |
|---|---|
| Total | 879 |
| dont: | |
| présenté en vue d'un contrôle | 129 |
| présenté en vue du lancement d'une procédure | 43 |
| transféré à d'autres instances compétentes | 24 |
| suspendu avec notification | 683 |

Les activités de contrôle précitées n'incluent pas celles qui concernent les ***communications commerciales non sollicitées*** («pourriel commercial»). En 2009, ce volet particulier comportait 2261 plaintes et autres requêtes, dont 1678 ont été traitées, avec 131 contrôles clôturés et 112 sanctions imposées.

En 2009, dans le cadre prioritaire des ***relations publiques et*** de ***la sensibilisation***, l'Office a poursuivi sa tradition d'organiser des conférences de presse équilibrées; cependant, la communication avec les médias se concentrait essentiellement sur la gestion quotidienne et la diffusion de sujets d'actualité sur le site web.

Le concours annuel destiné aux enfants et aux adolescents intitulé «C'est mon espace à moi, ne venez pas fouiner!» a à nouveau été organisé en 2009 et l'Office a constaté une plus grande participation et une évolution de la qualité. Les récompenses décernées aux lauréats ont comme de coutume été présentées dans le cadre du Festival international du film pour les enfants et la jeunesse de Zlín. Les contributions des enfants au concours ont été exposées à l'entrée de la salle de réunion du Sénat au début de la nouvelle année scolaire, ainsi qu'en plusieurs autres occasions.

L'année 2009 célébrait la troisième année de l'actuel programme de formation du corps enseignant mis en place par l'Office et portant sur la protection des données à caractère personnel dans l'enseignement dans

le cadre d'une accréditation de trois ans accordée par le ministère de l'éducation, de la jeunesse et des sports. Environ 200 enseignants ont participé à un atelier bénéficiant de l'expertise de l'Office.

L'Office a également jugé important de rencontrer les personnes âgées (en collaboration avec la troisième faculté de médecine de l'Université Charles), auxquels il s'impose d'expliquer régulièrement en quoi consiste la protection des données à caractère personnel, en plus de les sensibiliser à leur droit à la protection de la vie privée.

En automne 2009, le Sénat a organisé, sous les auspices de son vice-président, un atelier sur les profils ADN, articulé autour des conclusions des contrôles de l'Office. L'atelier a soulevé plusieurs questions qui requièrent une base législative précise.

## 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 dans le 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 (APD) 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 projets de lois. En 2008, l'APD a rendu un avis sur plusieurs lois et règlements ayant une incidence sur la vie privée et la protection des données.

En 2009, la loi danoise sur le traitement des données à caractère personnel a subi deux modifications:

- une nouvelle section 72 bis de la loi danoise sur le traitement des données à caractère personnel a été adoptée en vue de mettre en œuvre la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.
- une nouvelle sous-section 3 à la section 1 de la loi danoise sur le traitement des données à caractère personnel a été adoptée. Jusqu'en 2009, la loi danoise sur l'administration publique s'appliquait à l'échange manuel de données à caractère personnel entre des organes publics. Suite à cette modification, la loi danoise sur le traitement des données à caractère personnel s'applique désormais à la divulgation manuelle de données entre des organes publics.

### B. Jurisprudence importante

L'APD a été saisie de plusieurs cas impliquant les réseaux sociaux en ligne.

Ces derniers collectent un grand nombre de données personnelles des utilisateurs et possèdent également un grand nombre d'informations.

Les réseaux sociaux sont un domaine en évolution. De nouveaux enjeux en matière de protection des données à caractère personnel ne cessent d'apparaître parallèlement aux développements technologiques et aux nouveaux cadres de protection de la vie privée sur les sites des réseaux sociaux.

Au Danemark, Facebook a fait l'objet d'une vaste couverture médiatique et bon nombre de citoyens ont contacté l'APD à son sujet. Facebook affirme compter plus de deux millions d'utilisateurs danois.

L'APD a engagé un dialogue avec Facebook en avril 2009 et a soulevé une série de questions – en partie basées sur les demandes de renseignement formulées par les utilisateurs danois – concernant la politique de traitement des données à caractère personnel suivie par le réseau.

De plus, l'APD a appelé Facebook à fournir de plus amples informations sur le partage de données avec des tiers, intervenant à travers les différentes applications.

L'APD est toujours en dialogue avec Facebook. Le site web de l'agence fournit davantage d'informations et de conseils au sujet des réseaux sociaux, à l'adresse www.datatilsynet.dk. Les courriers envoyés par Facebook peuvent également y être consultés.

## C. Questions diverses importantes

**Vidéosurveillance en général**
En 2008 et 2009, l'APD a été saisie de plusieurs cas relatifs à la vidéosurveillance. Certains de ces cas concernaient des plaintes relatives à la divulgation injustifiée de données. D'autres concernaient des dossiers ouverts par l'APD à sa propre initiative, en raison, par exemple, de la couverture médiatique. La plupart de ces cas concernent la divulgation illégale, via internet ou dans la presse, de données de vidéosurveillance contenant des données personnelles.

En 2008 et 2009, l'APD a transmis à la police certains cas de violation des dispositions énumérées au chapitre 6 bis sur la vidéosurveillance de la loi danoise sur le traitement des données à caractère personnel.

Quelques-uns de ces cas ont été portés devant les tribunaux et, parmi ceux-ci, certaines réclamations ont été rejetées au terme de l'examen du fond de l'affaire par les juridictions. Dans d'autres cas de violation rapportés par l'APD, les entreprises inculpées ont accepté de se voir notifier une amende préétablie.

En 2009, l'APD n'a pas rencontré autant de cas que les années précédentes de violation du chapitre 6 bis de la loi danoise sur le traitement des données à caractère personnel méritant d'être signalés à la police. L'APD attribue cette situation à la couverture médiatique de certains cas antérieurs rapportés aux forces de l'ordre.

**Vidéosurveillance dans les taxis**
En 2009, l'Agence danoise de la sécurité routière et des transports a consulté l'APD concernant un avant-projet de décision du Parlement danois sur la vidéosurveillance dans les taxis. Les remarques de l'APD au sujet de cet avant-projet se montraient critiques à l'encontre de plusieurs points.

Plus tard dans l'année, l'APD a rendu un avis sur un projet de loi rendant obligatoire la vidéosurveillance dans les taxis. Ce projet de loi s'inspirait de l'avant-projet de décision du Parlement sur la vidéosurveillance dans les taxis, qui avait fait l'objet de remarques critiques de la part de l'APD, et cette dernière a également formulé une série de commentaires par rapport au projet de loi.

Le projet de loi introduit l'obligation d'installer un dispositif de vidéosurveillance dans les taxis en vue de contribuer à la résolution des faits de vol et d'attaque violente dont sont victimes les chauffeurs de taxi. Il contribuera en outre à prévenir et à résoudre les actes de vol et d'attaque violente commis sur les passagers.

Le projet de loi devrait être déposé au printemps 2010.



## Estonie

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

La directive 95/46/CE est transposée dans la loi estonienne sur la protection des données à caractère personnel (la version anglaise est disponible sur le site de l'Inspection à l'adresse http://www.aki.ee/eng/?part=html&id=105). La nouvelle version de la loi est entrée en vigueur le 1er janvier 2008. Depuis cette date, la législation sur la protection des données à caractère personnel n'a pas subi la moindre modification.

Les directives 2002/58/CE et 2006/24/CE sont mises en œuvre dans la loi sur les communications électroniques (dont la dernière traduction n'est pas encore disponible). L'obligation de collecter et de conserver les données de trafic a été promulguée en 2007. La rétention des données relatives à la téléphonie fixe en réseau et à la téléphonie mobile est entrée en vigueur le 1er janvier 2008, tandis que la conservation des données concernant l'accès à internet, les courriers électroniques via internet et la téléphonie sur internet est en vigueur depuis le 15 mars 2009. En conséquence, depuis 2009, tous les fournisseurs de services de télécommunications estoniens sont contraints de collecter les données de trafic, comme l'a démontré la procédure de contrôle conduite par l'Inspection.

### B. Jurisprudence importante

**Concernant les blogs et les réseaux sociaux**
L'Inspection estonienne de protection des données reçoit de nombreuses plaintes relatives à l'utilisation de données à caractère personnel sans consentement dans des blogs ou réseaux sociaux. Dans la plupart des cas, les requêtes concernent le retrait de photographies ou d'autres données personnelles. Dans le même temps, l'Inspection a dû tenir compte du fait que, dans certains cas, le motif de la plainte concernait un désaccord entre deux personnes, signifiant que les données ou photos avaient été publiées dans un esprit de vengeance. Malheureusement, sous l'effet de la sensibilisation accrue du public, ce genre de cas devient de plus en plus courant. L'Inspection est d'avis que ces matières doivent être portées devant les tribunaux civils et non devant l'autorité de protection des données.

Dans certains cas, l'Inspection interprète les blogs comme du «journalisme public», et donc soumis aux mêmes principes que le journalisme professionnel. La divulgation de données personnelles à des fins journalistiques est régie par la loi sur la protection des données à caractère personnel, comme suit:

*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 prédomine et conformément à l'éthique journalistique. La divulgation d'informations ne peut nuire de manière excessive aux droits de la personne concernée.*

*La personne concernée a le droit d'exiger, à tout moment, que la personne qui divulgue ses données personnelles en cesse la divulgation, sauf si cette divulgation a un fondement légal ou est conforme au principe susmentionné et pour autant que la poursuite de la divulgation ne nuise pas de manière excessive aux droits de la personne concernée. Une demande visant à mettre fin à la divulgation de données à caractère personnel ne sera pas adressée à la personne qui divulgue les données personnelles dans le cas de supports de données sur lesquels la personne qui divulgue les données personnelles n'a aucun contrôle au moment de la demande en question.*

**Concernant les caméras en ligne et la vidéosurveillance**
Au cours de l'année 2009, l'Inspection a mené des opérations de surveillance liées aux caméras en ligne. Elle a été saisie de cas où des caméras publiques en ligne sont configurées de telle manière qu'elles violent la vie privée des personnes (il est notamment possible d'orienter la caméra et de zoomer sur une habitation précise).

Par ailleurs, l'Inspection mène sur site des opérations majeures de contrôle de la vidéosurveillance dans le cadre d'un projet à long terme (par exemple, dans des grands magasins et sur les lieux de travail). Il en ressort pour l'instant que, dans certains cas, la simple notification ne suffit pas. La loi sur la protection des données à caractère personnel stipule que:

*Un équipement de surveillance transmettant ou enregistrant des données personnelles peut être utilisé pour la protection de personnes ou de biens uniquement s'il ne porte pas atteinte de manière excessive aux intérêts légitimes de la personne ou du bien concernés et si les données collectées sont utilisées aux fins exclusives de l'objet de leur collecte. Le cas échéant, le consentement de la personne concernée est remplacé par une communication suffisamment claire de l'utilisation de l'équipement de surveillance et/ou le nom et les coordonnées du responsable du traitement des données. Cette exigence ne s'étend pas à l'utilisation d'équipements de surveillance par les agences gouvernementales, en vertu de et conformément à la procédure légale.*

## C. Questions diverses importantes

Pour la troisième année consécutive, l'Inspection a défini des priorités et publié des lignes directrices sur ces matières. Les lignes directrices pour l'année 2009 sont uniquement disponibles en estonien:

- le traitement de données à caractère personnel dans le cadre de campagnes électorales - http://www.aki.ee/download/1101/erakondadekampaaniad_200309%20(2).rtf
- le traitement de données à caractère personnel par les autorités financières - http://www.aki.ee/download/1037/AKI%20krediidiasutuste%20juhend.pdf
- le traitement de données à caractère personnel dans le cadre de la recherche généalogique - http://www.aki.ee/download/1404/Isikuandmete%20töötlemine%20suguvõsa%20uurimiseks%20171109.rtf
- le traitement de données à caractère personnel dans le cadre de la recherche scientifique - http://www.aki.ee/download/1469/Isikuandmete%20töötlemine%20teadusuuringus.rtf
- l'utilisation des numéros d'identité nationale - http://www.aki.ee/download/1102/Isikukoodi%20kasutamise%20juhis.rtf
- la divulgation de données à caractère personnel de débiteurs des entreprises de service public - http://www.aki.ee/download/1240/JUHIS%20%20Korterivõlglaste%20avaldamine%20090309.rtf
- le droit des personnes de demander les données les concernant - http://www.aki.ee/download/1045/kusi_oma_andmeid_090309.rtf

En outre, nous avons élaboré des directives à l'intention des détenteurs d'informations publiques. Ces directives concernent, entre autres, la tenue des registres de documents et la divulgation de données sur les sites web des autorités publiques. Les directives sont disponibles en estonien à l'adresse http://www.aki.ee/est/?part=html&id=125.

## 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 des données à caractère personnel et à la libre circulation de ces données a été transposée dans le 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 au sujet du processus décisionnel de la Commission et de la force exécutoire de ses décisions concernant le 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 régie 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 chargé de 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 chargé de 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 à caractère personnel (523/1999).

La modification de la loi sur la protection de la vie privée dans les communications électroniques est entrée en vigueur le 1er juin 2009. Elle autorise l'opérateur de l'abonné à procéder au traitement des données d'identification dans le but de prévenir et de détecter l'utilisation illégale de services de la société de l'information payants, de réseaux ou services de communications, ou le recours à l'espionnage industriel, tel que stipulé dans le Code pénal (*Rikoslaki* 39/1889).

L'utilisation illégale d'un réseau ou service de communications peut consister, par exemple, en l'installation d'un dispositif, logiciel ou service sur le réseau de communications de l'opérateur de l'abonné, offrant à un tiers un accès illégal au réseau ou service de communications de l'opérateur de l'abonné, ou toute utilisation comparable du réseau ou service de communications qui transgresse les instructions d'emploi.

Le droit précité ne s'applique pas aux données d'identification de services de téléphonie fixe ou mobile en réseau.

Les modifications requises par ce que l'on appelle la «LexNokia» ont été intégrées aux sections 2 et 21 de la loi sur la protection de la vie privée dans la vie professionnelle (*Laki yksityisyyden suojasta työelämässä* 759/2004), avec prise d'effet le 1er juin 2009.

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). L'obligation légale de conserver les données d'identification de télécommunications est entrée en vigueur le 15 mars 2009.

En 2006, le Parlement finlandais a prié le gouvernement de s'atteler à la préparation de 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 commencera plus tard. Toutefois, la loi relative à l'authentification électronique forte et aux signatures électroniques (*Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista* 617/2009) est entrée en vigueur le 1er septembre 2009. Elle fixe des obligations de qualité strictes aux fournisseurs de services d'identification. La loi permet aussi d'utiliser l'identification biométrique en guise d'authentification forte.

## B. Jurisprudence importante

Le 16 décembre 2008, la Cour de justice de l'Union européenne (grande chambre) a rendu son arrêt sur la publication de données relatives aux revenus du travail. Cette affaire avait trait au champ d'application de la directive 95/46/CE, au traitement et à la circulation des données fiscales à caractère personnel, à la protection des personnes physiques et à la liberté d'expression. La Cour a laissé à une juridiction nationale le soin 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 de listes ou services déjà publiés**.** La Cour administrative suprême a rendu son jugement le 23 septembre 2009 (KHO:2009:82). Elle a renvoyé l'affaire devant la commission de protection des données, obligeant cette dernière à interdire à Satamedia de continuer à publier les données. Cette interdiction concernait tant les publications que le service SMS. Dans son jugement, la Cour a déclaré que l'article 2.4 de la loi finlandaise sur la protection des données à caractère personnel n'est pas conforme à l'interprétation que fait la Cour de justice de l'UE du champ d'application de la directive. Pour prendre sa décision, la Cour a veillé à l'équilibre entre liberté d'expression et protection de la vie privée. Elle a souligné que cet équilibre nécessite, pour ce qui est de la liberté d'expression, que les informations communiquées au public revêtent une importance pour la société et ne servent pas uniquement à assouvir la curiosité. Quant à déterminer si le traitement était ou non effectué à des fins de journalisme, la Cour s'est focalisée sur la manière dont ces «journaux» ont été réellement produits. Dans la mesure où la base de données (registre) a été imprimée en tant que telle, elle ne pouvait avoir été créée à des seules fins journalistiques. La Cour a décidé qu'aucune base légale ne justifiait le traitement de données à caractère personnel par Veropörssi et que, par conséquent, le service de SMS était également illégal. La Cour n'a pas abordé les questions des données fiscales en tant que telles, ni celle de l'équilibre entre liberté d'expression et vie privée. Le fournisseur du service SMS a fait savoir à l'APD le 28 septembre 2009 qu'il mettrait fin au service le 30 septembre 2009 en raison de son caractère illégal manifeste. Dans la pratique, les journaux finlandais publieront aussi à l'avenir ce type de données à caractère personnel au sujet de personnes susceptibles d'occuper une place importante dans la société.

De futurs amendements à la loi finlandaise sur les données à caractère personnel concernant l'incohérence de l'article 2.4 seront préparés par le ministère de la justice, qui a récemment publié un futur plan de travail incluant notamment une mise à jour de la loi sur les données personnelles.

Dans sa décision du 26 novembre 2009, la commission de protection des données a interdit à la société Satakunnan Markkinapörssi Oy de traiter les données relatives aux revenus du travail et du capital ainsi qu'au patrimoine de personnes physiques selon la méthode suivie pour les dossiers fiscaux de 2001 et avec la même ampleur. En outre, la commission de protection des données a interdit à Satakunnan Markkinapörssi de diffuser, via un service SMS ou à toute autre fin, les données relatives aux revenus du travail et du capital ainsi qu'au patrimoine de personnes physiques collectées et conservées par ses soins. La commission a également interdit à Satamedia Oy, en raison de la violation de la loi sur les données à caractère personnel (*Henkilötietolaki* 523/1999), de collecter, de conserver et de diffuser d'autres données relatives aux revenus du travail et du capital ainsi qu'au patrimoine de contribuables issues du registre de Satakunnan Markkinapörssi Oy et publiées dans un journal intitulé *Veropörssi*. Selon des informations reçues de la Cour administrative d'Helsinki, il a été interjeté appel

contre la décision (communiquée le 12 janvier 2010) de la commission de protection des données. L'entreprise ayant changé de domicile, l'affaire a été transférée à la Cour administrative de Turku.

La commission de protection des données a tranché dans le dossier ouvert par le bureau du médiateur chargé de la protection des données quant à l'authentification des demandeurs de crédits rapides par téléphone mobile. Dans sa décision, la commission de 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, la commission a interdit au défendeur, qui suivait un processus d'authentification couramment utilisé dans le secteur, de traiter les données personnelles de la manière susmentionnée. Le défendeur a introduit un recours contre la décision de la commission de protection des données devant la Cour d'appel compétente. Suite à cette affaire notamment, une proposition visant à adopter une loi générale sur l'authentification a été déposée en Finlande. La réforme générale de la législation sur le crédit à la consommation a été mise en œuvre avec l'amendement du chapitre 7 de la loi sur la protection des consommateurs (***Kuluttajansuojalaki*** 38/1978), entré en vigueur le 1er février 2010.

## 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.

À titre d'exemple du principe de responsabilité, plusieurs lois spéciales imposent de produire un bilan en matière de données. Ainsi, conformément à la sous-section 1 de la section 2 du décret du gouvernement sur l'agence pour les TIC (HALTIK) (*Valtioneuvoston asetus Hallinnon tietotekniikkakeskuksesta* 810/2007), cette dernière doit soumettre pour fin avril un rapport annuel sur les questions significatives relatives au traitement de données dans le cadre de son mandat au ministère de l'intérieur ainsi qu'au bureau du médiateur chargé de la protection des données. Le décret est entré en vigueur le 1er mars 2008.

Conformément à la section 60 de la loi sur le système d'information de la population et les services d'identification du Centre du registre de la population (*Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista* 661/2009), le Centre du registre de la population doit fournir, au moins une fois par an, un rapport détaillé sur le traitement des données et événements conservés dans le registre. La loi est entrée en vigueur le 1er mars 2010.

*Études réalisées*

Au cours de l'année de référence, le bureau du médiateur chargé de la protection des données a réalisé plusieurs études.

Durant l'été 2009, le bureau du médiateur chargé de la protection des données a procédé à une étude sectorielle relative aux enquêtes d'opinion et de marché. Les questionnaires envoyés à une centaine d'entreprises ont permis de répertorier les différentes procédures suivies en matière de sondages et de montrer l'ampleur prise par le traitement des données personnelles. Le respect des droits civils a fait l'objet d'une attention particulière. L'étude sectorielle a révélé que certains des auteurs d'enquêtes d'opinion et de marché connaissent les exigences de la législation sur la protection des données et en tiennent compte dans leurs activités. Toutefois, certaines réponses traduisent un manque de connaissances concernant les exigences en matière de protection des données. Le nom et les coordonnées de contact des citoyens sont obtenus à des fins de recherche, surtout par le biais de services de répertoire électronique et de demande de renseignements, ainsi que via les registres officiels.

Le bureau du médiateur chargé de la protection des données a mené une vaste opération de contrôle, concentrée sur le registre national du Centre pour l'emploi et le développement économique. Le Centre

possède 200 agences à travers la Finlande. Les clients bénéficient de services liés à la recherche d'emploi, à la planification de carrière, à la réadaptation professionnelle et à l'entrepreneuriat. Le Centre pour l'emploi et le développement économique fournit également des conseils concernant les demandes d'allocations de chômage et soutient de diverses manières l'accès à l'emploi. Le contrôle visait à vérifier que le traitement des données à caractère personnel dans le registre national respecte la législation en vigueur. Les conclusions de l'inspection ont été soumises au ministère de l'emploi et de l'économie, qui a ensuite adopté plusieurs amendements et mesures sur cette base.

Étant donné que la commission finlandaise de protection des données peut accorder une autorisation de traitement des données à caractère personnel et fixer des conditions spéciales en la matière, le bureau du médiateur chargé de la protection des données a réalisé une étude afin de voir dans quelle mesure les bénéficiaires de ces autorisations respectent les décisions et se plient aux conditions. Selon les résultats de l'étude, les conditions d'autorisation sont bien respectées.



## 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 en le 20 octobre 2005. Il a fait l'objet d'une modification le 25 mars 2007 en vue d'apporter les modifications procédurales nécessaires.

### B. Jurisprudence

**Arrêt de la Cour de Cassation du 8 décembre 2009 relatif aux alertes professionnelles**
Dans un arrêt du 8 décembre 2009, la chambre sociale de la Cour de cassation rappelle que les alertes professionnelles autorisées par la CNIL dans le cadre de l'autorisation unique n° 4 doivent avoir un champ d'application limité.

Cette décision ne remet pas en cause le principe même des dispositifs d'alerte et vient clarifier les difficultés d'interprétation rencontrées par les tribunaux.

Afin de se conformer aux exigences de la loi américaine dite «Sarbanes Oxley» , la société Dassault Systèmes a mis en place un «code de conduite des affaires» énumérant les règles que les salariés s'engagent à respecter dans l'exercice de leur activité professionnelle. Ce code instaure notamment un dispositif d'alerte professionnelle permettant aux salariés de signaler tout manquement via une adresse électronique dédiée. Préalablement à la mise en place du dispositif, la société Dassault Système a effectué une déclaration de conformité à l'autorisation unique n° 4.

À l'occasion du contentieux né de ce système d'alerte, la Cour de cassation rappelle que le champ d'application de l'autorisation unique doit être limité. Elle indique clairement que la mise en œuvre d'un dispositif d'alerte professionnelle, faisant l'objet d'un engagement de conformité à l'autorisation unique, doit se limiter aux seuls domaines comptables, financiers, et de lutte contre la corruption.

En effet, la CNIL avait prévu, à l'article 3 de son autorisation unique n° 4, la prise en compte de faits ne relevant pas de ce champ d'application mais mettant en jeu «l'intérêt vital de l'organisme ou l'intégrité physique ou morale de ses employés». La Cour de cassation précise que cet article ne doit pas être interprété comme permettant un élargissement de la finalité des dispositifs d'alertes tels que prévus par l'autorisation unique. Les systèmes d'alertes qui ne répondent pas strictement aux conditions de l'autorisation unique n° 4 doivent faire l'objet d'une autorisation spécifique accordée au cas par cas par la CNIL.

Par ailleurs, la cour de cassation souligne la nécessité pour les entreprises d'informer les personnes concernées conformément aux dispositions de la loi «Informatique et Libertés». Sur ce point, l'arrêt rappelle que «les mesures d'information prévues par la loi du 6 janvier 1978 reprises par la décision d'autorisation unique (…) doivent être énoncées dans l'acte instituant la procédure d'alerte». En effet, dans l'affaire Dassault, cette information était incomplète s'agissant des droits d'accès, de rectification et d'opposition.

La CNIL devrait prochainement modifier son autorisation unique à la lumière de l'arrêt rendu par la Haute juridiction et des constats opérés lors des contrôles récemment menés auprès d'entreprises.

### C. Fonctionnement et activités de la CNIL

**L'adoption des délibérations**
Au cours de l'exercice 2009, la CNIL a siégé 48 fois au cours de 35 séances plénières et 13 formations contentieuses.

Ces réunions ont conduit à l'adoption de **719** délibérations, soit une progression de 22,7 % par rapport à l'exercice 2008.

La CNIL a adopté en 2009 :
- **544** autorisations (**+39 %** par rapport à 2007;
- **5** refus d'autorisation;
- **35** avis sur des traitements de données sensibles ou à risques.

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 2009, la CNIL a prononcé:
- 5 sanctions pécuniaires;
- 4 avertissements;
- 90 mises en demeure.

**Les saisines**
**La CNIL a fait l'objet de 6482 saisines en 2009**
En 2009, la CNIL a été saisie de 4 265 plaintes pour non-respect de la loi « informatique et libertés » et 2217 demandes de droit d'accès indirect, soit un nombre en légère diminution (-11,8 %) par rapport à 2008 (2 516 demandes).

Les déclarations de fichiers connaissent une légère diminution en 2009 puisqu'elles s'élèvent à 68 185 contre 71 990 en 2008, soit une baisse de l'ordre de **5 %**.

**Les contrôles**
2009 aura confirmé l'importance croissante des contrôles dans les missions de la CNIL, tant au regard du nombre de contrôles effectués, que des secteurs contrôlés de plus en plus variés. La CNIL a mis en place de nouvelles procédures pour faire suite aux évolutions jurisprudentielles concernant son activité.

Les chiffres, d'abord. **270 contrôles** ont été effectués en 2009, soit **une augmentation de près de 24 %**. L'augmentation soutenue du nombre de contrôles réalisés n'est pas un phénomène nouveau et témoigne de la volonté de la CNIL de s'inscrire pleinement dans la philosophie de la loi de 2004 qui privilégie le contrôle sur place des fichiers, au bénéfice des personnes dont les données sont traitées.

La première source des contrôles opérés s'inscrit dans **la mise en œuvre du programme annuel** des contrôles (31 % des contrôles effectués) adopté par la formation plénière. Le programme 2009 des contrôles aura été très largement respecté.

**Les temps forts de l'activité 2009**
**a. La CNIL à l'âge de la maturité**
L'année 2009 a été marquée par plusieurs initiatives parlementaires visant à réviser la loi informatique et libertés.

Il convient de mentionner plus particulièrement le fait que, fin 2008, la commission des lois du Sénat a confié aux sénateurs Anne-Marie Escoffier et Yves Détraigne **une réflexion sur le respect de la vie privée à l'heure des mémoires numériques**.

Les recommandations qu'ils ont formulées dans leur rapport d'information ont été traduites pour partie dans une proposition de loi examinée par le Sénat en mars 2010. Cette proposition de loi envisage, tout d'abord, de donner une plus grande effectivité au droit à l'oubli numérique, en renforçant l'obligation d'information sur la durée de conservation des données et en facilitant l'exercice du droit de suppression notamment sur internet. Sur ce sujet, la Secrétaire d'État à la prospective et au développement de l'économie numérique, Nathalie Kosciusko-Morizet, a par ailleurs lancé, en novembre 2009, une large consultation publique sur le droit à l'oubli numérique, dont l'objectif est notamment d'identifier les bonnes pratiques et rédiger une charte d'engagement pour leur mise en œuvre.

En outre, la proposition de loi vise à rendre obligatoires les correspondants « informatique et libertés » lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel et que plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en œuvre.

Il s'agirait, de plus, de conforter les pouvoirs de contrôle et de sanction de la CNIL, ainsi que de renforcer ses possibilités d'actions devant les juridictions. Enfin, le texte présenté au Parlement a également pour objet, entres autres, de préciser les obligations incombant au responsable de traitement en cas violation de l'intégrité ou de la confidentialité des données personnelles ou encore de modifier le régime d'encadrement des fichiers de police.

**i. La stratégie d'ouverture**

*Le défenseur des droits*

Le Défenseur des droits, institué par la révision constitutionnelle du 23 juillet 2008, va devenir membre de la CNIL. Il pourra participer, personnellement ou en désignant un représentant, au Collège de la Commission, mais avec une voix consultative (article 9 du projet de loi organique). La CNIL comprendra donc 18 commissaires.

Le Président de la CNIL se réjouit l'arrivée prochaine du Défenseur à la CNIL, qui fera progresser encore la protection des droits et libertés de nos concitoyens.

*Multiplication des auditions et ouverture à l'international*

Dans un souci d'ouverture vers l'extérieur et de compréhension des projets du gouvernement, des technologies/offres de services actuellement en cours de développement et/ou des problématiques actuelles et futures, la CNIL a organisé plus de 20 auditions lors de ses séances plénières en 2009.

Ont notamment été auditionnés des membres du gouvernement, à savoir: Nathalie Kosciuzko-Morizet, secrétaire d'État à la prospective et au développement de l'économie numérique et Eric Besson, ministre de l'Immigration, de l'intégration, de l'Identité nationale et du Développement solidaire. Des sociétés telles que St Gobain, PSA, Air France, IBM ont également été entendues par la CNIL.

En outre dans le cadre de séances plénières dédiées exclusivement aux sujets internationaux, le Président de la Federal Trade Commission américaine a été reçu par la CNIL en octobre 2009. De surcroit, dans le cadre de la coopération internationale, la CNIL accueille régulièrement des délégations étrangères du monde entier en mission d'étude en France et/ou en Europe pour échanger sur son expérience en matière de protection des données personnelles ainsi que sur l'organisation et les pouvoirs de son autorité de contrôle. Ainsi, en 2009, la CNIL a donc eu le plaisir d'accueillir des délégations de Chine, de Russie (à deux reprises), d'Indonésie, d'Arménie, et enfin de Turquie afin d'échanger sur des problématiques notamment de signature électronique, de fichiers de police, d'accès à l'information, de cybercriminalité et d'administration électronique.

Enfin, en 2009, le Président de la CNIL s'est pleinement engagé, notamment au travers de l'AFAPDP (Association Francophone des Autorités de Protection des Données Personnelles), pour initier et consolider les actions favorisant cette dynamique positive. L'AFAPDP a notamment organisé, grâce au soutien de l'Organisation internationale de la Francophonie, la 3e Conférence francophone annuelle des commissaires à la protection des données personnelles, qui s'est tenue à Madrid en novembre 2009. Cette Conférence a offert une tribune unique aux 30 délégations représentant des pays francophones et des organismes internationaux et a permis notamment de sensibiliser et partager des expériences avec les États francophones dépourvus, pour le moment, de législation sur la protection des données personnelles, mais également d'initier la mise en place d'un partenariat avec le réseau ibéro-américain de protection des données.

**ii. Une plus grande transparence**

La CNIL n'était, jusqu'à présent, pas autorisée à communiquer ses avis sur les projets de loi.

En effet, la CADA (Commission d'Accès aux Documents Administratifs) considérait que la CNIL ne pouvait communiquer un avis au public «aussi longtemps qu'il revêtait un caractère préparatoire, c'est-à-dire aussi longtemps que le projet de loi, d'ordonnance ou de décret auquel il se rapportait n'avait pas été adopté». Même lorsqu'il avait perdu son caractère préparatoire, l'avis de la Commission se rapportant à « des dossiers examinés en conseil des ministres, c'est-à-dire les projets de loi, projets d'ordonnance et de décrets », n'était pas communicable. Dès lors, les parlementaires se trouvaient dans une situation paradoxale : ils étaient amenés à débattre de questions examinées par la CNIL, mais ne pouvaient disposer de son avis, dont ils connaissaient pourtant l'existence.

*L'exemple d'HADOPI*

Un quotidien économique a publié, le 3 novembre 2008, l'avis de la CNIL du 29 avril 2008 sur l'avant-projet de loi HADOPI, en dehors de tout cadre juridique légal et alors même que notre Commission n'était pas autorisée à le communiquer. Cette publication a ainsi fait connaître la position de la CNIL sur le projet de texte, dans sa version originelle. Après cet avis, le texte a profondément été remanié par le Parlement. Par exemple,

dans l'avant-projet de loi, l'HADOPI pouvait conduire les fournisseurs d'accès à filtrer les contenus, ce qui présentait un risque d'atteinte à la liberté d'expression, que la CNIL avait souligné. Or, dans le texte soumis aux assemblées, il était prévu que seule l'autorité judiciaire pouvait ordonner aux fournisseurs d'accès de procéder au filtrage des contenus.

Cette situation, qui obligeait la CNIL à être silencieuse sur ses propres avis et qui en privait le Parlement, est désormais révolue. En effet, la loi du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures, issue de l'initiative de M. Jean-Luc Warsmann, Président de la Commission des Lois de l'Assemblée nationale, prévoit désormais que: «**À la demande du Président de l'une des commissions permanentes du Parlement, l'avis de la commission sur tout projet de loi est rendu public**».

La récente évolution législative constitue donc une avancée majeure au regard de la transparence de l'activité de la Commission et permettra d'améliorer la qualité des travaux parlementaires.

### iii. LA CNIL a accueilli de nouveaux membres en février 2009

Jean-Paul Amoudry, Sénateur (UC) de la Haute-Savoie
Jean-François Carrez, Président de chambre à la Cour des comptes
Claire Daval, Avocat, Maître de conférences de droit public à l'Université de Lille 2
Marie-Hélène Mitjavile, Conseiller d'État
Dominique Richard, Consultant

## b. L'expertise technologique

La CNIL accompagne les entreprises et les pouvoirs publics dès la conception de leurs systèmes. À travers son rôle de conseil et lors de l'examen des dossiers de formalités, la Commission peut être amenée à inciter les entreprises ou les pouvoirs publics à modifier leur système, à utiliser des solutions techniques alternatives ou à prévoir des garanties pour la protection des données des personnes.

Ainsi, dans le domaine de la santé, la CNIL participe au comité de pilotage chargé de mettre en place le nouvel identifiant de santé, qui sera la pierre angulaire du futur Dossier médical personnel de chacun. Elle fait également partie du comité du RGI (Référentiel Général d'Interopérabilité), publié le 12 juin 2009, qui est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration.

En outre, suite aux études menées l'année dernière sur les dispositifs biométriques de reconnaissance du réseau veineux du doigt, une biométrie considérée sans trace, la CNIL a adopté en mai 2009 une autorisation unique relative à ces dispositifs quand ils sont utilisés aux fins de contrôler l'accès aux locaux sur les lieux de travail. Par ailleurs, la reconnaissance du réseau veineux de la paume de la main a également été mise en œuvre dans des applications visant à lutter contre la fraude aux examens.

### Publicité ciblée

Le modèle économique de nombreuses sociétés phares d'Internet est basé sur la fourniture de services apparemment «gratuits» pour l'internaute, mais financés majoritairement, sinon exclusivement, par la publicité.

Le marketing ciblé est ainsi devenu le «carburant» de l'économie numérique, de plus en plus gourmande en données personnelles.

Ces évolutions font craindre notamment un «profilage» systématique des internautes qui plus est, à leur insu, ainsi qu'un risque de «marchandisation» des profils individuels entre les fournisseurs de contenus et les annonceurs.

Dans son rapport, rendu public en mars 2009, la CNIL a fait le point sur les différentes techniques de publicité en ligne, sur les risques d'atteinte à la vie privée et les parades possibles.

### Nanotechnologies

Jouant un rôle d'alerte et de conseil, la CNIL a fondamentalement pour mission de veiller à ce que le développement des nouvelles technologies ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Les principaux enjeux liés à l'essor des nanotechnologies résident dans la difficulté à contrôler ce qui ne se voit pas et dans la juste perception des risques qu'elles présentent notamment en termes de traçabilité des personnes et de respect de la vie privée.

Comment être informé de l'existence, de l'objet et des effets d'une technologie invisible (ou quasi invisible) et dispersée? Comment assurer que le développement de ces technologies ne se fera pas au prix d'une «hypertraçabilité» des personnes remettant en question leur liberté d'aller et venir? Car cette liberté n'existe pas si l'anonymat n'est pas garanti!

Face à ces enjeux, il faut dès à présent s'interroger sur la régulation à envisager et sur une éventuelle évolution du cadre législatif. En particulier, faut-il interdire certains usages des nanotechnologies?

Il convient aussi d'identifier les règles de protection des personnes à promouvoir. Les principes d'innocuité, de proportionnalité, de sécurité, d'information et de maîtrise des personnes sur leurs données sont autant de garanties qu'il convient d'intégrer en amont, dès la conception des systèmes et des applications des nanotechnologies.

C'est pourquoi la CNIL a participé activement au grand débat public national organisé sur les nanotechnologies dans le but de sensibiliser les personnes et les pouvoirs publics aux risques que ces technologies comportent. Elle a notamment rédigé un « cahier d'acteurs » résumant ses interrogations.

**Normalisation et standards**

En 2008, la CNIL avait rejoint le GCSSI, le groupe en charge de la normalisation de la sécurité à l'AFNOR (Agence Française de Normalisation), dans le but de se positionner comme un acteur incontournable de la normalisation dans des domaines clés de la protection des données. Ce groupe élabore les positions françaises sur les projets de normes ISO.

L'ISO développe actuellement des projets de normes dans le cadre de la protection de la vie privée et de la protection des données personnelles. Elle travaille depuis 2005 sur un projet de norme appelé ISO 29100 "Privacy Framework" (cadre de protection de la vie privée) qui détermine des exigences et une terminologie communes en matière de protection de la vie privée à l'échelle internationale. Il s'agit d'un document fondateur qui pourrait à terme servir de référence à d'autres normes.

Comme la structure et les principes de ce projet de norme apparaissaient en retrait et souvent en contradiction avec les standards européens, le président de la CNIL a mobilisé en urgence le G29 et la Commission européenne sur cette question au mois de juin 2009. Le G29 s'est pleinement mobilisé sur cette question et la CNIL a coordonné l'élaboration de commentaires avec ses homologues européens, ainsi qu'avec ses interlocuteurs industriels ou institutionnels à l'AFNOR.

Pour la première fois, en novembre 2009, un représentant de la CNIL a participé à l'une des réunions internationales bisannuelles du groupe chargé de l'élaboration de cette norme à l'ISO. L'ISO a d'ailleurs souligné son intérêt pour les contributions des autorités de protection des données en exprimant le souhait de formaliser une « liaison » avec le G29.

En outre, l'ISO à décidé de mettre en place un Comité d'orientation sur la vie privée (Privacy Steering Committee, PSC) afin de mieux coordonner ses activités dans le domaine de la vie privée. Consciente de l'importance stratégique et transversale de ce comité, la CNIL a obtenu qu'un de ses représentants fasse partie de la liste des experts intégrant le PSC, dont la première réunion aura lieu en février 2010.

**Contrôles des systèmes de vote électronique**

Au cours de l'année 2009, la CNIL a effectué des contrôles d'élections électroniques organisées par des organismes privés et des ministères (élections prud'homales et de l'Ordre des infirmiers). Ces contrôles furent également l'occasion de vérifier les dispositifs de vote proposés par les différents prestataires du marché.

La CNIL vérifie notamment les conditions du scellement physique et logique de l'urne électronique, afin de détecter toute modification du dispositif de vote et d'empêcher toute manipulation des bulletins. Elle examine s'il existe, ou non, des moyens de connexion au dispositif de vote durant le scrutin. Elle vérifie ensuite si les différents programmes constitutifs du dispositif de vote utilisé ont été expertisés dans leur intégralité, en faisant notamment des copies de documents et de fichiers informatiques comme le lui permet la loi. Enfin, la Commission examine les moyens mis en œuvre pour s'assurer de l'identité des votants et du secret des votes.

Ces contrôles ont permis de mettre en évidence l'insuffisance des garanties apportées par les dispositifs de vote, en termes de sécurité et de confidentialité des données.

Ainsi, la Commission a sanctionné plusieurs organismes ayant procédé à des votes par voie électronique, car elle a considéré que certains points importants de sa recommandation n'avaient pas été suivis.

**c. Le STIC contrôlé et épinglé**

Le STIC est un fichier national qui enregistre les informations recueillies à partir des procédures établies par les services de police dans le cadre de leurs missions de police judiciaire. Il a pour finalité de *«faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs et l'exploitation des données à des fins de recherche statistique»*.

Toutefois, ce fichier est aussi devenu un instrument d'enquête administrative puisque, depuis la loi du 21 janvier 1995 «d'orientation et de programmation relative à la sécurité», il peut être consulté à l'occasion du recrutement, de l'agrément ou de l'habilitation des personnels de professions très diverses. Ainsi en est-il, à titre d'exemple, des personnels de surveillance et de gardiennage, des personnes souhaitant travailler dans les zones aéroportuaires, des agents de police municipale, des préfets, ambassadeurs, magistrats, etc. Au total, la consultation du STIC à des fins d'enquête administrative est susceptible de concerner aujourd'hui plus d'un million d'emplois.

La CNIL s'est prononcée sur les textes successifs intervenus pour encadrer ce fichier et a pu, à cette occasion, faire part de ses observations[18]. Elle exerce par ailleurs au quotidien les vérifications demandées par les intéressés eux-mêmes dans le cadre du droit d'accès indirect. En outre, elle a effectué en 2009 un contrôle d'ensemble du fichier, qui a permis d'effectuer un état des lieux complet du fonctionnement du STIC.

Ainsi, de nombreux contrôles sur place ont été menés (commissariats, services régionaux de police judiciaire, tribunaux, préfectures, etc.), afin de vérifier sur place les modalités d'alimentation du fichier, les conditions et l'effectivité de sa mise à jour, les modalités d'accès et les mesures de sécurité existantes.

Les résultats obtenus sont assez inquiétants et montrent notamment que ce fichier n'est pas mis à jour de façon régulière. En effet, il apparait notamment que pour l'année 2007, seulement 21,5 % des classements sans suite pour insuffisance de charges ou infraction insuffisamment caractérisée, 31,17 % des décisions de relaxe, 6,88 % des acquittements et 0,47 % des décisions de non-lieu sont transmis pour mise à jour du STIC.

La CNIL a formulé **11 propositions** pour que son utilisation soit mieux contrôlée et plus sécurisée, afin de conforter l'exactitude et la mise à jour des informations enregistrées et largement consultées.

**d. Les fichiers utilisés en matière d'immigration**

Au-delà des controverses politiques qui ont marqué l'année 2009 en la matière, les fichiers utilisés dans le cadre de la gestion administrative des étrangers ont connu de nombreuses évolutions.

**Le fichier OSCAR**

Un nouveau fichier dénommé OSCAR, prévu par la loi du 20 novembre 2007 relative à la maîtrise de l'immigration, à l'intégration et à l'asile, a été créé en 2009. Il s'agit d'un traitement biométrique qui enregistre les empreintes digitales des bénéficiaires d'une aide au retour, c'est-à-dire des étrangers résidant en France et qui souhaitent retourner dans leur pays d'origine en

[18] Délibérations n°98-97 du 24 novembre 1998, n° 00-064 du 19 décembre 2000, n° 2005-187 du 8 septembre 2005.

contrepartie d'une aide financière. Notre Commission a notamment demandé que les données biométriques de ces étrangers soient bien effacées du fichier si l'aide au retour leur a été refusée, et qu'elles ne soient utilisées qu'à la seule fin de déterminer s'ils ont déjà bénéficié d'une telle aide.

**RMV2 (Réseau Mondial Visas)**
En ce qui concerne les demandeurs de visa, une refonte complète du système dénommé RMV 2, qui enregistre les dossiers de demande de visa, a été entreprise. Cette refonte doit permettre la mise en œuvre du ***VIS*** (Visa Information System, qui mettra en commun, entre les États européens, les informations relatives aux demandeurs de visa Schengen), en même temps qu'il élargit l'accès à ces informations aux préfectures, aux services des douanes ou encore à certains agents de police. Il est également prévu de recourir à des prestataires extérieurs pour collecter les dossiers de demande de visa et enregistrer ces informations dans le traitement, ce sur quoi notre Commission s'est montrée très réservée, eu égard aux possibilités de captation de données par ces prestataires ou par les autorités des pays dans lesquels les visas sont délivrés.

**Le GIDESE et le FNAD (fichier des non-Admis)**
Deux autres fichiers ont été mis en œuvre en 2009, à titre expérimental : le traitement GIDESE a pour but de contrôler les entrées et les sorties de l'Ile de la Réunion des étrangers munis d'un visa, afin de permettre aux autorités de repérer les personnes se maintenant illégalement sur le territoire.

Le FNAD (Fichier des Non-Admis) est un système biométrique qui enregistre les empreintes digitales et les photographies des étrangers qui, ayant été contrôlés à l'occasion du franchissement de la frontière, ne remplissent pas les conditions d'entrée requises. Créée pour deux ans en 2007 et limitée à la frontière de l'aéroport de Roissy, l'expérimentation du FNAD a été reconduite pour deux années supplémentaires par le ministère de l'immigration. Notre Commission a obtenu que cette expérimentation soit rigoureusement évaluée, afin que l'intérêt de ce fichier, qui ne permettrait que d'identifier les personnes commettant de nouveau une infraction aux règles d'entrée sur le territoire français, soit plus clairement établi avant d'envisager une généralisation à l'ensemble du territoire national.

**Les traitements relatifs aux demandeurs d'asile**
Notre Commission est particulièrement attentive aux évolutions de ces fichiers, qui doivent faire l'objet de garanties spécifiques, dans la mesure où les dossiers de demande d'asile contiennent des données très sensibles, comme les origines ethniques, les opinions politiques et religieuses des personnes.

Le ministère de l'immigration a créé cette année le fichier DN@ qui vise à améliorer la gestion des capacités d'accueil des centres d'accueil des demandeurs d'asile (CADA). Il enregistre des informations permettant le suivi individualisé des personnes qui y sont prises en charge. L'avis de notre Commission a permis que ne soient pas enregistrées, dans le fichier DN@, des données relatives à la protection sociale ou à la santé des personnes accueillies en CADA, non nécessaires à la finalité de gestion administrative des capacités d'accueil des centres. Elle a également exigé que les destinataires des informations (et notamment l'OFII, les services de l'asile du ministère de l'immigration et les préfectures) fassent tous l'objet d'une procédure de désignation et d'habilitation individuelle, afin que seuls les agents directement en charge de l'accueil des demandeurs d'asile aient accès aux informations enregistrées dans DN@.

Les autorités administratives ne sont pas les seules à utiliser des fichiers contenant des informations sur les demandeurs d'asile. Ainsi, notre Commission a autorisé cette année la CIMADE, association de défense des droits des étrangers qui intervient notamment dans les centres de rétention administrative, à mettre en œuvre deux traitements informatiques ayant pour finalité la gestion des dossiers des étrangers assistés dans ses permanences et dans les centres de rétention. Elle s'est montrée particulièrement attentive aux mesures de sécurité entourant le fonctionnement de ces fichiers (modalités d'accès aux données, traçabilité des actions, etc.), à la durée de conservation des informations, qui ne peut excéder un an, ainsi qu'aux modalités d'information des personnes et d'exercice des droits d'opposition, d'accès et de rectification ou de suppression des données qui les concernent.

# Allemagne

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

Le 1er septembre 2009, plusieurs modifications importantes de la loi fédérale sur la protection des données sont entrées en vigueur. En réponse à la vague de scandales qui ont secoué le secteur privé en matière de protection des données, à partir de début 2008, les règles relatives au traitement de données par des tiers et à l'utilisation des données d'adresse à des fins publicitaires ont été renforcées. En outre, les autorités en charge de la protection des données ont vu leurs pouvoirs étendus afin d'imposer des sanctions au secteur privé. Elles ont obtenu pour la première fois des moyens d'action effectifs et sont désormais en mesure de solliciter une intervention juridique pour clarifier des questions d'interprétation prêtant à controverse. Une nouvelle règle consiste également en la notification obligatoire dans le cas de violations de la protection des données: les entreprises privées ont l'obligation d'informer les personnes concernées ainsi que l'autorité de protection des données compétente en cas de violation grave des règles de protection des données. Enfin, le législateur a établi des dispositions spécifiques concernant la collecte, le traitement et l'utilisation des données d'employés, y compris les dossiers papier et les registres manuscrits. Bien que cette réglementation ne régisse pas toutes les formes de manipulation de données d'employés, le gouvernement fédéral envisage toutefois de la développer en 2010.

## B. Jurisprudence importante

**Prolongation des décisions préjudicielles de la Cour constitutionnelle fédérale concernant la conservation des données en vue d'un usage ultérieur**

Dans ses arrêts de mars et octobre 2008 (numéro de dossier 1 BvR 256/08), la Cour constitutionnelle fédérale a préjudiciellement restreint l'utilisation des 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». C'est ainsi que la Cour constitutionnelle fédérale a réduit le nombre d'infractions pour lesquelles des données peuvent être conservées en vue de constituer un catalogue d'infractions graves et a limité les finalités d'utilisation des données, qui peuvent uniquement servir à prévenir les dangers et à aider les services de renseignement en cas de menace imminente pour la vie, l'intégrité et la liberté d'un individu ou pour l'existence ou la sécurité de la Fédération ou d'un Land, ou encore à prévenir un danger général. Étant donné que les arrêts étaient limités à six mois ou, autrement, jusqu'au jugement de la Cour sur le principal, ils ont été prolongés fort à propos en 2009 par la Cour constitutionnelle fédérale sans autre modification de contenu. La décision au principal est attendue en 2010.

**Décision du tribunal administratif de Berlin exemptant des fournisseurs de l'obligation de conserver les données, annulée par le tribunal administratif supérieur de Berlin-Brandebourg**

Dans une décision préjudicielle datant d'octobre 2008, le tribunal administratif de Berlin a interdit à l'autorité de régulation (Agence fédérale des réseaux) d'imposer une amende à des fournisseurs qui refusaient 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 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. L'Agence fédérale des réseaux a interjeté appel de ces décisions auprès du tribunal administratif supérieur compétent de Berlin-Brandebourg. Contrairement au tribunal administratif, cette juridiction a décidé, le 2 décembre 2009, que, quoi qu'il en soit, les doutes existant quant aux coûts de mise en œuvre du cadre technique devant permettre la conservation des données ne sont pas de nature à soustraire les entreprises de télécommunications à l'obligation de se conformer au droit communautaire obligatoire.

## C. Questions diverses importantes

**Fichier de données d'avertissement sur les visas**

Le gouvernement fédéral élu en 2009 envisage de se réatteler au projet législatif d'un fichier de données d'avertissement sur les visas, sous une forme réduite. Sous la législature précédente, ce projet avait échoué. Un point essentiel critique lié à la loi sur la protection

des données avait alors été soulevé à l'encontre du projet. Il s'agira aujourd'hui d'en tenir compte. Le gouvernement fédéral veut que les données relatives aux parties hôtes et aux signataires de l'engagement de prise en charge envers les autorités de l'immigration ne soient enregistrées que si ceux-ci ont été convaincus d'un comportement illégal dans le cadre de la procédure d'octroi d'un visa ou par rapport à un pays étranger.

Or, au regard de la loi sur la protection des données, des doutes subsistent quant à la réglementation envisagée. Plus particulièrement, le besoin réel et l'existence à long terme d'une «solution nationale distincte» dans le contexte du système d'information européen sur les visas (VIS) nous semblent douteux. À cela s'ajoute la nécessaire clarification concernant la création du fichier de données d'avertissement sur les visas et les droits d'accès aux données conservées.

**Adaptation de la loi sur le registre central des étrangers (loi AZR)**
Suite à l'arrêt de la Cour de justice de l'Union européenne dans l'affaire *Huber* (arrêt du 16 décembre 2008, affaire C-524/06), il s'impose d'amender la loi sur le registre central des étrangers. La nouvelle réglementation doit veiller à ce que les données conservées dans le registre concernant les citoyens de l'Union européenne soient uniquement celles qui sont indispensables à l'application des dispositions en matière de droit de séjour.

De surcroît, l'objet des données conservées dans le registre central des étrangers doit être strictement limité. Dès lors, du point de vue de la protection des données, l'accès aux données des citoyens de l'UE par les services répressifs dans le cadre d'un prétendu «chevauchement des tâches» (les données sont collectées aux fins de différentes tâches et mises à la disposition de différentes autorités dans l'exercice de leurs missions) est contestable en l'absence de la garantie que les données collectées et traitées sont utilisées aux fins exclusives de décisions relatives au droit de séjour.

**Adoption de la loi relative au diagnostic génétique**
Le Bundestag allemand a adopté le 24 avril 2009 une loi sur le diagnostic génétique régissant les examens génétiques à des fins médicales, en vue de la clarification de liens de parenté et des questions liées au secteur des assurances et à la vie professionnelle. La loi régit en outre le traitement des données génétiques. Au centre des grands principes de base de l'avant-projet: le droit des individus à l'autodétermination informationnelle, qui affirme tant le droit de connaître ses propres résultats médicaux d'analyse génétique que le droit de les ignorer (le droit de ne pas savoir).

Seul un docteur en médecine est habilité à pratiquer un examen génétique à des fins médicales. À cet égard, l'information des patients est essentielle. Si un examen conclut à un pronostic de risque de maladie (diagnostic génétique prédictif), il est obligatoire de fournir au patient des conseils de nature génétique avant et après l'examen.

Un examen génétique visant à établir des liens de parenté n'est admis que si les personnes titulaires de l'échantillon génétique à examiner ont consenti à l'examen.

En matière de droit du travail, il est tout particulièrement interdit de pratiquer des examens génétiques à la demande d'un employeur. Un employeur n'est pas autorisé à demander les résultats d'un examen génétique antérieur, ni à les recevoir ou à les utiliser. Cependant, dans un souci de sécurité au travail, les examens génétiques peuvent être autorisés dans des cas exceptionnels et sous réserve de conditions strictes dans le cadre des examens médicaux préventifs auxquels doivent se plier les travailleurs.

Les compagnies d'assurance ne sont pas autorisées à demander à leurs clients de subir des examens génétiques ou de leur communiquer les résultats d'examens génétiques antérieurs, pas plus qu'à recevoir ou à utiliser ces résultats ou données, avant ou après avoir contracté une assurance. Toutefois, certaines exceptions existent, soumises à des restrictions strictes: dans le cadre de la conclusion d'un contrat d'assurance-vie, d'assurance-invalidité, d'assurance-invalidité professionnelle et d'assurance-soins infirmiers, les résultats d'examens génétiques réalisés antérieurement doivent être présentés si le contrat porte sur une allocation supérieure à 300 000 euros ou sur un revenu annuel chiffré à plus de 30 000 euros.

Malheureusement, la réglementation est défaillante en ce qui concerne le traitement des examens génétiques dans le cadre de la recherche.



## Grèce

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

En 2009, une série de développements législatifs ont porté sur l'ordre juridique interne relatif à la protection des données à caractère personnel. Le ministre de la justice, de la transparence et des droits de l'homme du nouveau gouvernement a récemment annoncé la révision des modifications apportées l'été dernier à la loi grecque sur la protection des données (voir point 1, ci-dessous) et au Code pénal (voir point 3, ci-dessous), conformément aux avis y afférents de l'Autorité hellénique de protection des données (AHPD) (voir avis 1/2009 et avis 2/2009, ci-dessous).

*1. Modification de la loi grecque 2472/97 sur la protection des données, concernant les systèmes de vidéosurveillance dans les lieux publics*

Un nouvel amendement a été apporté à la loi grecque 2472/97 sur la protection des données, et plus spécifiquement à son article 3, à savoir le champ d'application de la loi. En conséquence, la loi ne s'applique pas au traitement de données à caractère personnel effectué par les autorités publiques compétentes au moyen de dispositifs techniques spéciaux destinés à l'enregistrement de sons ou d'images dans des espaces publics, dans le but de garantir la sécurité de l'État, la défense nationale, la sécurité publique, la protection des personnes et des biens et la gestion du trafic. Le matériel collecté au moyen de tels dispositifs (pour autant qu'il ne relève pas du point b du présent article[19]) est conservé durant une période de 7 jours, au terme de laquelle il est détruit sur ordre du ministère public. Toute violation des dispositions susmentionnées est sanctionnée d'une peine d'emprisonnement d'au moins un an, sous réserve d'une peine plus stricte imposée en vertu d'une autre loi.

Conformément au rapport accompagnant la disposition susmentionnée, l'introduction de l'exception précitée est jugée nécessaire compte tenu de la forte hausse des délits et des méthodes employées par leurs auteurs.

*2. Nouvelle loi imposant l'identification des abonnés, utilisateurs et équipements techniques dans le secteur de la téléphonie mobile*

La nouvelle loi 3783/2009, publiée en août 2009, met fin à l'anonymat des abonnés (et des utilisateurs) de téléphones mobiles prépayés à des fins de sécurité nationale et d'enquête sur des infractions graves. Pour les mêmes raisons, et indépendamment du type de contrat, elle impose des obligations d'enregistrement pour a) l'équipement technique des téléphones mobiles des abonnés et utilisateurs et b) les données d'identification des utilisateurs (c.-à-d. lorsqu'un abonné prend en charge les paiements correspondant à plusieurs numéros de téléphone mobile utilisés par d'autres personnes, à savoir les employés).

[19] La présente loi ne s'applique pas au traitement de données à caractère personnel effectué par:
a) une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques,
b) le ministère public et les autorités agissant sous son contrôle dans le cadre de l'attribution de la justice ou pour leurs propres besoins opérationnels, dans le but de vérifier des faits qualifiés d'actes délictueux graves ou de délits intentionnels, et surtout des attentats à la vie, des atteintes à la liberté sexuelle, des délits relatifs à l'exploitation sexuelle à des fins commerciales, des atteintes à la liberté, des atteintes au patrimoine, des atteintes au droit à la propriété, des violations de la législation sur les drogues, des conspirations contre l'ordre public ainsi que des délits sur mineurs. Eu égard à ce qui précède, le matériel existant ou les dispositions de procédure pénale s'appliquent. Lorsque les citoyens exercent leur droit de réunion, conformément à l'article 11 de la Constitution, l'utilisation de moyens d'enregistrement audio et vidéo ou d'autres moyens techniques spéciaux est autorisée aux conditions stipulées dans l'article suivant.
L'enregistrement audio et vidéo à l'aide de moyens techniques en vue de vérifier la perpétration des délits précités est autorisé sur ordonnance du ministère public et si l'ordre public et la sécurité sont gravement menacés.
Les enregistrements précités sont uniquement destinés à être utilisés comme preuves de la perpétration d'un délit devant une autorité d'enquête, un représentant du ministère public ou un tribunal. Le traitement de tout autre matériel non nécessaire pour atteindre l'objectif précité dans le cadre de la vérification de délits commis est interdit, et le matériel concerné sera détruit sur ordre du procureur compétent.

Plus spécifiquement, les fournisseurs doivent collecter des données personnelles relatives à l'identification des abonnés et utilisateurs, nouveaux et existants. En ce qui concerne les abonnés existants, l'opération devait être terminée pour le 30 juin 2010. Si un abonné a omis de soumettre ses données d'identification au fournisseur pour le 30 juillet 2010, le fournisseur doit procéder à la déconnexion du service de l'abonné en question. Les fournisseurs sont tenus de conserver les données jusqu'à un an après l'interruption de l'abonnement, sans que cela représente un surcoût pour l'abonné.

Les données d'identification devant être collectées au sujet de l'abonné comprennent le nom, le nom du père, le lieu et la date de naissance, la photocopie de la carte d'identité nationale ou du passeport et le numéro de registre national du contribuable. Les catégories de données diffèrent légèrement pour les abonnés personnes morales. D'autres données doivent être collectées en vue d'identifier l'équipement mobile, telles que les numéros IMSI (*International Mobile Subscriber Identity*, littéralement «identité internationale de l'abonné mobile») et IMEI (*International Mobile Equipment Identity*, littéralement «identité internationale de l'équipement mobile»), ainsi que l'heure et le lieu (*cell-id*) de la première activation. Chaque carte SIM (*subscriber identity module*) vendue doit être liée à un abonné identifié. Les abonnés ont l'obligation de notifier par écrit au fournisseur tout changement d'utilisation du téléphone mobile prépayé, à l'instar d'une perte, d'un vol ou de tout transfert de la carte SIM à une autre personne.

L'accès aux données conservées par le fournisseur ne sera accordé qu'aux services répressifs, conformément à la loi sur l'interception légale de communications. Actuellement, selon de récentes estimations, on recense 13,5 millions d'abonnements de téléphonie mobile prépayée anonymes en Grèce, dont 9 millions sont actifs. Seuls 5 millions sont enregistrés (c.-à-d. que l'abonné est identifié).

*3. Amendement du Code pénal grec concernant l'analyse ADN et la création d'une base de données de profils ADN*

L'article 200$^{A}$ du Code de procédure pénale a été récemment amendé comme suit (les modifications apparaissent en italiques):

1. *«En présence d'indications sérieuses qu'un individu a perpétré un acte délictueux grave ou un délit punissable d'une peine d'emprisonnement d'au moins trois mois, les autorités répressives collectent un échantillon cellulaire en vue de procéder à des tests ADN pour identifier le contrevenant.»*

L'analyse est strictement limitée aux données nécessaires à l'identification du contrevenant et est pratiquée dans un laboratoire public ou universitaire.

L'accusé a le droit d'utiliser son analyse ADN pour sa propre défense.

2. Si l'analyse précitée s'avère concluante, le résultat est annoncé à la personne titulaire de l'échantillon cellulaire et celle-ci a le droit de demander une contre-analyse. Le cas échéant, les dispositions des articles 204 à 208 s'appliquent. Le responsable de l'enquête ou le procureur a également le droit de demander une contre-analyse. Si l'analyse s'avère négative, l'échantillon cellulaire et le profil ADN sont immédiatement détruits. Si, toutefois, l'analyse s'avère positive, l'échantillon cellulaire est immédiatement détruit; par contre, le profil ADN de la *personne accusée du délit est conservé dans une base de données spéciale, gérée par le département d'enquête criminelle du siège de la police hellénique. Cette donnée est conservée de manière à pouvoir être utilisée dans l'enquête sur d'autres délits et est détruite dans tous les cas après la mort de la personne concernée. L'exploitation de la base de données est supervisée par un substitut du procureur ou par un procureur désigné par le Conseil supérieur de la magistrature, conformément à la loi, pour un mandat de deux ans.*

3. *La destruction de l'échantillon cellulaire et du profil ADN, telle que définie au paragraphe 2, se fait en présence de l'officier de justice chargé de superviser l'exploitation de la base de données.* Le titulaire de l'échantillon cellulaire est prié d'assister à la destruction de son échantillon. Il peut se faire accompagner par un avocat et un expert technique.»

## B. Jurisprudence importante

*Avis 1/2009 – sur la modification de la loi grecque sur la protection des données concernant l'exploitation de systèmes de vidéosurveillance dans les lieux publics (voir amendement susmentionné de la loi 2472/1997)*

Eu égard à la Constitution, à la Convention européenne des droits de l'homme (CEDH) et à la Convention n° 108 du Conseil de l'Europe, et après avoir réalisé une synthèse comparative de la législation pertinente dans d'autres États membres de l'Union européenne, l'Autorité hellénique de protection des données a rendu l'avis suivant:

- La disposition en question exclut dans la pratique l'exploitation de dispositifs d'enregistrement audio et vidéo dans les lieux publics du champ d'application de la loi 2472/97 et du champ de contrôle de l'AHPD. Dans ce sens, la disposition ne satisfait pas aux exigences de qualité fixées par la jurisprudence de la Cour européenne des droits de l'homme concernant toute loi introduisant des restrictions à un droit fondamental. Plus précisément, l'amendement soumis ne répond pas aux exigences de prévisibilité de ses effets, faute de spécifier les conditions et la procédure présidant au traitement des données d'une manière qui offrirait aux personnes concernées des garanties appropriées contre une action arbitraire. En outre, d'un point de vue législatif, la disposition doit être intégrée à la loi régissant les autorités publiques, lesquelles agiront en qualité de responsables du traitement.
- L'invocation générale de la protection de la sécurité publique ne répond pas à l'exigence de spécificité. Le motif du traitement des données doit être précisé, au moyen par exemple d'une formule légitime invoquant la volonté de décourager les personnes susceptibles de commettre des attentats à la vie ou des atteintes à la liberté et à la propriété individuelles. À moins de spécifier un tel objectif, il est impossible de vérifier si le principe de proportionnalité (tel que formulé dans le système constitutionnel grec et la CEDH) est respecté et si l'intervention spécifique des pouvoirs publics dans la vie privée (vidéosurveillance des lieux publics) et, partant, les restrictions imposées de ce fait sur le droit à la protection des données à caractère personnel se justifient pour atteindre l'objet visé.
- La disposition ne spécifie pas les critères de danger (taux de criminalité élevé dans une zone/des bâtiments pouvant requérir une protection spéciale) en vertu desquels il sera décidé, *in fine*, de l'opportunité ou non d'autoriser l'installation et l'exploitation de systèmes de vidéosurveillance dans les espaces publics. En conséquence, la décision du lieu et de la période d'installation de systèmes de vidéosurveillance est laissée à la discrétion absolue des autorités compétentes. Cette discrétion illimitée outrepasse toutefois la mesure nécessaire qui, selon la jurisprudence de la Cour européenne des droits de l'homme et du Conseil d'État grec, justifie d'imposer des restrictions aux droits de l'homme. Ce cas particulier présente un risque de transgression illégale non seulement de l'article 9A de la Constitution, mais aussi d'autres droits constitutionnels (article 2, paragraphe 1, article 5, paragraphe 1, et article 11).
- Outre la limitation de durée de conservation de ces données, il n'existe pas de règles spécifiques régissant la collecte, la conservation, l'utilisation et la transmission ultérieure des données. Cette omission soulève de grandes inquiétudes quant à la conformité de l'amendement aux exigences de qualité stipulées par la Cour européenne des droits de l'homme concernant l'ingérence dans l'exercice du droit au respect de la vie privée (article 8 de la CEDH).
- Il n'y a pas de disposition relative aux mesures techniques et organisationnelles requises pour garantir la sécurité des données collectées et conservées.
- Il n'y a pas de disposition relative à la protection effective des droits des personnes concernées, que le traitement de données risque de bafouer. Pourtant, une telle garantie fait partie de l'essence même du droit constitutionnel à la protection des données à caractère personnel (art. 9A de la Constitution).
- Aucune disposition ne définit clairement l'identité du responsable du traitement desdites données. La référence générale à l'«autorité publique compétente» ne protège pas suffisamment l'individu en cas de violation de la disposition. De plus, cette dernière crée un risque de conflit de compétences entre les différentes autorités en présence.
- Aucune disposition n'exige que l'installation du dispositif de vidéosurveillance se fonde sur un acte administratif préalable. Cette omission implique que l'examen judiciaire d'une telle installation ne pourra être très efficace. Elle laisse pour seule possibilité aux personnes lésées (celles dont les données ont été

enregistrées sans qu'elles aient participé à une activité criminelle) d'engager une procédure de dédommagement contre l'État.
- Enfin, et surtout, l'exclusion d'un secteur vaste et sensible des actions de l'État du champ de compétences de l'AHPD transgresse l'essence même de l'article 9A de la Constitution et pourrait être déclarée non conforme à l'article 8, paragraphe 2, de la CEDH, tel que l'interprète la Cour européenne des droits de l'homme. Le libellé des articles 9A et 101A de la Constitution, ainsi que le débat parlementaire relatif à l'adoption de ces dispositions en 2001, indiquent que le législateur a vu dans la création et l'opérationnalisation de l'APD une garantie institutionnelle nécessaire à la protection des données à caractère personnel. La nécessité de créer une autorité indépendante, dotée de tout le savoir-faire technique requis, découle du fait que la rapide évolution des développements TI menace la protection de la vie privée. C'est pourquoi la supervision de l'AHPD dans le domaine du traitement de données dans les secteurs public et privé appartient à l'essence même du droit fondamental à l'autodétermination informationnelle.

En conclusion, l'amendement exclut purement et simplement l'exploitation des dispositifs d'enregistrement audio et vidéo dans les lieux publics du champ d'application de la loi 2472/97 et du champ de compétences de l'AHPD. Il n'est par conséquent pas conforme à l'article 9A de la Constitution et à l'article 8 de la CEDH.

*Avis 2/2009 – sur l'amendement du Code pénal concernant l'analyse ADN et la création d'une base de données de profils ADN*

Les principales observations sont les suivantes:
- Malgré certains aspects positifs de l'amendement, ce dernier ne rencontre pas tous les critères de qualité requis dans le cadre du droit à la protection des données à caractère personnel, en particulier dans le cas des profils ADN utilisés à des fins d'enquête criminelle.
- Afin d'observer le principe de proportionnalité, en particulier le volet «nécessité», il convient de stipuler dans la loi que l'analyse génétique n'est autorisée qu'en l'absence de tout autre mode de preuve permettant d'identifier le contrevenant.
- La liste des délits pour lesquels le recours aux profils ADN dans le cadre d'une enquête est autorisé a été allongée; elle inclut désormais tous les actes délictueux graves et délits passibles d'une peine d'emprisonnement d'au moins trois mois.
- Il est nécessaire d'établir, sur la base de critères qualitatifs, une distinction entre l'enquête sur un délit actuel et la future investigation d'autres délits (rendue possible par la création d'une base de données de profils ADN). Afin de limiter le recours aux profils ADN dans le souci de garantir le principe de proportionnalité, le législateur doit envisager soit de limiter la liste des délits aux actes délictueux graves dans le cadre des enquêtes actuelles et futures, soit d'autoriser l'utilisation des profils ADN dans le cadre d'une enquête effective sur tous les actes délictueux graves et les délits pénaux. Cependant, la conservation des profils en vue d'un usage ultérieur ne doit être autorisée qu'à des fins d'enquête portant sur des délits très graves, comme des crimes, et/ou des délits qui enfreignent des intérêts légaux spécifiques, comme la liberté sexuelle (bien que cette dernière puisse relever de la catégorie des délits pénaux). Si la seconde solution est privilégiée, chaque jugement *in concreto* devra se fonder sur la gravité du délit, mais aussi sur d'autres critères relatifs au contrevenant lui-même (antécédents, personnalité, etc.), pouvant établir la probabilité d'une récidive (pronostic négatif).
- L'amendement n'établit aucune distinction entre la conservation de profils ADN de personnes condamnées ou acquittées, ou d'adultes et de mineurs. De plus, cette conservation peut durer pendant une période de temps illimitée (la seule limite temporelle étant le décès du suspect). Les problèmes susmentionnés peuvent être résolus comme suit: a) les profils ADN des personnes irrévocablement acquittées pour quelque raison que ce soit doivent être supprimés de la base de données des profils ADN; b) les profils ADN des personnes irrévocablement condamnées ne peuvent être conservés que pendant une période de temps limitée une fois leur peine purgée; c) les profils ADN de mineurs âgés de moins de 13 ans, vis-à-vis desquels ne peuvent être prises que des mesures de redressement et de réhabilitation, ne doivent pas être conservés; et d) les profils ADN de mineurs âgés de plus de 13 ans ayant été irrévocablement condamnés peuvent être conservés pendant une période

de temps déterminée, sensiblement plus courte que celle applicable aux adultes.
- Il n'y a pas de protection des profils ADN non identifiés.
- Pour tout ce qui concerne la base de données de profils ADN, une loi ou un décret présidentiel relatif aux pouvoirs et à la structure de la police hellénique doit prévoir des dispositions couvrant, entre autres, les aspects suivants: a) l'objet du transfert des profils ADN et de l'accès en ligne à ces profils, qui doit coïncider avec l'objet de la conservation initiale; b) les autorités publiques ayant accès à la base de données ou auxquelles le transfert est autorisé; c) les droits d'accès et d'opposition des personnes concernées, y compris l'obligation du responsable du traitement des données d'informer les personnes concernées au sujet du fonctionnement de la base de données et de la conservation de leur profil dans ladite base de données; d) les procédures de suppression et de blocage en vigueur lorsque les données ne sont pas supprimées; e) les mesures appropriées pour la sécurité de la base de données, la prévention des accès non autorisés, la modification et le transfert des données, et le contrôle de chaque intervention.
- L'amendement abroge le rôle du Conseil de la magistrature en tant que garantie procédurale pour l'obtention et l'analyse d'échantillons cellulaires et, ce faisant, rétrograde ce procédé à un simple acte d'enquête. Cependant, dans la mesure où l'obtention (et l'analyse) d'un échantillon cellulaire constitue une ingérence particulièrement intrusive, qui requiert la clarification et la précision de concepts légaux vagues (c.-à-d. des présomptions sérieuses, un pronostic négatif), une garantie judiciaire doit être fournie par une décision du Conseil de la magistrature ou, à tout le moins, par un ordre du ministère public spécialement émis à cette fin.
- La base de données de profils ADN doit être placée sous la supervision d'un substitut du procureur ou d'un procureur. Le procureur du ministère public constitue sans aucun doute une garantie institutionnelle supplémentaire. Si, toutefois, celle-ci devait être considérée comme une solution de remplacement au contrôle exercé par l'autorité de protection des données, elle irait à l'encontre de l'essence de l'article 9A de la Constitution, qui stipule clairement que l'APD offre une garantie institutionnelle du droit à la protection des données à caractère personnel.

En conclusion, l'amendement doit être modifié conformément aux observations ci-dessus, afin de s'inscrire dans le droit fil des exigences de l'article 9A de la Constitution grecque et de l'article 8 de la Convention européenne des droits de l'homme.

*Décision 75/2009 – portant sur la création d'une base de données reprenant les membres praticiens de l'Association médicale d'Athènes, accessible sur internet*

- Dans cette affaire, une entreprise demandait à collecter les données à caractère personnel des membres praticiens de l'Association médicale d'Athènes à partir du site internet de l'Association (qui est un organe public) en vue de créer un nouveau portail devant permettre aux visiteurs de trouver plus facilement un médecin sur la base de sa spécialisation et de critères géographiques, ainsi que d'autres critères également (p. ex. les médecins affiliés à des mutualités spécifiques). Les membres de l'Association médicale ont été avertis au préalable que leurs données pouvaient être divulguées à des tiers ou sur le site internet de l'association en vue, par exemple, d'informer le public et de favoriser la collaboration scientifique, et ont été autorisés à s'y opposer.

  L'AHPD a décidé que l'objectif secondaire du traitement est différent de sa finalité première (registre de médecins destiné à informer le grand public, à favoriser la collaboration scientifique, etc.) mais pas incompatible, à condition que la création et l'exploitation de la nouvelle base de données enrichie soient également destinées à informer le public.

- La réutilisation des informations du secteur public à des fins d'exploitation commerciale est déjà autorisée et n'est pas jugée incompatible avec la finalité première du document public. Cependant, les intérêts légitimes des personnes concernées, qui ont communiqué leurs données personnelles dans un but spécifique et ne s'attendent pas à les voir utilisées à d'autres fins que celles directement liées à la finalité première, comme c'est le cas de l'objectif secondaire d'exploitation commerciale, doivent être dûment protégés. Les dispositions de la loi 3448/2006 sur la réutilisation des informations du secteur public, qui transpose en droit national la directive européenne

2003/98/CE concernant la réutilisation des informations du secteur public, s'appliquent également à la réutilisation des informations issues de sources publiquement accessibles, étant donné que, dans le cas présent, les informations dérivées sont toujours «en possession» du responsable du traitement de données.

Le traitement par l'entreprise est légal sous réserve des conditions suivantes: les personnes concernées doivent en être préalablement informées par écrit et avoir le droit de s'y opposer. Le traitement ne doit pas constituer un coût économique pour les personnes concernées et leur nom doit apparaître dans l'ordre alphabétique.

*Décision 83/2009 – concernant la collecte, l'utilisation et la commercialisation de données de communications électroniques et autres*

Suite à un nombre significatif de plaintes, l'AHPD a mené une inspection dans les locaux d'une entreprise qui fournissait un produit appelé «Hellas Navigator – Golden Customer Lists». L'AHPD a imposé des sanctions administratives pour:

- La collecte et la vente d'adresses électroniques. L'entreprise utilisait un robogiciel Larbin (initialement créé pour les noms de domaine .gr et .com.gr) afin de collecter des adresses sur internet (un total d'environ 160 000 adresses a été mis à jour). La liste de diffusion a été vendue à plus de 400 clients, y compris des agences publicitaires, des banques, des hommes politiques et des organismes publics.
- La collecte de données à partir de listes de syndicats professionnels et de catalogues d'exposition (dont des adresses électroniques) sans en informer au préalable les personnes concernées.
- La mise en correspondance de données téléphoniques publiées dans les répertoires de fournisseurs de télécommunications publics avec des données de géolocalisation, sans le consentement des personnes concernées.
- L'envoi de pourriels, c.-à-d. des courriers électroniques vantant les produits de l'entreprise sans le consentement préalable des destinataires. Les pourriels étaient envoyés au moyen du logiciel Turbo Mailer via quatre fournisseurs/connexions ADSL différents (l'adresse de l'expéditeur changeait: hnv@otenet.gr, hellasnv@otenet.gr, hnv2@altecnet.gr, hnv1@hol.gr et calino1@ath.forthnet.gr).
- La vente de droits de licence pour les données de cette base de données à des agences gouvernementales américaines en 2004 sans notification ni obtention d'un permis auprès de l'AHPD.

L'AHPD a publié un avertissement officiel portant sur la violation de l'interdiction d'utiliser les données de l'annuaire téléphonique à d'autres fins sans le consentement préalable des personnes concernées. Pour toutes les autres violations, l'AHPD a infligé une amende totale de 65 000 euros et ordonné la suppression de toutes les adresses électroniques conservées par l'entreprise à ses propres fins ainsi que celles contenues dans le produit «Hellas Navigator – Golden Customer Lists».

*Décision 91/2009 – concernant les services de navigation routière virtuelle en trois dimensions basés sur internet*

L'AHPD a statué que la fourniture d'un service de navigation routière virtuelle en trois dimensions visant des régions grecques, par l'entreprise «KAPOU S.A. GEOINFORMATICS», peut être considérée comme un traitement de données à caractère personnel dans la mesure où les images présentent des personnes, des plaques d'immatriculation de véhicules et des maisons identifiables. Le traitement est conforme à la loi 2472/1997, en particulier sur la base de l'article 5, paragraphe 2, alinéa e, en ce sens que le développement d'une activité économique au bénéfice des utilisateurs, mis en mesure de naviguer virtuellement d'un endroit à l'autre, constitue un objectif légitime. Toutefois, puisque les personnes concernées, directement ou indirectement identifiables à partir des images, n'ont pas de contact préalable avec le responsable du traitement de données, susceptible d'autoriser le traitement éventuel de leurs données, le service doit être fourni sous réserve des conditions suivantes: a) les visages des personnes et les plaques d'immatriculation de véhicules seront floutés avant la fourniture du service au public; b) la période de conservation des données brutes (images non floutées) est fixée à six mois à partir de la capture d'image et, en outre, des mesures de sécurité techniques et organisationnelles appropriées doivent être prises; c) des mesures additionnelles doivent être prévues pour les données sensibles (elles doivent notamment être

floutées en priorité). En outre, le responsable du traitement de données doit accorder un droit d'accès (aux données brutes) et un droit d'opposition avant la publication du service sur internet. L'opposition doit mener au floutage ou à la suppression des données brutes. Une fois les données publiées sur internet, la personne concernée ou tout autre tiers peut signaler l'absence de floutage ou le caractère inadéquat du floutage d'un visage ou d'une plaque d'immatriculation. Le floutage de l'image d'une personne peut également couvrir une zone plus large que le visage, si la personne concernée le demande (avant ou après la publication sur internet), dans la mesure où, dans certaines circonstances, la personne concernée peut être identifiée grâce à sa morphologie. Seules les personnes concernées peuvent demander le floutage de leur maison. Enfin, l'obligation d'informer les personnes concernées sera observée par le biais du marquage des véhicules utilisés pour collecter les images, mais aussi via la presse (les journaux par exemple) ainsi que via le site internet de l'entreprise, et ce de manière simple et accessible.

*Décisions 56/2009 & 74/2009 concernant la biométrie*

L'AHPD a remis deux décisions concernant la légalité du traitement de données biométriques au second semestre 2009. Elles reposaient toutes deux sur le principe de proportionnalité. Plus particulièrement, la décision 56/2009 de l'AHPD a autorisé un fournisseur de services de certification à établir un système biométrique de relevé d'empreintes à partir de cartes, destiné au contrôle de l'accès à la zone spécifique réservée à la création et à la maintenance de clés cryptographiques (c.-à-d. les clés privées des autorités de certification utilisées pour signer les certificats électroniques des utilisateurs). Par contre, dans sa décision 74/2009, l'AHPD a interdit l'utilisation d'un système biométrique à géométrie faciale relié à une base de données centrale en guise de mesure de contrôle de l'accès des employés aux locaux d'une entreprise de services bancaires. Dans ce dernier cas, l'AHPD a conclu que l'entreprise pouvait recourir à des mesures de contrôle de l'accès physique moins intrusives, tandis que des mesures plus fortes pouvaient être appliquées dans les lieux réservés au stockage de données sensibles, en combinaison avec des mesures de contrôle d'accès logique dans le système technique de l'entreprise.

*Décision 9/2009 concernant des mesures organisationnelles dans les centres de santé*

Un patient a déclaré avoir fourni à un centre de santé une radiographie réalisée dans un autre établissement, en vue d'un nouvel examen et d'un nouveau traitement par le personnel médical dudit centre. L'opération chirurgicale qui s'en est suivie s'étant révélée infructueuse, le patient a prié l'établissement de soins de lui remettre la radiographie dans le but de soumettre son dossier médical à un autre centre en vue d'une nouvelle consultation et d'un éventuel traitement. L'établissement n'a pas réagi à sa demande par écrit et le patient a été informé oralement que la radiographie en question avait été perdue. Après une inspection sur site, l'AHPD a découvert que cet établissement de soins ne conservait pas de dossiers médicaux complets, mais uniquement quelques informations relatives au type d'examens médicaux pratiqués par l'établissement même ainsi que les données administratives des patients. L'AHPD a relevé l'obligation légale de tenir des dossiers médicaux complets, en vertu de la loi sur le code de conduite des médecins. L'AHPD a infligé une amende à l'établissement de soins pour ne pas avoir répondu formellement à la demande du patient (ce qui équivaut à une violation du droit d'accès) et pour ne pas avoir pris les mesures organisationnelles à même de démontrer que les données médicales des patients sont conservées en toute sécurité et peuvent leur être restituées.

# Hongrie

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

La directive sur la conservation de données a été intégralement transposée en droit hongrois. Les données de trafic liées aux appels réussis sont conservées pendant un an, contre six mois pour les données relatives aux appels infructueux. La période de conservation d'un an s'applique également aux données de trafic générées par le biais d'internet.

La loi transposant la directive sur la conservation de données a été contestée devant la Cour constitutionnelle. Cette dernière n'a toutefois pas encore rendu sa décision.

## B. Jurisprudence importante

**Surveillance par caméra lors de manifestations**
De nombreux citoyens ont dénoncé une pratique policière consistant à installer des caméras pour surveiller les participants à des manifestations organisées dans des lieux publics. Dans son avis, le commissaire à la protection des données a tout d'abord souligné que chaque action entreprise par les autorités publiques doit promouvoir l'exercice des droits fondamentaux, dont la liberté d'expression. L'utilisation de caméras par les forces de police peut dissuader les citoyens de participer à des manifestations. L'utilisation de ces dispositifs n'est acceptable que s'il existe un risque réel d'actes illégaux et violents susceptibles de troubler la manifestation et si l'intervention des forces de police est nécessaire au rétablissement de l'ordre.

**Ordinateurs saisis par la police**
Un citoyen se plaignait que la police avait saisi son ordinateur dans le cadre de poursuites judiciaires et qu'il était incapable d'en obtenir la restitution depuis plus de six mois. Le commissaire a jugé acceptable que la police saisisse du matériel TI si celui-ci a été utilisé pour commettre un délit. Toutefois, des poursuites judiciaires ne peuvent causer un préjudice que ne justifie pas la conduite d'une enquête en bonne et due forme. La période de plus de six mois a manifestement excédé le délai acceptable pouvant être invoqué dans le cadre des objectifs poursuivis par les poursuites judiciaires.

**Accès aux enregistrements vocaux**
Plusieurs citoyens se sont plaints du refus opposé à leurs demandes d'accéder aux enregistrements vocaux conservés par divers fournisseurs de services. Les demandes étaient généralement refusées au motif que le demandeur n'avait pas besoin d'être en possession de l'enregistrement. Le commissaire a insisté sur le droit des personnes concernées à consulter les informations détenues à leur sujet: seule une disposition légale explicite peut restreindre ce droit. À défaut d'une telle restriction légale au droit d'accès, les plaignants ont le droit d'obtenir une copie de la conversation enregistrée par le fournisseur de services. Cette approche a été ensuite confirmée par le législateur, qui a amendé les règles de protection des consommateurs en garantissant clairement le droit d'accès des personnes concernées à la copie de l'enregistrement, y compris leur conversation avec l'opérateur.

## C. Questions diverses importantes

En 2009, deux entreprises ont engagé des négociations avec le commissaire afin de le persuader de la nécessité d'établir une liste de débiteurs dits positifs. Des fichiers négatifs concernant le non-respect d'obligations financières existent déjà en Hongrie, sans nécessiter le consentement de la personne concernée. Cependant, la collecte d'informations liées à la solvabilité financière nécessite bel et bien le consentement de la personne concernée.

Le commissaire n'est pas favorable à la création d'un registre de solvabilité (liste positive). Selon lui, le caractère «libre» du consentement au traitement ne semble pas garanti, car les clients sont fortement poussés à le donner. Des doutes entourent également le caractère suffisant des informations données aux personnes concernées. De nombreuses institutions financières défendent l'idée d'une liste de débiteurs positifs et, malgré les avertissements du commissaire, ont lancé une «phase pilote» du projet, en collectant des informations de solvabilité auprès de diverses parties intéressées.

**Surveillance par caméra dans les transports publics**
La société de transport de Budapest (BKV) a consulté le commissaire au sujet d'une éventuelle installation de caméras à bord des véhicules de BKV. Le commissaire a

souligné que le consentement des passagers ne peut constituer la base légale du traitement, des points spécifiques du droit hongrois stipulant qu'une loi doit être adoptée pour légaliser le traitement. Le législateur doit trouver un équilibre approprié entre le respect de la vie privée et les considérations d'ordre public. L'avis du commissaire a reçu le soutien de l'Institut national hongrois de criminologie, lequel a suggéré des solutions de remplacement pour améliorer la sécurité dans les transports publics.

# 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 dans le droit irlandais.

En 2009, parmi les développements législatifs ayant une incidence significative sur la protection des données en Irlande, citons la publication en juillet du projet de loi 2009 sur les communications (conservation de données) transposant la directive 2006/24/CE sur la conservation des données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public (modifiant la directive 2002/58/CE).

## B. Jurisprudence importante

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, par exemple, les responsables du traitement des données ne respectent pas les droits d'accès des personnes concernées. Dans certains cas, les responsables du traitement des données sont cités dans des études de cas incluses dans le rapport annuel du commissaire. Dans le courant de l'année 2009, le commissaire a été impliqué dans plusieurs procédures judiciaires (ayant abouti) en relation avec les droits des personnes concernées au titre des lois de 1998 et de 2003 sur la protection des données et du *Statutory Instrument* 535 de 2003 (qui met en œuvre la directive 2002/58/CE en Irlande). Cette situation faisait suite à une série de contrôles sans préavis d'entreprises actives dans le secteur du marketing par SMS en 2007, et au rejet par la Haute Cour de la contestation de la base juridique des poursuites en 2008.

## C. Questions diverses importantes

Toujours en 2009, le ministre irlandais de la justice, de l'égalité et des réformes législatives a créé un comité d'examen sur la protection des données, chargé de formuler des recommandations sur la nécessité de modifier la législation irlandaise sur la protection des données en vue de rendre obligatoire la notification des violations en la matière, assorties d'amendes. À ce jour, le comité a publié un document de consultation, lancé un appel public de propositions, engagé un exercice de consultation parmi les membres du comité et entrepris une recherche de documents fouillée.

## Italie

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

Le cadre réglementaire transposant les directives 95/46/CE, 2002/58/CE et 2006/24/CE n'a pas subi de modifications majeures en 2009. Toutefois, le Parlement a promulgué certaines mesures qui ont amené l'APD à exprimer son inquiétude quant à leurs effets potentiellement négatifs sur la protection des données à caractère personnel.

Plus particulièrement, la loi n° 15/2009 relative à l'amélioration de la productivité dans le secteur public a introduit un amendement à la section 1 du décret de loi 196/2003 en matière de protection des données personnelles, selon lequel *«les informations relatives à l'exercice des tâches se rapportant à toute entité en charge de fonctions publiques, incluant les données d'évaluation respectives, ne seront pas soumises à des garanties de respect de la vie privée»*. L'APD a attiré l'attention du gouvernement sur l'opportunité de déplacer cette disposition au chapitre du code en matière de protection des données personnelles régissant le traitement d'opérations par des organes publics et a également mis en cause sa conformité tant au droit constitutionnel qu'au droit communautaire. En effet, certains éléments d'information et des catégories entières de personnes concernées sont exclus du champ de protection offert par la législation sur les données à caractère personnel.

Les sections 130 et 162 du code en matière de protection des données personnelles ont également été modifiées en 2009 afin de permettre aux entreprises qui avaient créé des bases de données sur la base des informations contenues dans des répertoires téléphoniques publics avant le 1er août 2005 de continuer à utiliser ces données à des fins publicitaires; un registre d'exclusion («opt-out») public a également été introduit et placé sous le contrôle de l'APD. Il convient de rappeler que, le 28 janvier 2010, la Commission européenne a envoyé au gouvernement italien un courrier lui enjoignant de l'informer sur les amendements ci-dessus, car elle estimait que ces derniers violaient les directives 2002/58 et 95/46 – ceci étant la première étape de la procédure d'infraction établie par le droit communautaire.

Par ailleurs, il convient ici de faire référence à la loi 69/2009, qui a introduit diverses exigences favorisant l'informatisation des agences administratives publiques et la publication en ligne de décisions judiciaires. Des dispositions pertinentes en matière de protection des données sont fixées à la section 21 de cette loi, qui oblige les instances administratives publiques à publier les salaires annuels des hauts fonctionnaires/cadres supérieurs, les CV, les adresses électroniques et les numéros de téléphone de bureau sur les sites internet respectifs; à la section 32, par laquelle les exigences applicables à la publication de décisions et d'instruments administratifs sont remplies par la publication de ces décisions et instruments sur les sites des agences concernées; à la section 36, qui vise à accélérer la mise en œuvre du «système de connectivité public» afin de garantir l'«interopérabilité complète des bases de données et des registres de recensement» en vue d'offrir de meilleurs services aux citoyens et d'améliorer l'efficacité de l'administration publique; et à la section 45, qui modifie le code de procédure civile en autorisant également la publication des décisions judiciaires sur les sites internet.

Une autre réglementation importante promulguée en 2009 visait à mettre en œuvre les dispositions du traité de Prüm en créant une base de données ADN nationale et en fixant les mécanismes de procédure pertinents (loi n° 85/2009). La base de données ADN nationale sera créée au sein du ministère de l'intérieur et intégrera les profils ADN obtenus dans le cadre de poursuites judiciaires, ainsi que ceux de personnes disparues et/ou de leurs parents consanguins, de corps et de restes humains non identifiés, et d'individus faisant l'objet de mesures judiciaires restreignant leur liberté. La supervision de cette base de données sera confiée à l'APD italienne. La plupart des suggestions et modifications qu'elle a proposées ont été suivies, en particulier celles visant à garantir le respect de la dignité des personnes et la proportionnalité des opérations de traitement; des garanties additionnelles devront être intégrées par le biais d'une législation secondaire, à adopter après consultation et/ou en accord avec l'APD italienne. Cependant, les recommandations relatives au champ trop large des dispositions sur l'obtention d'échantillons ADN par des moyens coercitifs et aux périodes excessivement lon-

gues de conservation des données n'ont pas été suivies de manière satisfaisante.

**Propositions écrites au Parlement** – Une proposition écrite a été adressée au Parlement en décembre 2009 concernant l'opportunité de voter une législation ad hoc régissant les dispositifs d'alerte professionnelle («*whistleblowing*» ou «lignes éthiques») dans le secteur des entreprises. L'APD a tout particulièrement attiré l'attention sur la nécessité de réguler l'utilisation légale des données à caractère personnel collectées par le biais des rapports de «bonne foi» soumis par des lanceurs d'alerte ainsi que l'accès des personnes concernées à leurs propres données collectées de la sorte.

**Auditions parlementaires** – L'APD a été entendue à plusieurs reprises en 2009 sur des questions de première importance par les commissions parlementaires compétentes, soit dans le cadre d'initiatives d'information, soit lors des débats conduisant à l'adoption de projets de lois affectant la protection des données à caractère personnel. Citons en particulier l'audition du 30 janvier 2009 devant la commission parlementaire pour la sécurité de la République concernant une affaire impliquant la collecte de données à caractère personnel dans le cadre d'une enquête judiciaire et le rôle des experts et consultants désignés par la Cour; l'audition du 15 juillet 2009 devant la commission des affaires constitutionnelles de la Chambre des députés, dans le cadre d'une initiative d'information sur l'informatisation des agences administratives publiques; et l'audition du 25 novembre 2009 devant la commission des finances de la Chambre des députés, dans le cadre d'une initiative d'information sur le crédit à la consommation, axée surtout sur les agences d'évaluation du crédit, la mise en œuvre du code de conduite et de pratique professionnelle pertinent et les projets de loi relatifs à l'usurpation d'identité et aux fraudes en la matière.

## B. Jurisprudence importante

### Écoutes téléphoniques

Le **Conseil d'État** (dernière instance de la Cour des procédures administratives) a statué qu'un fonctionnaire pouvait être légalement démis de ses fonctions sachant que la procédure disciplinaire le concernant reposait sur des transcriptions d'écoutes téléphoniques incluses dans le dossier de la procédure judiciaire instituée à son encontre pour les mêmes motifs, et qui s'était soldée par son acquittement – bien que les transcriptions en question aient été déclarées irrecevables au cours de la procédure judiciaire en raison de leur obtention illégale. Les faits sous-tendant la procédure disciplinaire n'ont pas été contestés. En conséquence, la question de la recevabilité des transcriptions doit être considérée comme non pertinente (décision n° 7703/2009).

La **Cour constitutionnelle** a statué que la destruction de dossiers contenant des transcriptions d'écoutes obtenues illégalement doit toujours se conformer aux règles sur le droit d'être entendu, afin de concilier les exigences de respect de la vie privée et de procès équitable (décision n° 173/2009).

La **Cour de cassation** s'est attelée à la même question en décidant que la destruction des transcriptions d'écoutes doit être ordonnée, à tous les stades et devant toutes les instances de la procédure judiciaire, par la Cour qui les a déclarées irrecevables (en cas de litige quant à leur recevabilité); toutefois, la destruction ne peut jamais intervenir avant le prononcé de la décision judiciaire finale (décision n° 25590/2009).

### Données médicales

*Tests VIH, consentement éclairé, diffusion de données.*

La **Cour de cassation** (division droit civil) a statué que, préalablement à la réalisation de tests VIH, le patient doit être impérativement informé et autorisé à donner son consentement, pour autant qu'il soit capable de prendre une décision libre et informée. Cette exigence ne peut être contournée que si le traitement médical s'avère objectivement urgent et/ou particulièrement nécessaire dans l'intérêt général. L'équipe médicale doit prendre toutes les mesures nécessaires pour garantir la confidentialité et empêcher la diffusion des informations sur les résultats du test et/ou la santé du patient. Dans le cas en question, la diffusion de ces informations avait conduit à la fermeture de l'entreprise du patient, alors que ce dernier aurait subi le test dans un autre hôpital s'il avait été informé de manière appropriée (décision n° 2468/2009).

**Questions diverses**
*Divulgation d'informations sur les membres d'une association professionnelle.* Le **Conseil d'État** a confirmé la décision en vertu de laquelle le conseil d'administration d'une association professionnelle avait divulgué uniquement les informations personnelles qu'elle était autorisée à détenir conformément à une loi spéciale. L'association avait tu les autres informations personnelles demandées par le demandeur – à savoir l'adresse des entreprises des professionnels, les numéros de téléphone et de télécopie, et les adresses électroniques – car ces informations complémentaires avaient été communiquées à l'association sur une base strictement confidentielle (décision n° 7946/2009).

*L'image en tant que «donnée à caractère personnel».* La **Cour de cassation** a statué que l'image d'un particulier, bien que permettant d'identifier cet individu, ne tombait pas automatiquement sous le coup du code en matière de protection des données personnelles; il conviendrait pour cela de faire expressément référence au particulier au moyen d'une légende ou de tout autre moyen (p. ex. une déclaration verbale) permettant son identification. Dans le cas contraire, l'image n'a pas valeur de donnée à caractère personnel (décision n° 12997/2009).

*Documents contenant des données à caractère personnel.* Selon la **Cour de cassation**, la production de documents contenant des données à caractère personnel dans le cadre de poursuites judiciaires est autorisée sans le consentement de la personne concernée si elle s'avère nécessaire à l'exercice d'un droit de défense, quelle que soit la manière dont les données personnelles ont été obtenues; cette position de la Cour est conforme à une décision antérieure de l'APD. Toutefois, le droit de défense exercé en invoquant les données personnelles d'autrui ne peut s'exercer au préjudice des exigences d'équité, de pertinence des données et de proportionnalité formulées dans le code en matière de protection des données (décision n° 3358/2009).

## C. Questions diverses importantes

**Sensibilisation des jeunes et réseaux sociaux**
L'APD italienne a décidé de lancer une initiative ciblant les étudiants à l'occasion de la Journée européenne de la protection des données (le 28 janvier). L'initiative, baptisée «Cinéma et vie privée», a duré quatre jours; il s'agissait de sensibiliser les jeunes à l'importance de la protection des données personnelles dans la société d'aujourd'hui et à la nécessité d'apprendre à protéger sa vie privée. Divers films choisis pour leur pertinence, selon différents points de vue, en matière de protection de la vie privée ont été projetés dans la salle de conférence de l'APD italienne. Chaque film était présenté par l'un des quatre membres du panel collégial de l'APD et accompagné d'une vidéo spécialement conçue par l'APD italienne en vue de décrire – à nouveau à l'aide des films – les intrusions mineures et majeures dans notre sphère privée. Des étudiants d'écoles supérieures romaines ont été invités à la projection, suivie d'un débat et d'un échange de vues.

En outre, l'APD a publié en 2009 une brochure de conseils (ciblant tout particulièrement les jeunes) sur les réseaux sociaux et l'exploitation de leur potentiel en connaissance de cause. La brochure, intitulée «Réseaux sociaux: attention aux effets secondaires», est disponible gratuitement dans la plupart des bureaux de poste italiens. Cette initiative visait à aider les utilisateurs, expérimentés ou novices, à tirer pleinement parti du potentiel de ces outils de communication innovants sans mettre en danger leur vie privée et professionnelle.

**Sécurité des bases de données**
L'APD a procédé à la refonte (le 25 juin 2009) d'une décision datée du 28 novembre 2008 afin d'améliorer les garanties des personnes concernées dans le cadre des activités exercées par des «administrateurs système» – un concept qui n'est en réalité pas expressément défini par la loi italienne. Le nouveau texte entend clarifier différents points, notamment pour tenir compte des questions présentées à l'APD. Les exigences stipulées par l'APD concernent plus spécifiquement la connexion d'accès (des systèmes doivent être mis en place pour se connecter aux systèmes de traitement et aux bases de données électroniques utilisés par les administrateurs système, au moyen par exemple de l'horodatage et de journaux d'événements, sans toutefois enregistrer les activités exécutées par les administrateurs système après leur accès); la supervision par les responsables du traitement de données des activités exercées par les administrateurs système (afin de vérifier leur conformité aux mesures organisationnelles, techniques et de

sécurité stipulées dans la législation sur la protection des données); l'élaboration d'une liste des administrateurs système et de leurs caractéristiques (contenant les informations d'identification des administrateurs système, dont une liste des fonctions qui leur sont assignées), que chaque responsable du traitement de données consignera dans un document interne soumis à l'inspection de l'APD. L'APD a mis en évidence la nécessité de veiller tout particulièrement à l'évaluation de l'expérience, des compétences et de la fiabilité de chaque individu chargé des fonctions d'administrateur système, en particulier pour s'assurer de leur parfaite conformité à la législation sur la protection des données et à leur sécurité.

**Soins de santé et données sensibles**

*Dossiers d'examen en ligne*. L'APD italienne a formulé des orientations concernant l'utilisation de données à caractère personnel en relation avec «l'accès en ligne aux dossiers d'examen». Les lignes directrices visent à établir un cadre unifié spécifique destiné à offrir des garanties aux citoyens, notamment quant au caractère optionnel de l'accès en ligne aux dossiers d'examen. Les personnes concernées doivent pouvoir décider librement d'accéder ou non au service de dossiers d'examen en ligne sur la base d'un avis d'information spécifique et après avoir donné leur consentement *ad hoc* pour le traitement des données à caractère personnel liées au service en question; elles doivent, dans tous les cas, continuer à pouvoir obtenir ces dossiers d'examen sur papier auprès du (des) prestataire(s) de soins de santé individuel(s). Des dispositions techniques spécifiques sont formulées en vue de garantir des mesures de sécurité appropriées: des protocoles de communication sécurisés basés sur des standards de chiffrement pour les transferts de données électroniques, y compris la certification numérique des systèmes livrant des services en réseau; des dispositions adéquates pour empêcher l'obtention des informations contenues dans le dossier électronique si ce dernier est conservé dans des systèmes de cache locaux et/ou centralisés après avoir été consulté en ligne; et une disponibilité à court terme (maximum 45 jours) du dossier d'examen en ligne.

*Lignes directrices sur le dossier de santé électronique et le fichier de santé*. Les lignes directrices suggèrent que le dossier de santé électronique doit être développé en donnant la priorité à des solutions qui n'entraînent pas la duplication des informations médicales créées par les professionnels/organes de soins de santé qui ont traité la personne concernée.

Étant donné que les données et documents médicaux contenus dans le DSE proviennent de différentes sources, il convient de prendre des mesures appropriées afin de pouvoir retrouver les entités responsables de la création et de la collecte des données et de les mentionner dans le DSE (également dans un souci de responsabilité). Étant donné, plus particulièrement, que sont ici en jeu des rapports cliniques distincts, chaque entité qui a créé/élaboré ces rapports doit impérativement rester l'unique responsable de traitement des données desdits rapports.

La personne concernée doit être en mesure de décider librement de la création ou non d'un DSE/FS incluant des informations médicales la concernant; son consentement doit être obtenu sur une base spécifique et distincte; et elle doit pouvoir obtenir des explications pertinentes. Il convient d'envisager également un consentement partiel, limité à un champ spécifique, afin de permettre à la personne concernée d'exprimer ses désirs. Des restrictions spécifiques sont fixées au regard des finalités poursuivies par le DSE/FS, en établissant clairement que le traitement de données à caractère personnel par le biais d'un DSE/FS doit poursuivre l'unique objectif de missions de prévention, de diagnostic et de traitement à l'égard de la personne concernée; par conséquent, le traitement ne peut être confié qu'aux praticiens de soins de santé. Cette approche modulaire permet, par exemple, de sélectionner les informations de soins de santé qui peuvent être traitées par les responsables du traitement de données individuels autorisés à accéder au DSE dans le cadre de leurs missions respectives – p. ex. un réseau d'oncologie constitué d'unités opérationnelles spécialisées dans le traitement du cancer. De même, certaines catégories de praticiens, tels que les pharmaciens, n'ont accès qu'aux données (ou modules de données) indispensables à l'administration des médicaments.

*Transparence publique et publication en ligne de données médicales*. L'APD a ordonné que les informations médicales relatives à plus de 4 500 personnes invalides soient retirées du site d'un institut régional et a également engagé une procédure de sanctions à l'encontre de

l'autorité locale en question. Il a été découvert que la liste des personnes invalides ayant bénéficié d'une allocation régionale en vue d'acheter un ordinateur pouvait être consultée en toute liberté en ligne – cette liste comprenait leur nom, leur invalidité, leur lieu de résidence et leur date de naissance. L'APD a confirmé que les informations de nature médicale ne peuvent être diffusées sans garantie et que les exigences de transparence publique ne peuvent outrepasser les obligations de protection des données applicables aux instances publiques – en particulier, l'obligation de ne pas divulguer des informations excessives dans le cadre des objectifs spécifiques.

*Registre national et régional des implants mammaires*. L'APD s'est opposée à l'élaboration d'un registre reprenant les noms de femmes ayant subi une pose d'implants mammaires, dans le cadre d'un projet de loi gouvernemental relatif à la chirurgie mammaire. L'APD a rappelé que la chirurgie plastique peut tout à fait être contrôlée dans le respect de l'anonymat des patientes opérées, moyennant l'utilisation de codes et outils statistiques. L'APD a insisté sur la nécessité de désigner les personnes autorisées à accéder au registre ainsi que les motifs spécifiques pouvant donner lieu à la consultation du registre, le libellé du projet de loi étant excessivement vague.

**Entreprises**

Fusions et scissions – L'APD a précisé les obligations devant être remplies par les entreprises en cas de fusions (par absorption et/ou amalgamation) et de scissions afin de se conformer à la législation en matière de respect de la vie privée. Les entreprises concernées doivent notamment informer leurs clients, employés et fournisseurs du (des) nom(s) du nouveau responsable du traitement de données et des (de la) personne(s) traitant les données, le cas échéant; à cette fin, des mécanismes simplifiés peuvent être utilisés, comme la publication préalable des informations sur les sites internet des entreprises et, par la suite, la communication d'informations individuelles à leur personnel.

Services d'information d'entreprises – L'APD a exonéré des sociétés fournissant des services d'information d'entreprises de l'obligation de fournir des avis d'information à toutes les personnes concernées, estimant que cette obligation entraînait un effort disproportionné au regard des intérêts en jeu; cependant, l'APD a exigé que les entreprises concernées déploient des mesures alternatives efficaces.

Législation anti-blanchiment et courtiers financiers – L'APD a précisé que les courtiers financiers appartenant au même groupe d'entreprises peuvent légalement communiquer et traiter des données à caractère personnel sans le consentement des personnes concernées, s'agissant de signaler des transactions «suspectes», dans la mesure où cette activité de signalement est conforme à la législation anti-blanchiment et vise exclusivement à contrer le blanchiment d'argent.

Registres de société – L'APD a précisé que le code en matière de protection des données personnelles ne pose aucune restriction à l'accès des actionnaires aux données à caractère personnel contenues dans les registres de société, de même qu'il ne s'oppose pas à la transparence des activités d'entreprise. Les actionnaires ont le droit de connaître les adresses et informations personnelles des autres actionnaires afin de les contacter et de défendre leurs demandes légitimes.

**Communications téléphoniques et électroniques**

*Télémarketing*. La possibilité de réutiliser (jusqu'au 31 décembre 2009) les données contenues dans les répertoires téléphoniques créés avant le 1er août 2005 à des fins commerciales sans le consentement des personnes concernées, introduite par la loi 14/2009 (voir le 12e rapport annuel), avait incité le commissaire à la protection des données (Garante) à clarifier les restrictions s'appliquant à la compilation et à l'utilisation de telles données à travers une décision *ad hoc* (mars 2009). Plus particulièrement, l'APD avait requis, entre autres choses, que les responsables du traitement de données désireux de faire valoir cette disposition prouvent que les données avaient bel et bien été extraites de répertoires téléphoniques datant d'avant le 1er août 2005 et utilisent les données dans le seul objectif de contacter les abonnés à des fins commerciales. En d'autres termes, l'APD interdisait aux sociétés de marketing de contacter ainsi les abonnés dans le but d'obtenir subrepticement leur consentement à l'utilisation de leurs données à des fins commerciales après le 31 décembre 2009. Dans la foulée des amendements apportés au code

en matière de protection des données personnelles par la loi 166/2009 (voir ci-dessus «Développements législatifs»), qui allongent le délai d'utilisation des données en question et prévoient la création d'un registre d'exclusion (***«opt-out»***) applicable au télémarketing pour le 25 mai 2010, l'APD a décidé d'élargir en conséquence la force exécutoire des exigences stipulées dans la décision susmentionnée. Dans cette même note, l'APD a rejeté la pratique consistant à utiliser des numéros de téléphone composés de manière aléatoire pour contacter des abonnés à des fins commerciales, estimant que ces numéros, bien que composés selon des mécanismes aléatoires, constituent bel et bien des données à caractère personnel au sens du décret de loi italien en matière de protection des données personnelles et, en tant que telles, bénéficient de toutes les garanties accordées par la loi – dont l'obligation d'obtenir le consentement éclairé des abonnés avant l'utilisation de leurs données.

*Profilage de clients* – L'APD (en sa décision du 25 juin 2009) a imposé des obligations spécifiques aux fournisseurs de services de communications électroniques accessibles au public portant sur le profilage de leurs clients. Une analyse détaillée a conduit à une distinction des différentes catégories de profilage, obligeant les responsables du traitement de données à prévoir différents mécanismes. Plus précisément, deux scénarios ont été envisagés: 1. le profilage basé sur des informations personnelles «identifiables», qui nécessite le consentement libre, éclairé et spécifique des personnes concernées; 2. le profilage basé sur des informations personnelles «agrégées», c.-à-d. des données générales déduites des informations personnelles identifiables, qui nécessite soit le consentement de la personne concernée, soit, lorsque ce consentement n'a pas été obtenu, une demande de vérification préalable à soumettre à l'APD par le responsable du traitement de données, conformément à la section 17 du code en matière de protection des données personnelles. Dans ce dernier cas, le niveau d'agrégation (c.-à-d. le niveau de détail des données agrégées) et les modalités techniques applicables au traitement devront être pris en compte. D'autres obligations ont également été imposées, telles que la notification à l'APD et la communication d'informations appropriées aux personnes concernées.

**Journalisme**

À diverses occasions, l'APD a dû intervenir pour garantir le respect de la vie privée d'enfants. Dans le cas en question, des journaux se sont vu interdire de publier les noms et images d'enfants impliqués dans certaines affaires et/ou de fournir des informations susceptibles de les identifier. Dans les cas d'abus d'enfant, l'APD a rappelé la nécessité de protéger la vie privée à la fois des enfants et/ou des autres individus impliqués, en s'abstenant de divulguer l'âge, le sexe et le lieu de résidence des enfants; la relation, le cas échéant, entre l'enfant et le suspect; ou l'emploi ou la profession du père.

L'APD a été saisie de plusieurs demandes d'effacement de données et images disponibles sur internet (par exemple via Google, Emule, YouTube, des forums et des blogs). Dans certains cas, l'APD n'était pas en mesure d'entreprendre des démarches directes, car le responsable du contenu du site internet ne résidait pas en Italie; à l'inverse, dans d'autres cas, le responsable du traitement de données a reçu l'instruction d'effacer les images/données jugées contraires à la loi.

Deux dossiers traités par l'APD concernaient des journaux et des chaînes télévisées qui avaient publié des images tirées directement de Facebook pour commenter la mort de deux individus, alors que ces photos n'étaient pas celles des individus décédés, mais d'homonymes. L'APD a jugé que la publication de ces images violait la législation sur la protection des données, en raison de l'absence de vérification des informations collectées et de la diffusion d'informations personnelles erronées. Il convient de mentionner le nombre croissant de plaintes relatives au traitement de données à caractère personnel extraites des profils Facebook; ces plaintes dénoncent majoritairement un usage abusif des informations personnelles et des faits de diffamation.

Une autre décision importante en la matière a réaffirmé l'illégalité de l'enregistrement et de l'utilisation d'images d'individus dans un cadre privé, sans le consentement des individus en question. L'APD a interdit la diffusion/publication, par n'importe quelle partie, d'images acquises et/ou obtenues en violation des garanties applicables aux lieux privés, eu égard notamment aux techniques intrusives développées pour capturer ces images, à l'absence de consentement des personnes

concernées et au caractère exclusivement personnel des activités montrées dans ces images.

**Plaintes officielles**

En 2009, 360 décisions ont été rendues à la suite de plaintes officielles (régies spécifiquement). À l'instar des années précédentes, la plupart d'entre elles concernaient des banques, des organismes financiers et des agences d'évaluation du crédit. Cependant, les questions les plus intéressantes avaient trait à la voix en tant que donnée personnelle, à l'exercice des droits relatifs à la protection des données de personnes décédées et à la diffusion sur internet d'informations accessibles publiquement.

*La voix en tant que donnée à caractère personnel.* L'APD s'est penchée sur la plainte d'un consommateur à l'encontre d'un opérateur téléphonique qui avait ouvert un contrat sur la base d'un «ordre verbal». Selon l'APD, l'enregistrement de l'appel doit être mis à la disposition de la personne concernée qui le demande; la remise d'une transcription synthétique du contenu concerné ne suffit pas. Les droits énoncés dans la législation sur la protection des données peuvent aussi être exercés par les personnes concernées dans le cadre de données audio et vidéo, lesquelles sont des données à caractère personnel; en conséquence, le droit d'accès aux données personnelles contenues dans l'«ordre verbal» implique de transmettre l'enregistrement de l'appel de manière à permettre l'accès à la donnée vocale spécifique.

*Dossiers cliniques d'une personne décédée.* L'APD a traité la plainte déposée à l'encontre d'un hôpital universitaire qui avait omis de répondre à plusieurs demandes d'informations personnelles relatives aux traitements subis par le conjoint du plaignant. L'APD a estimé que le conjoint d'une personne décédée a le droit de consulter le dossier clinique de la personne afin d'établir l'opportunité d'un recours judiciaire contre les prestataires de soins. En vertu de la section 9(3) du code en matière de protection des données personnelles, le droit d'accès aux données à caractère personnel relatives à une personne décédée «peut être exercé par toute entité y voyant un intérêt ou agissant dans le but de protéger la personne concernée ou pour des raisons familiales méritant une protection» – et le plaignant avait précisé que les données en question étaient nécessaires pour engager une action juridique dans le but d'établir la conduite défaillante et/ou négligente des prestataires de soins.

*Publication en ligne des résolutions par un organe municipal.* L'APD a ordonné à une municipalité d'effacer l'adresse du plaignant dans une résolution qui avait été publiée sur le site internet de la municipalité et pouvait être extraite au moyen de moteurs de recherche externes. Le plaignant faisait valoir que le «masquage» de son adresse dans la résolution ne portait pas ombrage à la transparence des instruments et rapports publics publiés par voie électronique. L'APD a souligné la nécessité de sélectionner rigoureusement les données personnelles à publier de la sorte, leur publication devant se justifier au regard des circonstances spécifiques aux fins poursuivies par la mesure donnée, conformément aux principes de pertinence et de proportionnalité et dans le respect de l'équilibre entre le droit à la vie privée et l'obligation de garantir la publicité des décisions prises par un pouvoir local. Totalement disproportionnée, la publication de la résolution en question a eu une incidence sur les droits du plaignant en ce sens qu'elle a mené à la diffusion d'informations non pertinentes sur internet.

**Inspections**

L'APD n'a pas non plus lésiné sur ses activités d'inspection en 2009. Un total de 449 inspections a été effectué en six mois d'activité. Dans le cadre de ces inspections, l'APD peut faire appel à un corps spécialisé au sein de la police financière, chargé de vérifier le respect des exigences en matière de notification, d'avis d'information, de mesures de sécurité et d'application des résolutions adoptées par le Garante. Quarante-cinq inspections ont été menées directement par le service d'inspection de l'APD. Ces inspections concernaient en particulier les organes publics ayant accès au système d'information du fisc (13); les entreprises fournissant des bases de données à des tiers à des fins commerciales (10); et les opérateurs de téléphonie concernant la conservation des données de trafic à des fins de profilage de clients (9). Quant aux contrôles menés par la police financière sur les instructions de l'APD (qui spécifient le responsable du traitement de données et le champ de l'inspection), ils couvraient les domaines suivants: hôpitaux privés (35); hôpitaux publics et maisons de santé (35); sociétés de transport public (30); sociétés de recrutement (26); fournisseurs de matériaux de construction (25); clubs

de golf (25); sociétés sous tutelle municipale actives dans la collecte des déchets (20); sociétés vendant du méthane (20); compagnies d'eau (20); complexes touristiques (20); bureaux de pari (15); sociétés de télésiège (10); entreprises de vente de matériel électronique (10); pharmacies (20); sociétés enregistrant l'utilisation de bases de données sur la solvabilité (20); autres entités suivant les requêtes spécifiques des services juridiques de l'APD (83).

À la suite des contrôles, 43 rapports ont été transmis aux autorités judiciaires et 368 procédures de sanctions administratives ont été ouvertes; en outre, dans environ 150 cas, les services juridiques *ad hoc* de l'APD ont reçu des propositions contraignant les responsables de traitement de données à aligner leurs opérations de traitement sur la loi.

170 procédures de sanctions ont été finalisées en 2009 et un total de 1 572 432 euros d'amendes a été infligé.

Quant aux affaires pénales, plusieurs concernaient l'omission de prendre des mesures de sécurité minimales (24). De surcroît, des cas d'opérations de traitement de données illégales (7), de communication de fausses déclarations et informations à l'APD (6) et de non-conformité aux ordres/mesures formulés par l'APD (4) ont été mis à jour.



## 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 et dont les derniers amendements s'appliquent depuis le 1er juillet 2009. La loi sur la protection des données a été modifiée le 12 juin 2009. Les principaux changements portaient sur les exceptions à la notification du traitement des données à caractère personnel à l'Inspection nationale des données et à l'obligation de soumettre une demande au responsable du traitement de données en cas d'éventuelle violation de la loi sur la protection des données à caractère personnel avant de déposer plainte auprès de l'Inspection nationale des données. Les amendements stipulent également que l'Inspection nationale des données n'accréditera plus les auditeurs internes et externes du traitement de données.

En outre, les avant-projets de deux nouveaux amendements à la loi sur la protection des données à caractère personnel ont été rédigés:

- concernant l'exception à la conclusion d'un accord sur les transferts de données à destination de pays tiers sur le plan répressif dans le cadre de la coopération internationale en matière de sécurité nationale et dans le domaine du droit pénal;
- concernant les décisions de l'Inspection nationale des données prévoyant l'interception ou l'interruption du traitement de données, l'amendement stipulant que les décisions ne peuvent être annulées dans le cas d'une décision d'appel.

**Loi sur l'Inspection nationale des données**
Afin de garantir la totale indépendance de l'Inspection nationale des données de Lettonie, un projet de loi a été élaboré à cet égard. Compte tenu de la nécessité de revoir 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 en 2009. La publication de la loi est suspendue jusqu'à l'arrêt de la Cour de justice de l'Union européenne sur l'indépendance de l'autorité allemande de protection des données.

**Réglementation relative au transfert de données à destination de pays tiers**
En 2009, l'Inspection nationale des données de Lettonie a poursuivi ses activités liées à la rédaction des règlements du cabinet des ministres définissant des normes contractuelles types pour les transferts de données personnelles à des pays tiers. Ces règlements mettent 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 types pour le transfert de données à caractère personnel. Les règlements seront publiés après l'amendement de l'article 28 de la loi sur la protection des données à caractère personnel. L'amendement a déjà été rédigé et envoyé au Parlement.

**Réglementation relative aux exigences associées au rapport d'audit sur le traitement des données à caractère personnel dans les institutions gouvernementales locales et nationales**
Les coupes budgétaires et la réduction des fonctions et pouvoirs administratifs de l'Inspection nationale des données ont donné lieu aux amendements de la loi sur la protection des données à caractère personnel, entrés en vigueur le 1er juillet 2009. En vertu de ces amendements, l'accréditation des auditeurs du traitement des données à caractère personnel n'est plus essentielle. En lieu et place, les exigences associées aux rapports d'audit sont déterminées sur la base des règlements du cabinet des ministres. En 2009, l'Inspection nationale des données a élaboré le règlement du cabinet des ministres (17 novembre 2009 n° 1322) intitulé «Exigences associées au rapport d'audit sur le traitement des données à caractère personnel dans les institutions gouvernementales locales et nationales», entré en vigueur le 25 novembre 2009. La réglementation spécifie que le contenu des rapports d'audit sur le traitement des données à caractère personnel dans les institutions gouvernementales locales et nationales doit être soumis à l'Inspection nationale des données tous les deux ans, accompagné d'une analyse de risques du traitement des données à caractère personnel, d'une évaluation de la conformité aux actes juridiques relatifs au traitement des données à caractère personnel pour

chacune des finalités du traitement des données, de conclusions comprenant les estimations de risques, et de recommandations d'amélioration.

**Loi sur la liberté d'information**
Suite aux amendements de la loi sur le budget national pour 2009, qui taillent considérablement dans le budget de l'Inspection nationale des données, cette dernière a amendé la loi sur la liberté d'information, établissant que le contrôle de cette loi ne relève plus des compétences de l'Inspection nationale des données depuis le 1er juillet 2010.

**Loi sur les services de la société de l'information**
Suite aux amendements de la loi sur le budget national pour 2009, qui taillent dans le budget de l'Inspection nationale des données, cette dernière a amendé la loi sur les services de la société de l'information. Les amendements établissent que l'Inspection nationale des données est tenue d'ouvrir une enquête lorsqu'une personne a reçu dix communications commerciales d'un même expéditeur en l'espace d'un an; ils n'excluent cependant pas les enquêtes menées d'initiative par l'Inspection.

**Réglementations relatives 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 de communications électroniques accessibles au public ou de réseaux publics de communication par les fournisseurs de services de communications électroniques, conformément à l'article 19 de la loi sur les communications électroniques et à l'article 10 de la directive 2006/24/CE *sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE*. Le règlement du cabinet des ministres de Lettonie (n° 820, du 4 décembre 2007), intitulé «Ordonnance relative 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 périodes de temps pendant lesquels les fournisseurs sont tenus de conserver les données statistiques et de les soumettre à l'Inspection nationale des données. L'année 2008 a été la première au cours de laquelle l'Inspection a compilé les statistiques.

Conformément à l'article 4 de la loi sur les communications électroniques, la protection des données à caractère personnel dans le secteur des communications électroniques est supervisée par l'Inspection nationale des données. En 2009, l'Inspection nationale des données s'est heurtée au problème des différences d'interprétation de la législation sur les droits d'accès de l'Inspection nationale des données aux données conservées. Face à la nécessité de résoudre ce problème, l'Inspection nationale des données a formulé un amendement de la loi sur les communications électroniques, qui devrait entrer en vigueur en 2010.

## B. Jurisprudence importante

En 2009, l'Inspection nationale des données a reçu 140 plaintes. La plupart portaient sur un traitement des données personnelles sans base légale ou sur un traitement des données dépassant le cadre déclaré (dans 20 cas, le plaignant a reçu des instructions de l'Inspection nationale des données sur la manière de résoudre la violation de la protection des données en passant par le responsable du traitement directement). Suite aux contrôles réalisés par l'Inspection nationale des données, l'infraction à la loi sur la protection des données à caractère personnel a été confirmée dans 58 cas. À cet égard, des avertissements ont été émis dans 29 cas, soit 50 % des violations administratives signalées. Ce pourcentage est en augmentation par rapport aux années précédentes. En 2008, des avertissements ont été émis dans 18 % des cas, et dans 10 % en 2007. Dix-huit dossiers supplémentaires ont été ouverts par l'Inspection nationale des données. Le montant total

des amendes infligées par l'Inspection nationale des données s'élève à 23 800 lats (environ 34 000 euros). 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 proportionnalité dans le traitement des données.

Les infractions les plus courantes au traitement de données personnelles avaient trait:
- à la publication de données personnelles sur internet,
- au traitement de données par des agences de notation et au transfert de données à des tiers,
- à l'utilisation de données personnelles par autrui à des fins d'identification en cas d'infractions administratives,
- à la vidéosurveillance,
- au traitement de données effectué par les services d'entretien domestique.

Un cas spécifique a attiré l'attention des médias: celui de la vidéosurveillance couvrant la zone des cabines d'essayage d'une grande chaîne de supermarchés. En 2009, le nombre de cas d'usurpation de données personnelles constatés à la suite d'un contrôle d'identité policier a augmenté.

## C. Questions diverses importantes

Les débats auxquels l'Inspection nationale des données a pris part au niveau national portaient sur les questions suivantes:
- les amendements de textes juridiques relatifs aux coupes budgétaires (dont la réduction des fonctions et pouvoirs administratifs de l'Inspection nationale des données);
- le traitement de données dans les systèmes nationaux à des fins éducatives;
- l'utilisation de scanners corporels dans les prisons;
- la publication des décisions de justice et l'anonymisation des données;
- le traitement des données relatives au crédit à la consommation et au recouvrement de créances; et
- l'accès aux bases de données durant la souscription d'une assurance automobile (systèmes de souscription en ligne).

**Cas particuliers** (liés aux principaux motifs de plaintes):
1. Une part significative des plaintes reçues avait trait à la publication de données personnelles sur internet sans le consentement de la personne concernée. L'Inspection nationale des données a arrêté des décisions concernant des dérogations relatives au traitement des données opérées sans base légale.
2. Une grande part des plaintes reçues avait trait aux cotes de crédit et au transfert des données personnelles de débiteurs à des tiers en vue du recouvrement des créances. Les violations se rapportent à l'absence du consentement des personnes concernées. Dans la plupart des cas, ces transferts sont considérés comme un traitement de données sans base légale et sortant du cadre autorisé.
3. Vidéosurveillance sans base légale ou traitement extensif de données de vidéosurveillance: la vidéosurveillance est généralement considérée comme un traitement de données personnelles excessif ou comme un traitement de données sans base légale et sortant du cadre autorisé.

Les représentants de l'Inspection nationale des données ont participé à sept ateliers de conférences sur la protection des données, la problématique des pourriels et le marketing direct. Les groupes cibles étaient les commerçants, le personnel administratif des conseils municipaux et de plusieurs grandes entreprises, les enseignants et travailleurs sociaux en milieu scolaire, et enfin les étudiants et élèves.

**Agents de protection des données**

En 2009, l'Inspection nationale des données de Lettonie a organisé quatre examens d'agents de protection des données et certifié dix-sept agents, issus tant du secteur privé que gouvernemental. En 2009, la formation des agents de protection des données a été confiée au secteur privé.

**Recommandations et directives élaborées**

En 2009, l'Inspection nationale des données a élaboré la «recommandation sur le transfert de données à destination de pays tiers». Compte tenu du nombre de demandes de précision reçues par l'Inspection nationale des données concernant l'article 28 de la loi sur la protection des données à caractère personnel régissant le transfert de données à destination de pays

tiers, l'Inspection nationale des données a jugé utile de formuler une recommandation en la matière.

Afin de clarifier la procédure de notification de traitement de données à caractère personnel auprès de l'Inspection nationale des données, des directives ont été élaborées à l'attention des responsables du traitement de données, tenant compte des récents amendements à la loi sur la protection des données à caractère personnel pour ce qui concerne les exceptions de notification.

**Journée 2009 de la protection des données**

À l'occasion de la Journée 2009 de la protection des données, l'Inspection nationale des données a mené des activités concernant la protection des données à caractère personnel dans le cadre de la photographie et du traitement de données personnelles par les photographes (amateurs et professionnels). Les associations de photographes lettones ont débattu de la question et un représentant de l'Inspection nationale des données a participé à un séminaire pour photographes dans le cadre duquel se tenait une conférence/atelier sur la responsabilité juridique des photographes. Au centre des discussions, notamment, la question de savoir comment garantir le respect de la vie privée dans le travail quotidien des photographes. L'Inspection nationale des données a soumis aux photographes des directives sur la protection des données à caractère personnel.



## Lituanie

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

- La loi modifiant la loi relative à la protection juridique des données à caractère personnel est entrée en vigueur le 1er janvier 2009.

  Le nouveau libellé définit les dispositions de la loi sur la protection juridique des données à caractère personnel régissant le traitement des codes d'identification personnels. Selon le nouveau libellé, les responsables du traitement de données employant des outils automatisés pour traiter des données personnelles de nature sanitaire 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 protection des données et demander un contrôle préalable. En outre, 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 ou unités responsables de la protection des données et à la procédure de gestion des plaintes. Le nouveau libellé de la loi sur la protection juridique des données à caractère personnel établit l'indépendance de l'Inspection publique de protection des données en tant qu'institution de contrôle et accorde un mandat de cinq ans au directeur de l'Inspection.

  Bien que la nouvelle loi sur la protection juridique des données à caractère personnel ne soit entrée en vigueur que le 1er janvier 2009, un nouvel avant-projet de loi visant à la modifier est en préparation. Cet avant-projet porte sur des amendements relatifs au statut juridique/à l'indépendance de l'Inspection publique de protection des données et au traitement de données à caractère personnel utilisées à des fins d'évaluation de la solvabilité.

- Les amendements à la loi sur les communications électroniques transposant 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, sont entrés en vigueur le 16 mars 2009.

  La loi stipule que les données de trafic de l'abonné ou de l'utilisateur enregistré de services de communications électroniques peuvent être stockées 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 recouvrement de créances, dans les cas prévus à l'article 77, paragraphe 2, de cette loi. Afin de garantir un accès aux données en cas d'infractions graves et très graves, lorsque de tels renseignements sont nécessaires à des fins d'investigation, de détection et de poursuite des actes criminels au sens du Code pénal de la République de Lituanie, les fournisseurs de réseaux de communications publics et/ou de services de communications électroniques publics doivent stocker leurs données de trafic 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 de communications publics et/ou de services de communications électroniques publics lors de la fourniture des services appropriés.

  Si les données susmentionnées sont nécessaires aux entités effectuant des activités opérationnelles, aux institutions chargées de l'instruction, aux tribunaux ou aux juges pour empêcher, investiguer et détecter des actes criminels, les institutions habilitées par le gouvernement (à savoir les fournisseurs de réseaux et/ou de services de communications électroniques) doivent, à la demande des entités effectuant des activités opérationnelles, 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).

L'Inspection publique de protection des données est chargée de contrôler la mise en œuvre des dispositions du chapitre 9 de la loi sur les communications électroniques, qui couvre aussi les dispositions transposant la directive 2006/24/CE.

- Une ordonnance du gouvernement modifiant l'ordonnance du gouvernement n° 788 «sur l'octroi d'une autorisation de mise en œuvre de la loi sur les communications électroniques» a été adoptée le 22 juillet 2009. L'Inspection publique de protection des données a été désignée responsable de la collecte et de la remise à la Commission européenne de statistiques 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, conformément à l'article 10 de la directive 2006/24/CE.
- L'ordonnance du gouvernement n° 789 «sur l'approbation des procédures relatives à la fourniture des données statistiques prévues à l'article 70 de la loi sur les communications électroniques» a été adoptée le 22 juillet 2009. Cette ordonnance décrit les procédures que doivent suivre les institutions chargées de l'application de la loi pour fournir les données de trafic visées à l'article 10 de la directive 2006/24/CE à l'Inspection publique de protection des données et que doit ensuite suivre cette dernière pour les transférer à la Commission européenne.

## B. Jurisprudence importante

### Définition des données à caractère personnel

L'Inspection publique de protection des données a ouvert un dossier d'infraction administrative à l'encontre d'une entreprise qui avait collecté les données à caractère personnel (noms complets et adresses) d'une autre entreprise et les avait utilisées pour envoyer des offres de changement de contrat aux personnes concernées. L'Inspection publique de protection des données a jugé que le traitement de ces données était sans fondement légal.

Un tribunal du district de Kaunas a arrêté que la définition des données à caractère personnel visée à l'article 2, paragraphe 1, de la loi sur la protection juridique des données à caractère personnel ne couvre pas le nom, le prénom et l'adresse des personnes physiques et, partant, ne régit pas la protection juridique de ces données.

Appel a été interjeté devant la Cour administrative suprême de Lituanie contre la décision du tribunal du district de Kaunas. La Cour administrative suprême a déclaré que, conformément à l'article 2, paragraphe 1, de la loi sur la protection juridique des données à caractère personnel, il faut entendre par donnée à caractère personnel toute information concernant une personne physique ou la personne concernée, identifiée ou identifiable directement ou indirectement par la référence à des données telles qu'un numéro d'identification personnel ou un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. L'article 2, alinéa a, de la directive 95/46/CE présente par ailleurs une définition allant dans le même sens. Compte tenu de ces définitions, le nom, le prénom et l'adresse doivent être assimilés à des données à caractère personnel en ce sens qu'ils permettent d'identifier un individu. La Cour administrative suprême a également relevé que la Cour de justice de l'Union européenne assimile ces données à des données à caractère personnel (décision du 6 novembre 2003, affaire C-101/2001).

### Droits des personnes concernées

L'Inspection publique de protection des données a été saisie d'une plainte concernant la collecte des données personnelles d'un plaignant à partir du registre des biens immobiliers. L'Inspection publique de protection des données a jugé que le critère déterminant la légalité d'un traitement de données personnelles était l'article 5, paragraphe 1, alinéa 6, de la loi sur la protection juridique des données à caractère personnel (des données à caractère personnel peuvent être traitées si ce traitement s'impose aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers à qui les données personnelles ont été divulguées, sauf si les intérêts de la personne concernée l'emportent sur les intérêts de ce responsable du traitement ou tiers). Bien que tenu à l'obligation d'informer le plaignant des droits des personnes concernées, le responsable du traitement de

données (en l'occurrence une banque) n'en a rien fait. Le responsable du traitement n'a donc pas informé le plaignant de son droit d'accès à ses données personnelles dans le registre des biens immobiliers, ni de son droit d'opposition au traitement de ses données personnelles. Par conséquent, l'Inspection publique de protection des données a ordonné au responsable du traitement de veiller à l'avenir à la bonne application de l'article 18, paragraphe 2, alinéas 2 et 3 (le droit d'être informé du traitement de ses données personnelles), et de l'article 21, paragraphe 1 (le droit de s'opposer au traitement de ses données personnelles), de la loi sur la protection juridique des données à caractère personnel (version en vigueur jusqu'au 31 décembre 2008).

Le responsable du traitement de données a fait appel de l'instruction de l'Inspection publique de protection des données sur la base de l'exception visée à l'article 17, paragraphe 2, alinéa 5, de la loi sur la protection juridique des données à caractère personnel (alinéa en vertu duquel le responsable du traitement de données doit fournir à la personne concernée les conditions présidant à l'exercice des droits stipulés dans ledit article, exception faite des cas visés légalement qui nécessitent de garantir la protection des droits et libertés de la personne concernée ou d'autres particuliers).

Le tribunal administratif du district de Vilnius a jugé illogique la position de l'Inspection publique de protection des données selon laquelle le traitement des données personnelles est légal tout en établissant la violation de l'article 18, paragraphe 2, alinéas 2 et 3, de la loi sur la protection juridique des données à caractère personnel (version en vigueur jusqu'au 31 décembre 2008). En reconnaissant que le responsable du traitement de données poursuivait des intérêts légitimes dans le traitement des données personnelles et que ces intérêts n'étaient pas outrepassés par les intérêts de la personne concernée, l'Inspection publique de protection des données ne tient pas compte de l'obligation du responsable du traitement de données d'informer la personne concernée du traitement de ses données personnelles. En vertu de l'article 17, paragraphe 2, alinéa 5, de la loi sur la protection juridique des données à caractère personnel, le responsable du traitement de données doit informer la personne concernée des conditions relatives aux droits de cette dernière fixées dans ledit article, **à l'exception des cas** visés légalement qui nécessitent de garantir la protection des droits et libertés de la personne concernée ou d'autres particuliers. Le tribunal administratif du district de Vilnius a conclu que les faits déterminés justifient l'intérêt légitime du responsable du traitement de données et sont conformes à l'article 17, paragraphe 2, alinéa 5 de la loi sur la protection juridique des données à caractère personnel. En foi de quoi, l'instruction de l'Inspection publique de protection des données a été révoquée.

Un appel a été interjeté devant la Cour administrative suprême de Lituanie contre la décision du tribunal administratif du district de Vilnius. La Cour administrative suprême a confirmé l'argument de l'Inspection publique de protection des données selon lequel une décision qui reconnaît la conformité d'un traitement de données personnelles avec l'article 5 de la loi sur la protection juridique des données à caractère personnel (critère déterminant la légalité d'un traitement de données à caractère personnel) ne signifie pas que ledit traitement soit conforme à toutes les procédures visées dans ladite loi. En conséquence, la décision du tribunal de première instance, selon laquelle les dispositions régissant les droits des personnes concernées n'avaient pas été violées, car l'Inspection publique de protection des données avait conclu à la légalité du traitement de données à caractère personnel, n'est pas fondée juridiquement.

En vertu de l'article 17, paragraphe 2, alinéa 5, de la loi sur la protection juridique des données à caractère personnel, le responsable du traitement de données doit informer la personne concernée des conditions relatives aux droits de cette dernière fixées dans ledit article, à l'exception des cas **visés légalement** qui nécessitent de garantir la protection des droits et libertés de la personne concernée ou d'autres particuliers. En conséquence, le droit du responsable du traitement de données de ne pas informer la personne concernée des conditions d'exercice de ses droits doit s'accompagner de deux conditions: (1) ce droit du responsable du traitement de données doit être stipulé légalement, et (2) ces actions doivent être nécessaires pour garantir la protection des droits et libertés de la personne concernée ou d'autres particuliers. En d'autres termes, il ne suffit pas au responsable du traitement de données de vouloir appliquer cette exception uniquement pour essayer de

garantir la protection des droits et libertés des personnes concernées: ce droit du responsable du traitement de données doit, de surcroît, être exercé sur la base d'un instrument légal. Le tribunal de première instance ne pouvait se prononcer en faveur de l'application de cette exception sans indiquer l'autre acte juridique certain du fait que l'article 17, paragraphe 2, alinéa 5 de la loi sur la protection juridique des données à caractère personnel est une disposition juridique à valeur de directive.

La Cour administrative suprême de Lituanie a par ailleurs arrêté que le responsable du traitement de données n'a pas mentionné cette exception à l'Inspection publique de protection des données au moment de fournir par écrit toutes ses explications au stade de l'enquête relative à la plainte, et les arguments fournis tardivement concernant l'application de l'exception peuvent donc être assimilés à une tentative de fuir ses responsabilités.

## C. Questions diverses importantes

**Activité préventive**

Le chapitre trois de la loi sur la protection juridique des données à caractère personnel régit la vidéosurveillance. L'Inspection publique de protection des données a mené des contrôles dans 92 stations-service en vue de cerner dans quelle mesure les droits des personnes concernées sont garantis dans le cadre du traitement des images.

Sur les 92 stations-service contrôlées, 33 n'avaient pas recours à la vidéosurveillance et 57 enfreignaient la loi sur la protection juridique des données à caractère personnel.

En vertu de l'article 31 de la loi sur la protection juridique des données à caractère personnel, les données personnelles ne peuvent être traitées au moyen d'outils automatisés que si le responsable du traitement ou son représentant en informe l'Inspection publique de protection des données. Or, cette dernière n'avait été informée de la présence de systèmes de vidéosurveillance que pour deux des stations-service contrôlées. Cinquante-cinq autres stations procédaient au traitement d'images sans en avoir informé l'Inspection publique de protection des données (11 stations sur ces 55 en ont informé l'Inspection publique de protection des données au cours des contrôles).

Il a été découvert que les stations-service ne garantissaient pas comme il se doit le droit des personnes concernées à être informées du traitement de leurs données personnelles. Quarante-sept stations-service informaient les personnes concernées de la présence de systèmes de vidéosurveillance par des signaux d'information spécifiques, mais ne fournissaient pas d'informations concernant le responsable du traitement de données et ses conditions, comme le stipule l'article 20, paragraphe 1, de la loi sur la protection juridique des données à caractère personnel. Vingt-sept stations-service avaient mis en place des panneaux d'information sur la présence de systèmes de vidéosurveillance, mais à une distance inappropriée: les personnes concernées prenaient conscience de la vidéosurveillance une fois à l'intérieur de la zone concernée.

En vertu de l'article 20, paragraphe 3, de la loi sur la protection juridique des données à caractère personnel, si des systèmes de vidéosurveillance sont utilisés sur le lieu de travail et dans les locaux ou zones où travaille le personnel du responsable du traitement de données, ce personnel doit être informé par écrit du traitement des images, conformément à la procédure fixée à l'article 24, paragraphe 1, de cette loi. Or, seules 31 stations-service avaient informé par écrit leur personnel du traitement des images.

Trente-sept stations-service respectaient bel et bien le droit des personnes concernées à consulter leurs données personnelles et à être informées du mode de traitement, mais 15 d'entre elles demandaient aux personnes concernées de leur fournir une demande motivée, bien que l'article 25 de la loi sur la protection juridique des données à caractère personnel stipule que les personnes concernées bénéficient d'un droit d'accès moyennant la soumission au responsable du traitement de données d'une pièce d'identité personnelle et d'une demande écrite, sans nécessité de la motiver.

En vertu de l'article 18, paragraphe 1, de la loi sur la protection juridique des données à caractère personnel, le traitement d'images doit faire l'objet d'un document écrit dans lequel le responsable du traitement de

données précise la finalité et la portée de la vidéosurveillance, la période de conservation des données vidéo, les conditions d'accès aux images traitées, les conditions et la procédure de destruction de ces données et d'autres exigences concernant le traitement légitime des données vidéo. En l'occurrence, 25 stations-service ne possédaient pas ce document. Vingt-huit en avaient un, sans toutefois respecter les dispositions de l'article 18, paragraphe 1, de la loi sur la protection juridique des données à caractère personnel.

Les stations-service contrôlées ont reçu des instructions concernant les violations de la loi sur la protection juridique des données à caractère personnel.

**Sensibilisation du public**

*Journée européenne de la protection des données*

La Journée européenne de la protection des données a été célébrée les 28 et 29 janvier 2009. Le 28 janvier 2009, une réunion a rassemblé des représentants d'autres organisations et agences publiques pour s'atteler à la résolution de diverses questions liées à la protection des données à caractère personnel. Les représentants du secteur public ont été informés de la récente célébration de la Journée de la protection des données en Europe, de sa mission, des questions d'actualité et d'un aperçu des activités de l'Inspection publique de protection des données.

Une e-conférence a été organisée dans le cadre du projet «Mano teisės» («Mes droits») du Centre des droits de l'homme. Les réponses aux questions relatives à la protection des données à caractère personnel posées au directeur de l'Inspection publique de protection des données, Algirdas Kunčinas, concernant les lieux de travail électroniques, la vidéosurveillance, le marketing direct, les documents éliminés, la compétence de l'Inspection publique de protection des données et les sanctions infligées pour divulgation illégale de données personnelles, ont été publiées sur le site internet.

Ensuite, l'Inspection publique de protection des données a célébré la Journée européenne de la protection des données le 29 janvier 2009 en compagnie d'un groupe de bibliothécaires, à la bibliothèque publique Adomas Mickevičius du comté de Vilnius.

La conférence a traité de questions sensibles auxquelles sont confrontés les bibliothécaires en matière de protection des données à caractère personnel, entre autres. La manifestation a permis d'exposer aux représentants des bibliothèques les questions prédominantes liées à la protection des données à caractère personnel dans un plus vaste contexte, en insistant sur la sensibilisation dans le domaine de la protection de la vie privée. Une heure avant le début de la conférence, les juristes de l'Inspection publique de protection des données ont donné, aux bibliothécaires et aux lecteurs, des conseils juridiques sur les questions relatives au traitement des données à caractère personnel et au respect de la vie privée.

Divers prospectus et brochures d'information consacrés au thème de la journée ont été publiés et distribués: «Connaissez-vous vos droits quant au traitement de vos données à caractère personnel?», «Protection des données à caractère personnel et vidéosurveillance» ou encore «Protection des données à caractère personnel des utilisateurs de réseaux sans fil».

*Conférence sur la «Protection de la vie privée et des données à caractère personnel en Lituanie»*

L'Inspection publique de protection des données, en partenariat avec une société par actions, «Expozona», a organisé le 26 novembre 2009 une conférence sur la «Protection de la vie privée et des données à caractère personnel en Lituanie». Cette conférence avait pour but d'initier des représentants des secteurs public et privé aux questions de respect de la vie privée et de protection des données, plus précisément sous les aspects de la vie privée, du recouvrement des créances et de la vidéosurveillance sur le lieu de travail. Parmi les participants, citons des intervenants issus de l'Inspection publique de protection des données, de compagnies d'électricité (UAB *«Réseaux de distribution orientaux»*), de sociétés de recouvrement de créances à titre préventif (UAB «Ekskomisarų biuras») et de l'administration municipale de Vilnius. Sept présentations ont développé les sujets suivants:

- Nous dirigeons-nous vers une société digne de la trame de 1984? (vie privée et publicité dans la société de l'information: tendances et menaces);
- Un employé a aussi droit au respect de sa vie privée;

- Le traitement des données à caractère personnel: comment peut-il contribuer à développer les relations avec les clients?
- Le traitement des données à caractère personnel et les problèmes rencontrés dans le cadre du recouvrement de créances à titre préventif;
- La réglementation de la vidéosurveillance;
- Exigences générales des mesures techniques et organisationnelles dans le cadre de la protection des données;
- La vidéosurveillance à Vilnius: aujourd'hui et demain.

Ces présentations ont été suivies de débats au cours desquels les membres de la conférence ont pu poser des questions et exprimer leur point de vue.

Le 16 décembre 2009, l'Inspection publique de protection des données a publié une recommandation sur la *«Protection de la vie privée en présence de systèmes de vidéosurveillance. Technologies de communication sans fil»*. Elle émet des recommandations sur la manière de protéger la vie privée en utilisant des systèmes de vidéosurveillance, webcams et autres dispositifs connexes, évalue les risques liés à l'utilisation de ces outils et décrit d'éventuelles mesures techniques et organisationnelles à prendre dans le cadre de la protection des données.

L'intégralité du texte (uniquement disponible en lituanien) de cette recommandation est disponible à l'adresse: http://www.ada.lt/images/cms/File/naujienu/IP%20kamera%20(Galutinis)%2020091216.doc.

Le 23 décembre 2009, l'Inspection publique de protection des données a publié une recommandation sur le *«Transfert sécurisé de données via le protocole https»*. Celle-ci traite de sujets tels que l'installation du protocole https, les principes d'activité du protocole https, et les types de certificats SSL. L'intégralité du texte (uniquement disponible en lituanien) de cette recommandation est disponible à l'adresse:
http://www.ada.lt/images/cms/File/Inspekcijos%20rekomendacijos/SSL20091228.doc.



# 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 cette loi au cours de l'année 2009.

**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 cette loi au cours de l'année 2009.

**Règlements et législation secondaire**
Le règlement grand-ducal du 13 février 2009 instituant le «*chèque-service*» dans le domaine de l'accueil éducatif extrascolaire détaille la création et l'utilisation d'une base de données liée à ces «*chèques-services*».

Un règlement ministériel du 10 novembre 2009 a modifié les dispositions du règlement grand-ducal du 1er août 2007 autorisant la création et l'exploitation par la police d'un système de vidéosurveillance des «*zones de sécurité*». Ce règlement ministériel ajoute une nouvelle «*zone de sécurité*» aux trois zones existantes, à savoir des zones où un système de vidéosurveillance sera exploité en permanence par les forces de police.

Le règlement grand-ducal du 9 mars 2009 dispose des modalités de délivrance de la documentation cadastrale.

Dans le règlement grand-ducal du 3 décembre 2009, le gouvernement détermine les procédés à suivre pour constater la mort d'une personne en vue d'un prélèvement.

**Autres nouvelles mesures législatives**
En 2009, la Commission nationale a conseillé le gouvernement luxembourgeois sur de nombreux sujets, les plus importants étant le projet de loi relatif à «*l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité*», le règlement grand-ducal susmentionné instituant le «*chèque-service*» dans le domaine de l'accueil éducatif extrascolaire, le projet de loi portant modification de la loi relative à «*l'accès des magistrats et officiers de police judiciaire à certains traitements de données à caractère personnel mis en œuvre par des personnes morales de droit public*», le projet de règlement grand-ducal concernant la coopération interadministrative et le projet de loi régissant l'échange de certaines informations fiscales et la signature de conventions bilatérales préventives de double imposition.

L'APD luxembourgeoise a également conseillé l'Association luxembourgeoise des employés de banque et assurance (ALEBA) concernant les transactions privées réalisées par les employés.

## B. Jurisprudence importante

**Jurisprudence civile et pénale**
*Tribunal d'arrondissement de Luxembourg, siégeant en 9e 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*

Les avocats défendant quatre individus accusés de vols répétés de cigarettes et d'alcool dans des stations-service à travers le pays plaidaient «*in limine litis*» que les cassettes vidéo utilisées comme preuves contre leurs clients devaient être rejetées, à défaut d'autorisation préalable obtenue auprès de la CNPD. Ils concluaient par conséquent que ces preuves devaient être considérées nulles et non avenues et que les poursuites judiciaires à l'encontre de leurs clients devaient être suspendues.

La Cour, invoquant la «*propriété privée*» et les heures d'ouverture des stations-service, ainsi qu'un objectif général de la loi de 2002 (l'intention de la loi n'étant pas de couvrir des activités illégales), a jugé que les cassettes pouvaient néanmoins être reçues comme preuves. Il convient de noter que dans le cas présent, les magistrats n'ont pas invoqué une disposition spécifique de la loi, mais se sont limités à faire référence à des concepts juridiques vagues déduits de leur conviction, ceci en opposition directe avec la jurisprudence antérieure.

Une telle interprétation fortement préjudiciable affaiblit considérablement la sécurité juridique procurée par la loi. Il est à espérer que la juridiction d'appel utilisera une base juridique en bonne et due forme pour fonder sa décision en la matière.

## C. Questions diverses importantes

**Approbation des règles d'entreprise contraignantes (REC) d'eBay**
La CNPD, agissant pour la première fois en qualité d'autorité responsable, a officiellement approuvé l'application des REC d'eBay quant au respect de la vie privée concernant les données de ses clients et de ses employés.

Vu le climat de collaboration très constructif instauré avec eBay et la liaison rapidement établie (dans le cadre de la procédure de reconnaissance mutuelle) avec les autorités de protection des données des 13 autres États membres de l'Union européenne, la CNPD a réussi à finaliser l'approbation des REC en moins de 12 mois.

**Google Street View**
Google Inc. a contacté l'APD luxembourgeoise au sujet des dispositions et exigences nationales spécifiques en matière de protection des données applicables à leur service «Google Street View», que Google envisage de déployer au Luxembourg.

La CNPD, suivant la position commune adoptée en février 2009 par différentes APD, a décidé que les images photographiées et publiées ne peuvent contrevenir à la législation luxembourgeoise sur la protection des données, et que Google doit instaurer des mesures de sécurité strictes et, plus spécifiquement, garantir le respect des droits des personnes concernées.

En particulier, le droit d'opposition à un tel traitement doit être strictement observé par Google et la procédure d'opposition doit être la plus simple possible. La CNPD a rédigé et publié une lettre type pour toutes les personnes concernées souhaitant faire valoir leur droit d'opposition, qu'il leur suffit d'envoyer à Google Inc.

En mai 2009, la CNPD a été contrainte de suspendre la prise d'images sur le territoire luxembourgeois pour le service «Google Street View», suite au non-respect de certaines conditions préétablies par l'APD. Plus particulièrement, Google n'avait pas respecté l'obligation de publier au préalable, par le biais des médias nationaux ou sur internet, les périodes et régions exactes où circuleraient les véhicules de Google afin de prendre des photographies.

Après s'être plié à toutes les conditions, Google a recommencé la capture d'images en août 2009 dans sept communes du Grand-duché de Luxembourg. La CNPD suit actuellement avec une grande attention tous les développements liés à ce service.

**Enquête sur les principales entreprises de télécommunications luxembourgeoises**
Au cours de l'année 2009, la CNPD a mené une enquête approfondie sur la *«conformité aux exigences légales concernant les mesures de confidentialité et de sécurité applicables aux données de trafic»* des principales entreprises de télécommunications luxembourgeoises. Cette étude a également abordé les questions relatives à la conservation des données telle qu'exigée dans le contexte des actions de coercition conjointes des APD, mises en place par le groupe de travail «Article 29».

# 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 automatisé 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 (avis juridique 16 de 2003), mais aussi par la loi sur les communications électroniques, en vertu des dispositions réglementaires sur les communications électroniques (données à caractère personnel et protection de la vie privée) de 2003 (avis juridique 19 de 2003). Ces deux règlements sont entrés en vigueur en juillet 2003.

*Autres développements législatifs*

Aucun pour la période de référence.

## B. Jurisprudence importante

Aucune pour la période de référence.

## C. Questions diverses importantes

Au cours de l'année 2009, le Bureau a reçu 54 plaintes, amenant le commissaire à examiner chaque cas conformément aux pouvoirs qui lui sont conférés par la loi et à communiquer sa décision en fonction du résultat de ses enquêtes. Aucune décision n'a fait l'objet d'un recours devant la juridiction d'appel sur la protection des données. Les motifs de plaintes les plus courants avaient trait à l'installation de systèmes de surveillance par des personnes privées et à l'envoi de communications électroniques à des fins de marketing direct dans le non-respect des critères fixés par la loi. Au cours de la période de référence, le commissaire a effectué de nombreuses inspections sur le traitement des données à caractère personnel entrepris par divers responsables de traitement, 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. Les responsables du traitement de données ont également adressé des demandes de contrôle préalable concernant l'introduction de systèmes biométriques sur le lieu de travail et dans les cas où les opérations de traitement impliquaient des risques spécifiques d'interférence avec les droits et libertés des personnes concernées.

Au cours de l'année, le Bureau a régulièrement organisé des réunions avec des représentants de différents secteurs, dans l'objectif principal de débattre des questions de protection des données applicables à chacun d'entre eux. Cette volonté d'encourager les contacts 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 réglementant l'ensemble des secteurs. À cet égard, des réunions se sont tenues avec divers corps constitués 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 maltaises, 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 maltaises et des représentants des services de sécurité maltais.

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 au sein de différents organisations et corps constitués en vue d'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.

Au regard de la récente directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE, le Bureau a entamé des discussions avec les autorités maltaises en charge des communications en vue de transposer, dans les cadres juridiques internes respectifs, les amendements introduits par la directive. Les deux autorités envisagent d'organiser, au début de l'année prochaine, une série de réunions conjointes avec les entreprises dans le but de connaître leur avis sur les nouvelles dispositions et sur les amendements. Cet exercice de consultation est destiné à livrer des résultats positifs et à faciliter le processus de transposition et de mise en œuvre effective.

Le 28 janvier, le commissaire à la protection des données s'est associé aux autres autorités européennes de protection des données pour célébrer la Journée européenne de la protection des données. Pour commémorer cette journée, le Bureau du commissaire à la protection des données a distribué du matériel d'information aux étudiants, dans toutes les écoles privées, religieuses et de l'État, le but ultime étant de faire passer le message et de sensibiliser les citoyens, surtout les jeunes, aux risques inhérents à la divulgation d'informations personnelles sur internet. Ceci s'inscrit dans l'intime conviction du Bureau qu'un réel changement de culture n'interviendra pas sans un investissement permanent auprès des jeunes générations. Les enfants d'aujourd'hui sont notre avenir. Si la culture est lente à changer, la consolidation de tous les éléments inhérents au respect de la vie privée finira par produire les résultats escomptés. Face au nombre croissant d'applications de réseau social disponibles, les frontières de la vie privée s'estompent et le Bureau entend renforcer les objectifs en la matière, guidé par l'essence même du concept d'attente raisonnable en matière de respect de la vie privée.

En février de cette année, M. Joseph Ebejer a été officiellement désigné au poste de commissaire à la protection des données pour un mandat de cinq ans, suite au décès inopiné de M. Paul Mifsud Cremona.

## 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[20], 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 par la nouvelle loi sur les télécommunications (*Telecommunicatiewet*) essentiellement, entrée en vigueur le 19 mai 2004[21]. D'autres dispositions de cette directive ont également été transposées, entre autres, dans la loi sur la criminalité économique (*Wet op de Economische Delicten*), qui met en œuvre l'article 13, paragraphe 4, de la directive 2002/58/CE.

### B. Jurisprudence importante

La loi néerlandaise sur la protection des données est actuellement soumise à évaluation. En vue de sa possible révision, l'autorité néerlandaise de protection des données (le *College bescherming persoonsgegevens*, CBP) a souligné toute l'importance de renforcer la position des personnes concernées par le traitement de leurs données. Ces personnes doivent pouvoir accéder facilement aux informations exposant les motifs du traitement de leurs données à caractère personnel, les mesures prises pour empêcher l'utilisation illégale de ces données et la manière dont ces personnes peuvent exercer leurs droits. En outre, il convient de développer/instaurer des procédures de plaintes accessibles ainsi que la possibilité de recours collectifs.

Quant à la position du responsable du traitement de données, on observe une évolution d'un contrôle ex ante à un contrôle ex post. Les responsables de traitement doivent s'attacher davantage à la conformité légale du traitement et subir le coût d'une éventuelle non-conformité. L'APD néerlandaise encourage davantage de transparence, notamment par l'obligation de rapporter les violations délibérées de données et de la vie privée. Enfin, la position même de l'autorité de contrôle doit être renforcée en lui conférant davantage de pouvoirs.

Outre son travail de conseiller du gouvernement sur la nouvelle législation sur le respect de la vie privée, l'APD néerlandaise a décidé, dans le cadre de ses missions de contrôle, de donner la priorité à l'application de la législation, contribuant ainsi le plus efficacement possible à la promotion du respect de la loi néerlandaise sur la protection des données. Afin de fixer les priorités de 2009, le traitement des données à caractère personnel a fait l'objet d'une analyse des risques dans différents secteurs de la société. L'APD néerlandaise a ensuite sélectionné des cas comportant des indications de violations graves de la loi, des violations structurelles qui affectent de nombreux citoyens et contre lesquelles l'APD avait le pouvoir d'agir. Elle est également restée attentive aux manifestations d'actualité au cours de l'année. En plus des résultats positifs obtenus avec les responsables de traitement individuels, les enquêtes et interventions menées par l'APD (108 en 2009) se sont aussi avérées avoir des effets indirects. Les «directives» thématiques pour 2009 ont induit l'obligation de fournir des informations sur le transfert de données personnelles à des tiers et d'en assurer la transparence.

### C. Questions diverses importantes

**Internet**

Après une enquête menée auprès d'une société internet, l'APD néerlandaise a conclu que la société en question avait violé la loi en collectant des données sensibles sur les utilisateurs de plateformes internet, avant de vendre ces données profilées à des tiers sans en avoir informé de manière claire et exhaustive les personnes concernées. À l'époque, quelque 2,2 millions d'internautes visitaient les sites internet de la société. Cette dernière leur offrait la possibilité de se soumettre à un test pour découvrir leur «âge réel», par exemple. L'enquête a révélé que

[20] Loi du 6 juillet 2000 sur les règlements applicables à la protection des données à caractère personnel (Wet bescherming persoonsgegevens), Staatsblad (Moniteur néerlandais) 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.

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

la société internet avait collecté et traité, entre autres, des données médicales alors que cette activité est en principe soumise à une interdiction légale. La société n'a pas informé les personnes concernées de l'utilisation de leurs données, au mépris des exigences légales.

Un site permettant aux élèves d'évaluer leurs professeurs a porté gravement préjudice à la vie privée des enseignants concernés. Suite aux investigations de l'APD, le site a été modifié et mis en cache dans les moteurs de recherche.

L'APD néerlandaise a également enquêté sur deux sites destinés aux jeunes. Le site de réseau social www.zikle.nl a été contraint d'informer en bonne et due forme ses utilisateurs de ses objectifs de collecte et de traitement des données à caractère personnel, d'appliquer des mesures de sécurité et de cacher les pages contenant des profils personnels. Quant au site Www.jiggy.nl, il utilisait un jeu pour amener les utilisateurs à communiquer les adresses électroniques d'autres personnes à des fins de marketing direct. Au terme de l'enquête, le propriétaire du site a retiré le jeu.

**Données financières**
Après l'introduction de l'instrument qu'est la lettre de recommandation en 2008, l'APD néerlandaise a rédigé sa première lettre de recommandation en 2009 à la demande du système d'information national des créances (*Stichting Landelijk Informatiesysteem Schulden*, ou LIS), suivie d'une deuxième en réponse à un nouvel avant-projet du LIS. Des tests menés par l'APD ont révélé qu'aucun des avant-projets ne respectait les exigences légales. Concernant le deuxième avant-projet, l'APD a conclu qu'il outrepassait de loin son objet initial, à savoir l'enregistrement des créances en souffrance afin d'éviter un endettement problématique. Cette situation peut conduire à l'enregistrement d'un groupe non négligeable de personnes qui, bien que n'ayant pas leur place dans le registre, subiront néanmoins les conséquences négatives associées à la réputation de débiteur problématique.

Une banque a communiqué les numéros de compte et les adresses de jeunes clients à une œuvre de bienfaisance sans en informer les clients en question ni avoir obtenu leur consentement. Suite à une plainte, l'APD s'est saisie du dossier et a contraint la banque à adapter sa pratique.

En 2009, le ministre néerlandais des finances a suivi l'avis de l'APD portant sur des propositions législatives liées à la création d'un registre des pensions. L'objectif est de permettre à chaque citoyen de vérifier ses droits à pension en ligne. Dans la mesure où ces données ne manqueront pas d'attiser la convoitise d'autres parties, l'APD a souligné la nécessité de mettre en place des mesures de sécurité très strictes.

**Données médicales**
Sur la base des investigations portant sur deux systèmes régionaux actuels de dossiers médiaux électroniques, l'APD néerlandaise a conclu à la violation de la loi néerlandaise sur la protection des données. L'APD a engagé une procédure de conformité à l'encontre des deux systèmes régionaux. Cette procédure a convaincu l'un des deux systèmes régionaux de cesser ses activités illégales, notamment en informant personnellement tous les patients de l'inclusion de leurs données dans les systèmes régionaux. La législation proposée sur les dossiers médiaux électroniques soulève toujours des inquiétudes. L'avis critique remis par l'APD sur la proposition législative initiale en 2007 a donné lieu à l'adaptation de l'avant-projet. Cependant, les amendements soumis par la Chambre des députés permettaient, dans certains cas, aux assureurs en soins de santé d'accéder aux dossiers des patients. L'APD a conseillé au ministre de lever cette exception à l'interdiction générale. Ce dernier a indiqué qu'il s'exécuterait.

Une autre source de préoccupation concerne la sécurité des informations dans les hôpitaux. L'enquête menée par l'APD et l'Inspection néerlandaise des soins de santé (*Inspectie voor de Gezondheidszorg*, ou IGZ) en 2007 et 2008 a révélé qu'aucun des vingt hôpitaux contrôlés ne satisfaisait à la norme de sécurité des informations. En 2009, l'APD a ordonné des sanctions pour non-conformité à l'encontre de quatre hôpitaux qui n'avaient toujours pas pris de mesures appropriées à cet égard.

Après contrôle des procédures de plusieurs services de santé et de sécurité au travail, force était de constater qu'au moins un service enfreignait systématiquement la loi en fournissant les données médicales d'employés

malades aux employeurs de ces derniers, et ce au mépris des règles de confidentialité médicale. L'APD a infligé en 2009 une sanction pour non-conformité à ce service de santé et de sécurité, lequel s'est par la suite abstenu de toute violation pendant la période de conformité fixée. L'enquête menée dans trois autres services de santé et de sécurité au travail se poursuit.

**Autres activités dans le secteur privé**

Même si nous semblons y être accoutumés de par l'ampleur du phénomène, la surveillance par caméra reste un vaste sujet de questions adressées à l'APD par les citoyens. Celle-ci a étudié l'usage de la vidéosurveillance sur un site industriel. La société responsable de la surveillance pouvait se targuer de résultats globalement positifs. Elle s'est par ailleurs engagée à modifier les règles d'inspection dans un souci de conformité aux exigences de la loi néerlandaise sur la protection des données. Étant donné le manque de clarté qui entoure parfois la question de savoir qui, des sociétés privées ou des instances gouvernementales, est responsable de la vidéosurveillance, l'APD a décidé d'élaborer de nouvelles lignes directrices en la matière.

La proposition d'introduire des compteurs électriques dits intelligents, capables de fournir une vision très détaillée du ménage d'un individu et des périodes au cours desquelles il n'est pas présent à son domicile, a suscité de vives réactions. Les consommateurs doivent être autorisés à faire des choix éclairés concernant la fréquence et le volume de la collecte d'informations. L'avant-projet de loi a été modifié suivant l'avis rendu par l'APD au ministre.

**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*). 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 l'APD – entre autres – sur plusieurs points, l'essence du texte reste malheureusement inchangée. En 2009, l'APD a été priée de rendre un avis sur certaines mesures exécutoires induites par la proposition de loi et, à nouveau, elle a mis en garde contre le risque d'arbitraire.

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. Plus de la moitié des écoles étudiées n'avaient pas indiqué si les parents étaient informés ou non. Suite à l'enquête, l'APD a publié des directives à l'attention des écoles primaires.

**Police et autorités judiciaires**

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 2007/2008, l'APD a enquêté 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 pour pouvoir répondre aux exigences de la loi sur les données policières (*Wet politiegegevens*), entrée en vigueur le 1er janvier 2008. En 2009, une enquête de suivi menée dans trois zones de police a révélé que, malgré des différences de contexte, aucune des zones ne respectait les exigences d'autorisation et de surveillance dans leur intégralité.

Les services de renseignement peuvent comparer les informations dont ils disposent avec les rapports de police directement. Dans son avis relatif à la proposition de loi sur cette forme indépendante de consultation des bases de données policières, l'APD a demandé au gouvernement de clarifier la nécessité d'une telle consultation à grande échelle.

En 2009, l'autorité néerlandaise de protection des données a élaboré des directives dans le cadre de la lecture automatisée des plaques d'immatriculation (LAPI) par la police. Dans ces directives, l'APD explique son interprétation des normes légales, en sa qualité d'autorité de contrôle exerçant ses pouvoirs. Plus tard au cours de la même année, l'APD a enquêté sur l'application faite de la LAPI par deux zones de police et est arrivée à la conclusion que les deux zones enfreignaient sciemment la loi néerlandaise sur la protection des données en traitant les «*hits*» (concordance) et les «*no-hits*» (non-concordance) pendant, respectivement, 120 et 10 jours. Une donnée «*no-hit*» signifie qu'une plaque d'immatriculation lue n'apparaît pas dans le fichier de référence et qu'elle n'est par conséquent pas recherchée par la police. L'enregistrement de cette plaque d'immatriculation doit être détruit sur-le-champ. En réponse aux conclusions finales de l'enquête, les deux zones de police ont annoncé début 2010 l'arrêt de cette pratique illégale.

Les passagers qui souhaitent participer à un système de franchissement automatisé de la frontière, par exemple au moyen d'une reconnaissance de l'iris ou d'un relevé d'empreintes, doivent faire l'objet d'un contrôle préalable. L'APD a invité le ministre de la justice à préciser les points de départ qui seront utilisés dans ces enquêtes de fond.

## Pologne

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

**Révision de la loi sur les télécommunications**
La loi du 24 avril 2009 modifiant la loi sur les télécommunications est entrée en vigueur le 6 juillet 2009. Parmi les modifications figuraient notamment de nouvelles dispositions sur la conservation des données, afin d'adapter la législation nationale aux exigences de la directive 2006/24/CE en imposant un grand nombre de nouvelles responsabilités aux opérateurs et fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications (comme l'obligation de conserver les données de trafic pendant une période de 24 mois à dater de l'appel et, au terme de cette période, de détruire les données à l'exception de celles conservées en vertu d'autres dispositions légales). Les obligations susmentionnées doivent être mises en œuvre de manière à ne pas entraîner la divulgation du transfert de télécommunications. L'amendement adopté implique également de la part des entrepreneurs qu'ils garantissent la sécurité des données à caractère personnel au moyen de mesures techniques et organisationnelles appropriées et limitent leur accès aux seuls membres du personnel autorisés.

**Avant-projet de loi modifiant la loi sur l'accès aux informations publiques**, qui stipule que les données relatives à l'état de santé des personnes occupant les fonctions de président et de premier ministre sont assimilées à des informations à caractère public. En exprimant clairement son opposition aux dispositions de l'avant-projet, l'inspecteur général souligne que les dispositions existantes de la Constitution polonaise, de la loi relative à la protection des données personnelles et de la directive 95/46/CE recommandent toutes que le législateur fasse preuve de la modération appropriée pour introduire des dispositions qui pourraient donner lieu à la publication de données sur un état de santé dit «sensible» - y compris dans le cas des titulaires des plus hautes fonctions publiques en Pologne. Bien que conscient du fait que le droit au respect de la vie privée et à la protection des données personnelles des titulaires de fonctions officielles soit beaucoup plus restreint que celui des «citoyens ordinaires», l'inspecteur général insiste sur l'absence d'une base légale disposant que ces droits ne doivent pas être appliqués du tout. L'autorité de protection des données souligne que cette position est aussi celle défendue dans la Déclaration sur la liberté du discours politique dans les médias du Comité des ministres du Conseil de l'Europe du 12 février 2004.

À la lumière de la position ferme de l'inspecteur général, l'avant-projet susmentionné n'est pas entré en vigueur, et toute nouvelle tentative se verra opposer une réponse tout aussi ferme de l'APD.

Le nouveau règlement 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** est entré en vigueur le 10 février 2009. Le nouveau modèle de notification, élaboré à l'initiative de GIODO, a été simplifié et énumère les principales responsabilités du responsable du traitement de données quant à la sauvegarde des données. L'introduction de ce nouveau modèle a permis de réduire le nombre de notifications incorrectes.

### B. Jurisprudence importante

Au cours de la période de référence, l'inspecteur général a été saisi de différents dossiers liés aux activités des agences d'information sur les crédits. La Cour administrative suprême a suivi à plusieurs reprises la position de l'inspecteur général. L'une des affaires les plus importantes concernait la facturation de frais par les agences, responsables du traitement des données, pour la fourniture aux clients de leurs informations personnelles. Cette pratique s'est heurtée à une forte opposition de l'inspecteur général. Au regard de la loi polonaise, les personnes concernées possèdent un droit d'accès une fois tous les six mois et cet accès doit être gratuit. Cette approche a été confirmée par la décision de la Cour administrative suprême rendue le 30 juillet 2009.

L'inspecteur général s'est également attelé à la problématique de l'acquisition et du traitement de données biométriques à des fins de contrôle du temps de travail. Il a jugé ce procédé comme étant une ingérence excessive dans la vie privée des personnes concernées. De tels cas font toujours planer un grand risque de

violation de la vie privée et il s'impose d'opter pour des méthodes moins intrusives. Cette opinion a été confirmée par la Cour administrative suprême qui, dans son arrêt du 1er décembre 2009, a statué que, pour évaluer l'opportunité d'obtenir les données biométriques des employés, avec leur consentement, à des fins de vérification du temps de travail, les principaux préalables au traitement sont les principes de proportionnalité et de légalité. Cela signifie que le risque de violation des libertés et droits fondamentaux doit être proportionné à l'objectif visé du traitement de ces données. Dès lors que le principe de proportionnalité exprimé dans la loi sur la protection des données personnelles constitue le premier critère devant sous-tendre les décisions relatives au traitement des données biométriques, l'utilisation de telles données aux fins du contrôle du temps de travail est disproportionnée par rapport à la finalité supposée de leur traitement. Selon la Cour, la collecte de données biométriques dans ces cas doit être considérée comme une intrusion excessive dans la vie privée, ce qui confirme la position de l'inspecteur général.

Au cours de la période de référence, l'inspecteur général a également examiné la question de l'admissibilité du traitement de données personnelles dans les copies de sauvegarde créées par les banques après le retrait de données du système d'archivage, sans qu'une base légale sous-tende un traitement ultérieur. Ce genre de situation peut survenir après une demande de crédit refusée, lorsque la banque retire du système d'archivage les données personnelles du demandeur, la base légale offerte par la loi sur la protection des données personnelles venant à expiration (traitement de données requis pour entreprendre les démarches nécessaires à la conclusion du contrat). En outre, le traitement de données dans des copies de sauvegarde, lorsque les données ont été supprimées du système d'archivage, est contraire à l'objet de la création de ces copies de sauvegarde (archivage destiné à assurer la sécurité opérationnelle de la banque). Le point de vue précité de l'inspecteur général a été étayé par le jugement du tribunal administratif régional de Varsovie le 16 janvier 2008. La Cour administrative suprême a ensuite rejeté l'appel le 3 juillet 2009.

## C. Questions diverses importantes

En juin 2009, GIODO a réalisé un audit du traitement des données à caractère personnel dans les systèmes TI de la société de transport public de Varsovie (ZTM) à la lumière d'articles de presse faisant état de l'enregistrement par ZTM des lieux et heures de déplacement en transport public (en particulier dans le métro de Varsovie, où les passagers doivent présenter à chaque portillon d'accès une carte électronique codée). L'inspection a confirmé l'existence des problèmes relatés par la presse ainsi que d'autres irrégularités liées à un traitement de données excessif, non conforme à l'objectif. GIODO a informé ZTM des irrégularités identifiées au cours de l'inspection et a exigé qu'elles soient corrigées. À présent, l'inspecteur général mène des contrôles dans d'autres villes afin de vérifier l'ampleur du traitement de données réalisé par d'autres sociétés de transport public ayant opté pour des systèmes de billetterie semblables à ceux de ZTM. L'audit de ZTM décrit ci-dessus a été l'élément déclencheur d'un plus vaste audit effectué par l'inspecteur général au sein d'autres sociétés de transport public.

Réseaux sociaux. Au cours des premier et deuxième trimestres de l'année, l'inspecteur général a mené une série de contrôles sur les sites de réseaux sociaux. Dans ce cadre, il s'est avéré que le responsable du traitement de données est en règle générale le fournisseur du site. L'irrégularité la plus fréquemment identifiée lors de ces contrôles portait sur une protection inadéquate des données collectées sur les profils d'utilisateurs. La procédure de connexion et de modification des profils était souvent insuffisamment protégée (mots de passe trop courts et transmission de données non sécurisées). Parmi les erreurs organisationnelles, citons des lacunes au niveau de l'obligation d'information, le manque d'informations claires sur la possibilité de notifier des abus, et des règlements imprécis. Suite aux actions entreprises par l'inspecteur général, en collaboration avec l'administrateur de «*Nasza Klasa*» (Nos camarades de classe), un onglet séparé a été créé sur le site du portail. Cet onglet donne des informations sur les questions relatives à la protection des données et aux menaces courant sur la vie privée et introduit une fonctionnalité permettant aux utilisateurs de configurer le niveau de sécurité de leurs données.

En 2009, les entités habilitées qui disposent d'un accès direct au système d'information national en vue d'insérer des entrées dans le système d'information Schengen (SIS) et de consulter les informations qu'il contient ont fait l'objet de contrôles. Les tribunaux étaient les principaux visés. Les audits ont mis à jour de nombreuses irrégularités, telles que l'absence d'une documentation adéquate (p. ex. absence d'une politique de sécurité) et la possibilité pour des personnes non autorisées et non formées d'accéder aux données personnelles. Au terme de l'inspection, et vu les irrégularités constatées, l'inspecteur général a prié le ministre de la justice de corriger les irrégularités, notamment celles relatives à la mise en œuvre de l'accès au système d'information Schengen.

L'inspecteur général poursuit ses initiatives pédagogiques visant à sensibiliser les citoyens à leur droit à la protection des données et au respect de la vie privée. Un autre projet revêt la forme d'un projet pilote destiné aux écoles secondaires, baptisé «Vos données – votre affaire. Protection efficace des données à caractère personnel. Une initiative pédagogique destinée aux étudiants et aux enseignants». Une telle initiative destinée aux enseignants et étudiants de l'enseignement secondaire nourrit l'objectif d'étoffer leur connaissance de la protection des données et du droit de chacun au respect de la vie privée. Le programme implique une collaboration sur la base d'un partenariat entre les centres de formation autonomes pour enseignants et l'inspecteur général pour la protection des données personnelles. Le projet pilote s'articule autour de deux phases, la première visant la formation des enseignants et la deuxième portant sur l'intégration de matières liées à la protection des données dans les programmes pédagogiques. Les écoles participant au programme recevront les exposés ainsi que le matériel conçus par l'inspecteur général à l'intention des enseignants et étudiants; un rapport d'évaluation sera également rédigé sur les activités entreprises et les résultats du projet de programme pédagogique à l'échelle nationale.

Le 27 janvier 2009, dans le cadre de la 3e Journée de la protection des données, l'inspecteur général a signé un accord avec l'association des banques polonaise, intitulé «Bonnes pratiques pour le traitement des données personnelles dans le secteur bancaire – le point de vue des acteurs de terrain». Cet accord vise à améliorer la protection des données personnelles ainsi que l'observation du droit au respect de la vie privée dans le secteur bancaire. Il doit contribuer à l'instauration d'un code de bonnes pratiques en matière de protection des données pour l'ensemble du secteur.

En collaboration avec l'épiscopat de Pologne, l'inspecteur général à la protection des données personnelles a développé les «Lignes directrices pour la protection des données à caractère personnel au sein de l'Église catholique de Pologne».

Ces lignes directrices précisent les principes de protection en bonne et due forme des données à caractère personnel. Elles doivent contribuer à protéger les données personnelles dans le cadre des activités de l'Église. Toutefois, le pouvoir de contrôle de l'inspecteur général est très limité pour ce qui est du fonctionnement de l'Église.

# 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 n° 7/2004 (uniquement l'article 13) et par la loi n° 41/2004 du 18 août.

La directive 2006/24/CE (directive relative à la conservation des données) a été transposée dans la législation nationale par la loi n° 32/2009, entrée en vigueur en août 2009.

## B. Jurisprudence importante

La Cour administrative centrale a donné raison à l'autorité portugaise de protection des données dans une affaire où l'APD n'a pas autorisé la municipalité de Porto à soumettre tous ses employés à des alcootests pratiqués par des professionnels non issus du secteur de la santé, et dont les résultats étaient directement communiqués au chef de l'employé.

Dans le droit fil des arguments de l'APD, la Cour a considéré que rien ne justifiait de soumettre tous les employés à des alcootests, hormis dans le cadre de certaines activités professionnelles spécifiques où la vie de l'employé ou de tiers peut être en jeu; de plus, les tests doivent être réalisés par des professionnels de la santé (médecins ou infirmiers) relevant du service de la santé et de la sécurité au travail; enfin, les résultats des tests ne peuvent être communiqués à la hiérarchie, mais uniquement indiquer la mention «apte ou inapte au travail».

Dans un autre arrêt rendu en appel contre une décision de l'APD, la Cour administrative a également statué en faveur de l'APD en maintenant l'interdiction d'installer des caméras de vidéosurveillance à l'intérieur de la salle de rédaction d'une chaîne télévisée, lieu de travail des journalistes.

## C. Questions diverses importantes

**Activités générales**

L'autorité portugaise de protection des données a maintenu son rythme intensif d'activités en 2009. Le nombre de notifications de traitement de données a dépassé la barre des dix mille. Les poursuites engagées à la suite de plaintes et les contrôles menés d'initiative ont dépassé le chiffre de 700, et 260 sanctions ont été prononcées pour un montant total de 540 000 euros.

On dénombrait 171 inspections sur site, dont un audit sur la base de données des listes d'électeurs. À la suite de ces inspections, des recommandations pertinentes ont été formulées, suivies du contrôle de leur mise en œuvre. Le rapport d'audit a été soumis au président de la République, au Parlement et au gouvernement.

L'APD a entamé la mise en œuvre de la procédure de notification en ligne dans le cadre du traitement de données spécifiques et poursuit le processus de dématérialisation de tous les documents, ainsi que la réforme du système d'information interne, en vue d'aboutir à un processus décisionnel plus rapide à court terme.

**Orientations pour les responsables du traitement de données**

En 2009, l'autorité portugaise de protection des données a publié des lignes directrices à l'attention des responsables de traitement de données concernant certains types spécifiques de traitement de données poursuivant les objectifs suivants: la pharmacosurveillance, les lignes d'intégrité (*whistleblowing*), la transaction de crédits et l'enregistrement des appels vocaux (centres d'appel).

Ces réflexions doivent orienter les responsables de traitement de données sur la manière de mieux se conformer aux règles de protection des données, ainsi que d'informer les personnes concernées de leurs droits et des modalités du traitement de données.

Concernant les lignes d'intégrité, l'APD autorise uniquement un système confidentiel de manière à prévenir toute diffamation et discrimination, répondant à des finalités limitées (prévention et répression d'irrégularités comptables, contrôles comptables internes, audit, lutte contre la corruption et le crime financier), et n'autorise

pas la dénonciation de manquements liés au gouvernement d'entreprise. Les personnes concernées doivent appartenir à des catégories spécifiques: les rapports doivent viser en premier lieu des individus ayant une responsabilité décisionnelle dans les domaines susmentionnés. Au sens de l'APD, ces lignes doivent être considérées comme des mécanismes optionnels complémentaires, subsidiaires par rapport aux méthodes légales existantes de dénonciation des irrégularités, et les employés doivent recevoir à l'avance et de manière claire toutes les informations pertinentes relatives au traitement de données.

**Avis sur des projets de loi**

L'APD a été invitée à formuler, en 2009, 86 avis sur des projets de loi ayant trait à la protection des données, que ce soit au niveau national ou international.

Au niveau communautaire, les plus importants concernaient la transposition de la décision-cadre n° 2006/960/JAI du Conseil, la révision du règlement n° 1049/2001, la décision-cadre n° 2005/222/JAI du Conseil, les amendements des règlements Eurodac et Dublin II et l'avant-projet de décision du Conseil sur le système d'information douanier.

Au niveau national, l'APD a rendu des avis sur divers accords bilatéraux conclus entre le Portugal et d'autres États concernant l'échange d'informations à des fins fiscales et répressives.

Au cours de l'année 2009, l'APD a également publié des avis concernant des avant-projets de loi sur le régime juridique légal dans le contexte de la santé et de la sécurité au travail, sur le droit d'information et de consentement éclairé dans le secteur de la santé; sur les répertoires de véhicules, sur l'inscription électorale et sur le système d'information d'enquête criminelle.

En vertu de la législation nationale, l'APD doit aussi remettre des avis concernant l'utilisation de systèmes de vidéosurveillance exploités par les autorités de maintien de l'ordre sur les voiries publiques. En 2009, l'APD a opposé trois avis négatifs à l'installation de tels systèmes, considérant que les exigences légales en matière de proportionnalité n'étaient pas respectées. Dans un cas, l'APD a remis un avis général positif, accompagné toutefois de restrictions quant à l'exploitation du système en période nocturne. S'ils sont défavorables, les avis de l'APD sont contraignants. Les conditions de l'autorisation sont par ailleurs établies par le ministère des affaires intérieures.

**Projet DADUS**

Développé par l'autorité portugaise de protection des données, le projet DADUS, destiné aux enfants et aux jeunes entre 10 et 15 ans, vise à introduire dans les écoles le concept de protection des données et de respect de la vie privée.

En 2009, plus de 2000 enseignants se sont inscrits au projet DADUS. Qui plus est, le site et le blog du projet sont apparus dans plus de 200 000 résultats de recherche.

Le projet a organisé trois concours sur le thème de la vie privée: paroles de rap, affiche et vidéo. Le taux de participation a été très élevé et les écoles lauréates ont reçu un prix.

L'APD a également signé un accord avec l'École supérieure de cinéma pour la production de matériels audiovisuels par ses étudiants, qui seront utilisés dans le cadre du projet DADUS afin d'en améliorer la composante multimédias, qui constitue à nos yeux l'un des meilleurs moyens de communication avec les plus jeunes.

## Roumanie

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

À l'instar des années précédentes, l'autorité de contrôle a adopté en 2009 des décisions visant à instaurer une pratique harmonisée, conforme aux règlements européens:

- afin de simplifier la procédure d'autorisation et d'éviter des formalités excessives, une décision établit une autorisation type pour le transfert de données à caractère personnel vers des pays tiers;
- afin de garantir la protection effective des droits des personnes concernées, notamment dans le cas d'opérations de traitement de certaines données comportant des risques spécifiques pour les droits et libertés individuels de par la nature des données traitées, la finalité du traitement, le caractère spécial des catégories de personnes concernées ou les mécanismes utilisés pour traiter les données, une décision a été adoptée en vue de déterminer les opérations de traitement de données personnelles susceptibles de menacer les droits et libertés individuels.

L'autorité de contrôle a été consultée, dans le cadre du processus de rédaction de textes législatifs concernant le traitement de données à caractère personnel, par plusieurs autorités et institutions publiques, à savoir le ministère de l'administration et de l'intérieur, le ministère des communications et de la technologie de l'information ainsi que le secrétariat général du gouvernement.

En 2009, nombre de responsables de traitement de données et de particuliers ont sollicité un avis concernant le traitement de données à caractère personnel, preuve de leur intérêt pour la protection des données personnelles et de leur sensibilisation à l'impact de ce traitement sur la vie privée. Parmi ces avis, les plus pertinents concernaient la définition du champ des capacités des responsables et agents de traitement de données, la divulgation de données personnelles et le traitement de ces données au sein des systèmes d'archivage des sociétés de renseignements commerciaux, par exemple.

### B. Jurisprudence importante

Les tribunaux ont continué à suivre une pratique harmonisée dans les litiges liés à la protection des données personnelles. Nous vous présentons ci-dessous divers cas pertinents dans lesquels les sanctions infligées par l'autorité de contrôle ont été contestées devant les tribunaux.

1. L'autorité de contrôle a mené une enquête au sein d'une compagnie privée qui traitait, depuis 2008, des données personnelles en offrant des services de visualisation de rues, et ce sans notification préalable. Cette enquête a permis de découvrir qu'aucune information n'était donnée aux personnes concernées à propos de la collecte et de la publication en ligne d'images panoramiques sur lesquelles figuraient des personnes physiques, et que le responsable du traitement de données n'avait pas pris les mesures nécessaires pour flouter les données personnelles apparaissant dans les images publiées sur le site internet.

   Une amende a donc été infligée. Insatisfait des conclusions du rapport d'enquête, le responsable du traitement de données a déposé plainte contre l'autorité de contrôle.

   Le tribunal a jugé que le responsable du traitement de données avait traité des données personnelles sans informer en bonne et due forme les personnes concernées de la collecte et du chargement d'images panoramiques contenant des données à caractère personnel (visages humains, numéros de plaques d'immatriculation des véhicules circulant au moment de la capture d'image, noms et numéros de bâtiments). En vertu du principe voulant que les données soient adéquates, pertinentes et non excessives au regard de la finalité du traitement, ces images auraient dû être traitées techniquement de manière à ne pas permettre l'identification des personnes présentes dans le champ au moment de la prise des images panoramiques.

   En foi de quoi, le tribunal a confirmé l'amende infligée par l'autorité de contrôle au responsable du traitement de données.

2. L'autorité de contrôle a constaté qu'un institut de soins de santé n'avait pas notifié le traitement de données à caractère personnel et avait divulgué certaines données de patients à d'autres établissements de soins de santé, sans le consentement de ces patients et sans les en avoir préalablement informés.

   En réaction à ces infractions, l'autorité de contrôle a imposé des amendes.

   Le responsable du traitement de données a contesté le rapport d'enquête.

   Le tribunal a jugé que le patient auteur de la plainte n'avait pas donné son consentement à la divulgation du numéro d'identification personnelle de son fils, que ces informations personnelles avaient été divulguées par la suite à tous les centres médicaux du comté, et que le responsable du traitement de données n'avait pas informé la personne concernée en conséquence ou publié une notification du traitement desdites données personnelles.

   En foi de quoi, le tribunal a confirmé de manière irrévocable la sanction imposée par l'autorité de contrôle.

3. À la suite d'un contrôle mené au sein d'une autorité publique, il s'est avéré que les obligations légales d'application de mesures de sécurité et de confidentialité dans le cadre du traitement de données personnelles n'étaient pas respectées.

   L'institution publique en question avait posté sur son site internet deux règlements adoptés par les autorités locales, lesquels contenaient, entre autres, des tableaux reprenant les noms, prénoms, numéros d'identification personnelle et données relatives à l'état de santé (handicaps) de bénéficiaires de certaines prestations légales.

   La divulgation de données personnelles spécifiques (articles 7 et 8 de la loi n° 677/2001), même accidentellement ou suite à une erreur technique, constitue une infraction aux dispositions de l'article 20 de la loi n° 677/2001, du fait qu'elle omet de garantir les mesures techniques et organisationnelles nécessaires pour protéger les données personnelles, ainsi qu'à celles de l'ordonnance n° 52/2002 relative à l'approbation de mesures de sécurité minimales dans le cadre du traitement de données à caractère personnel.

   Le tribunal a confirmé la sanction imposée par l'autorité de contrôle.

## C. Questions diverses importantes

**Mission d'évaluation de la Roumanie concernant la protection de données à caractère personnel dans la perspective de son adhésion à la Convention d'application de l'accord de Schengen**

Menée à Bucarest entre le 29 avril et le 1er mai 2009, la mission d'évaluation portant sur la protection des données à caractère personnel revêtait une importance capitale dans le cadre de la procédure d'adhésion de la Roumanie à l'espace Schengen.

Dans leur rapport d'évaluation, les experts se prononcent favorablement quant à la capacité de l'autorité de contrôle à agir indépendamment, au haut niveau de mise en œuvre de la législation relative à la protection des données à caractère personnel et à la collaboration efficace de notre bureau avec d'autres autorités concernées. Il est utile de mentionner que la campagne d'information menée en Roumanie par l'autorité de contrôle, en collaboration avec l'inspection générale de la police roumaine et, à une moindre échelle, avec l'école de droit «Constantin Brâncuşi» à Tg. Jiu et des inspecteurs de la police locale, a été appréciée à sa juste valeur.

Le président et le personnel de l'autorité de contrôle assistant aux débats ont été félicités pour leur professionnalisme et la qualité élevée de leurs activités, ainsi que pour l'organisation de la mission d'évaluation Schengen.

**Conférence des autorités de protection des données d'Europe centrale et orientale**

L'autorité de contrôle a accueilli la conférence des autorités de protection des données d'Europe centrale et orientale, la réunion annuelle des autorités pour la protection des données de la région, qui fournit une occasion idéale de débattre et d'analyser les enjeux spécifiques que rencontrent les autorités compétentes

en matière de protection de la vie privée dans l'exercice de leurs activités.

Les représentants des autorités de protection des données de Bulgarie, Croatie, République tchèque, Estonie, Hongrie, Pologne, Slovaquie et Slovénie, ainsi que ceux de notre propre autorité de contrôle, organisatrice de l'événement, participaient à cette 11e réunion. Ce fut l'occasion de débattre de questions générales sur les développements enregistrés dans chaque pays dans le domaine de la protection des données à caractère personnel, sous l'angle de la relation entre le droit à la vie privée, les données biométriques, l'environnement d'entreprise et les nouvelles technologies.

La manifestation, à laquelle étaient également conviés des professeurs d'université et des chefs de zones de police rompus à la question de la protection des données, aux côtés d'experts et de commissaires à la protection des données venus des quatre coins d'Europe centrale et orientale, représentait une formidable opportunité d'identifier et de promouvoir les bonnes pratiques dans le domaine de la protection des données à caractère personnel.

Quant aux activités d'inspection, les restrictions budgétaires imposées en 2009 ont contraint l'autorité de contrôle à changer sa stratégie. Désormais, hormis les contrôles menés avec les autorités compétentes en vue de l'adhésion de la Roumanie à l'espace Schengen et les inspections préliminaires effectuées en vertu des dispositions d'une loi spéciale, la résolution des plaintes est considérée comme une priorité.

Les plaintes reçues par l'autorité de contrôle concernaient la réception de messages commerciaux non sollicités, la communication de données personnelles de débiteurs à des systèmes de type bureau de crédit et le traitement ou la divulgation illégal(e) de données à caractère personnel.

Dans les cas déclarés fondés sur la base des preuves reçues, des sanctions ont été imposées et il a été décidé, le cas échéant, de mettre fin au traitement ou de supprimer les données personnelles traitées au mépris du respect des droits des personnes concernées.

Les plaintes portant sur des communications commerciales non sollicitées faisaient état de situations dans lesquelles les personnes concernées recevaient ces communications par SMS et par téléphone, sans avoir exprimé leur consentement explicite et sans équivoque.

Outre la compétence générale établie en vertu de la loi n° 677/2001, l'autorité de contrôle exerce un certain nombre de pouvoirs stipulés dans la loi n° 506/2004 relative au traitement des données personnelles et à la protection de la vie privée au sein du secteur des communications électroniques.

Les plaintes parvenues à l'autorité de contrôle, dénonçant de possibles violations du droit à la vie privée dans le cadre du traitement des données à caractère personnel dans des systèmes d'archivage de type bureau de crédit, avaient trait à la transmission de données personnelles au mépris du respect des droits des particuliers et sans leur consentement, ou au mépris des dispositions de la décision adoptée par le président de l'autorité de contrôle concernant le traitement de données à caractère personnel dans des systèmes d'archivage de type bureau de crédit.

# Slovaquie

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

En 2009, le Bureau pour la protection des données personnelles de la République slovaque (ci-après dénommé «le Bureau») a reformulé certaines dispositions de la loi relative à la protection des données personnelles actuellement en vigueur. L'avant-projet de loi doit modifier cette loi relative à la protection des données personnelles sur la base des recommandations issues du dialogue structuré mené avec les représentants de la Commission européenne, des incitants liés à l'application de la loi relative à la protection des données personnelles dans la pratique, ainsi que des derniers développements intervenus après l'adoption de la décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Le projet d'amendement sera soumis au gouvernement slovaque en octobre 2010.

## B. Jurisprudence importante

En 2009, le Bureau a été impliqué dans plusieurs procès. Pour deux d'entre eux, une requête a été introduite auprès des tribunaux en vue d'obtenir l'annulation de la décision du Bureau, qui ordonnait au responsable du traitement de données d'un système d'information – et à l'agent de traitement d'un fournisseur de crédit – de prendre des mesures de réparation. Cet ordre de réparation était imposé au responsable du traitement afin de mettre fin à la divulgation illégale d'une demande de paiement dévoilée dans une lettre recommandée ouverte. En procédant de la sorte, le responsable du traitement rendait accessible des données révélant l'identité économique de la personne concernée, sans base légale. Le responsable a porté l'affaire devant un tribunal, qui n'avait toujours pas rendu son jugement en 2009. Dans une affaire connexe, le tribunal traite une requête de l'agent de traitement d'un ancien responsable de traitement de données qui affirme que la décision du Bureau – un ordre d'entreprendre des mesures de réparation, impliquant dans le cas présent de se conformer au champ d'application et aux modalités de traitement des données personnelles tels que stipulés dans un contrat écrit par le responsable du traitement de données – n'est pas légale. Ici aussi, le tribunal n'a pas encore rendu sa décision.

Dans le troisième cas, une requête a été introduite auprès des tribunaux en vue d'obtenir l'annulation de la décision du Bureau infligeant une amende à un responsable de traitement de données, lequel n'avait pas adopté de mesures de sécurité appropriées. Le tribunal du comté, saisi en première instance, a jugé que l'imposition d'une sanction était conforme à la loi sur la protection des données. Le responsable du traitement a porté l'affaire devant une instance supérieure, interjetant appel auprès de la Cour suprême, dont l'arrêt n'a pas encore été rendu.

## C. Questions diverses importantes

### Activité d'inspection et émission de notifications

*Contrôle de la protection des données personnelles en chiffres*

En 2009, 108 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. Trente-six autres notifications portaient sur des soupçons d'infraction à la loi sur la protection des données. L'inspecteur en chef du Bureau a ordonné 128 procédures *ex officio* à l'encontre de responsables de systèmes d'archivage. En 2009, le département d'inspection a ouvert 272 procédures. Trente-neuf autres notifications datant de 2008 étaient toujours en instance. Au total, en 2009, le département d'inspection a traité 311 notifications.

Il a ainsi réalisé 107 contrôles et adressé 72 «demandes d'informations» aux responsables et agents de traitement de systèmes d'archivage, ceci en coordination avec le sous-département d'examen des plaintes. Au total, 161 ordres ont été émis en vue de corriger les lacunes identifiées par l'inspection, soit une augmentation de 120 % par rapport à 2008. Seuls quatre responsables de traitement de données ont fait usage de leur droit d'appel contre l'ordre émis, soit 2,5 % du nombre total de responsables de traitement de données à l'encontre desquels le Bureau a émis un ordre.

En 2009, le Bureau a infligé 19 amendes pour un montant total de 27 446,19 euros. Douze amendes ont été acquittées dans les délais. Dans trois cas, les procédures

d'exécution sont toujours en cours. Une action a été entreprise par des responsables de traitement de données à l'encontre des deux décisions du Bureau, conformément aux procédures administratives. Deux procédures ont été ouvertes fin 2009 et, pour l'une d'entre elles, un rappel de l'ouverture de la procédure administrative a été envoyé au responsable du traitement.

En 2009, 163 des 272 nouvelles notifications concernaient des responsables de traitement de données issus du secteur privé, et 55 – généralement soumises par d'autres organes publics – concernaient des agents de l'administration publique. Dans 31 cas, le Bureau a enquêté sur des notifications portant sur des instances gouvernementales autonomes. Dix-huit 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 cinq reprises.

Sur les 108 notifications soumises par des personnes concernées en 2009, le Bureau a clos 85 dossiers, dont 66 dans le délai légal de base de 60 jours, soit près de 78 % des cas. 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 de données, que la collecte d'autres éléments de preuve s'est révélée plus difficile ou que les pétitionnaires ont demandé à pouvoir coopérer. Au total, 47 notifications, parmi toutes celles traitées, ont été jugées non fondées.

Si un plaignant 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 101 affaires clôturées en 2009 (85 ouvertes et clôturées en 2009 et 16 ouvertes en 2008 et clôturées en 2009), seules 7 ont fait l'objet d'une nouvelle notification au Bureau. Six d'entre elles ont été rejetées conformément à la loi sur la protection des données, faute d'apporter de nouveaux éléments. Une notification renouvelée a été examinée par l'inspecteur en chef et a été résolue par l'émission d'un avis clarificateur. Une autre notification renouvelée a été classée, la période légale étant écoulée. Au cours de l'année 2009, le département d'inspection a communiqué une notification aux services répressifs.

**Activités d'inspection du Bureau à l'échelle nationale**

*Inspections visant le traitement des données personnelles par les agences d'emploi (chasseurs de têtes)*

Au cours de l'année 2009, le Bureau a mené plusieurs inspections d'envergure nationale. L'une d'entre elles ciblait le traitement des données personnelles par les agences d'emploi (chasseurs de têtes).

Les agences de chasseurs de têtes ne traitent pas uniquement les données d'identification des personnes concernées, mais aussi des données révélant leurs compétences professionnelles et leurs traits de personnalité. Ces données sont essentiellement obtenues par le biais d'une interface internet ou par envoi normalisé. L'examen portait principalement sur les points suivants:

- base légale pour obtenir les données personnelles,
- conformité aux champ et finalités du traitement de données tels que définis,
- avis d'information sur les modalités du traitement de données,
- exactitude, intégrité et mise à jour des données personnelles traitées,
- devoir de destruction des données personnelles dès la réalisation du but original du traitement,
- adoption de mesures techniques, organisationnelles et de ressources humaines pour garantir la protection des données personnelles, y compris des mesures de prévention des risques d'erreurs humaines en formant les «personnes habilitées» à accéder aux données personnelles et à les traiter.

Ces inspections ont révélé que les responsables de traitement de données n'informaient pas correctement les personnes concernées de leurs droits garantis par la loi sur la protection des données. Le Bureau a émis un ordre enjoignant tous les responsables de traitement contrôlés à remédier aux manquements identifiés dans un délai déterminé. Dans deux cas, le Bureau a versé à la procédure administrative une proposition de sanctions financières.

*Inspections visant le traitement des données personnelles par les agences de voyages*
Conformément au plan des activités d'inspection de l'année 2009, le département d'inspection a également visité des agences de voyages, les confrontant à un questionnaire semblable à celui des agences de chasseurs de têtes et vérifiant également la conformité des contrats conclus avec les agents de traitement de données au sens de la loi sur la protection des données.

Les inspections ont révélé que les agences de voyages passées en revue traitaient les données personnelles adéquates aux fins données, les détruisaient de la manière prescrite et avaient pris des mesures techniques, organisationnelles et de ressources humaines appropriées pour garantir la protection des données personnelles, à l'exception d'un cas. Pour ce dernier, il s'est avéré que les responsables de traitement de données n'informaient pas suffisamment les personnes concernées au sujet des droits que leur garantit la loi sur la protection des données.

Tous les responsables de traitement de données réunissaient les données personnelles des personnes concernées par l'intermédiaire d'agents de traitement. Il s'est avéré à deux reprises que les contrats n'étaient pas conformes aux dispositions de la loi sur la protection des données, du fait que les agents de traitement ne définissaient pas une liste/un champ des données personnelles traitées, ni les modalités de leur traitement. Le Bureau a donné des instructions pour corriger les manquements identifiés, et elles ont toutes été suivies.

*Activités d'inspection spéciales*
Dans le cadre de l'adhésion de la République slovaque à l'espace Schengen, le département d'inspection a réalisé, en 2009, de nouveaux contrôles dans certaines ambassades de la République à l'étranger ainsi que dans les bureaux slovaques pertinents. Leur but était de vérifier si les responsables des systèmes d'archivage observaient bien la loi sur la protection des données et si les procédures d'émission des visas Schengen répondaient aux exigences du catalogue Schengen (recommandations et meilleures pratiques) en la matière.

Les départements consulaires des ambassades de la République slovaque à Londres et à Dublin ont été contrôlés en mai 2009.

Au troisième trimestre 2009, c'était au tour des départements suivants du bureau de la police des frontières et des étrangers du ministère de l'intérieur de la République slovaque: l'unité de contrôle des frontières de l'aéroport de Bratislava Ružinov, l'unité de coordination de l'exploitation des systèmes d'information du bureau de la police des frontières et des étrangers, l'unité de contrôle des frontières de Vyšné Nemecké, l'unité de contrôle des frontières de l'aéroport de Ko'ice, l'unité de contrôle des frontières de l'aéroport de Poprad et la direction de la police des frontières de Sobrance. Par ailleurs, en novembre 2009, une inspection a été menée à l'office de l'immigration du ministère de l'intérieur de la République slovaque ainsi qu'au centre d'asile de Rohovce, dans le but d'examiner le traitement des données personnelles des demandeurs d'asile.

*Coopération du département d'inspection avec les APD étrangères*
Au printemps et à l'automne 2009, le département d'inspection a participé aux ateliers internationaux organisés pour les inspecteurs des autorités de protection des données personnelles. À l'occasion du XIX$^{e}$ atelier, organisé à Prague en mars 2009, le département a présenté sa contribution au thème «Traitement des données à caractère personnel dans le secteur des soins de santé». Lors de la réunion de travail automnale des inspecteurs en octobre 2009 à Limassol, le Bureau a partagé les enseignements tirés de ses contrôles sur le traitement des données à caractère personnel par les employeurs, y compris la copie et la collecte de documents officiels.

En novembre 2009, les employés du Bureau ont participé à la Conférence internationale des commissaires à la protection des données et de la vie privée organisée à Madrid par l'Association francophone des autorités de protection des données. Au sommet de l'ordre du jour de la conférence figuraient la protection des données à caractère personnel dans le monde numérique et la protection de la vie privée des enfants. Après la conférence, les représentants du Bureau ont pris part à l'assemblée générale de l'Association francophone des autorités de protection des données.

**Flux transfrontaliers de données personnelles**

En 2009, le Bureau a approuvé huit flux transfrontaliers de données personnelles à destination de pays ne fournissant pas un degré de protection adéquat des données. Dans le cas d'une multinationale, des approbations de transferts de données personnelles ont été émises sur la base du respect de l'exigence d'adhésion des importateurs de données aux *Safe Harbour principles* (principes de la sphère de sécurité) et, dans les cas restants, via l'application, dans les contrats respectifs sur le transfert de données personnelles, des clauses contractuelles types pour les agents de traitement de données dans les pays tiers. Nous avons aussi rencontré des cas où le responsable de traitement de données – la société multinationale – appliquait à la fois les principes de la sphère de sécurité et les clauses types conçues pour les agents de traitement de données dans des pays tiers ne fournissant pas un degré de protection adéquat des données. Les flux transfrontaliers de données personnelles concernaient essentiellement les données personnelles d'employés et de clients d'entreprises internationales.

Au cours de l'année 2009, le département des relations étrangères a rendu 48 avis écrits en réponse à des questions soulevées par les responsables de traitement de systèmes d'archivage d'information ou par les cabinets d'avocats les représentant. Ces questions avaient principalement trait au transfert des données personnelles des employés, à la gestion des ressources humaines, au déclenchement d'alerte (*whistleblowing)* et au traitement des données personnelles des clients des responsables du traitement.

Il s'agissait de clarifier les modalités du flux transfrontalier de données personnelles entre:

- les responsables et les agents de traitement de données établis dans les États membres de l'Union,
- les responsables et les agents de traitement de données établis en Inde et en République de Corée,
- les responsables et les agents de traitement de données établis dans les États membres de l'Union avec un transfert à destination d'un pays tiers ne fournissant pas un degré adéquat de protection des données,
- le flux transfrontalier de données personnelles à des fins de déclenchement d'alerte.

**Coopération internationale**

Les activités internationales du Bureau résultaient pour l'essentiel de l'adhésion de la République slovaque à l'Union européenne, à travers la mise en place de groupes de travail sous ses auspices, ainsi que d'actes juridiques des Communautés européennes. De par son adhésion, la République slovaque est tenue à des obligations spécifiques au sein d'Europol, du système d'information Schengen, du système d'information douanier, du groupe de travail sur la coopération policière et judiciaire, du groupe de coordination du contrôle d'Eurodac et du groupe de travail SCH-EVAL (*Schengen Evaluation Working Group*). Dans la lignée du programme de travail 2009 préparé par la Commission européenne et la Commission permanente d'évaluation et d'application de Schengen, le groupe d'experts SCH-EVAL a mené:

- un bilan de l'application des principes sous-jacents du traitement de données à caractère personnel dans le SIS par les «anciens États Schengen» (Allemagne, France, Belgique, Pays-Bas et Grand-duché de Luxembourg),
- un bilan de la capacité à mettre en œuvre l'acquis de Schengen dans le domaine de la protection des données personnelles dans les pays candidats – la Bulgarie et la Roumanie.

Les conclusions et recommandations des rapports d'évaluation ont mis à jour, d'une part, les limites de l'application pratique de la Convention SIS et, d'autre part, une approche responsable des pays candidats évalués, tentant de répondre aux critères requis pour adhérer à l'espace Schengen. Les rapports d'évaluation finale ont été soumis à l'approbation du groupe de travail SIS / SIRENE et du Conseil.

*Dans le cadre des réunions bilatérales et régionales organisées en vue d'aborder des points spécifiques de la coopération et d'échanger les meilleures pratiques, les plus importantes étant:*

- la participation à la 11e réunion des autorités de contrôle pour la protection des données en Europe centrale et orientale (APD des pays CEE) en mai 2009,
- la réunion avec le contrôleur européen de la protection des données, M. Peter Hustinx, dans les locaux du Bureau en septembre 2009. M. Hustinx a été informé en long et en large des activités du Bureau et a discuté avec les employés du Bureau des enjeux et des

nouvelles priorités de la protection des données au sein de l'Union européenne, ainsi que de la possibilité de concentrer au mieux les efforts des différentes autorités de contrôle pour la protection de données. M. Hustinx a également visité le Conseil national de la République slovaque, où il a rencontré des membres de la commission parlementaire sur les droits de l'homme, les minorités et le statut des femmes. À cette occasion, une conférence de presse spéciale était consacrée à sa visite en Slovaquie,

- un échange complet des meilleures pratiques sur la politique des médias de masse, en vue d'améliorer la sensibilisation et d'ouvrir des possibilités de coopération avec le Bureau de la protection des données personnelles de la République tchèque, à Bratislava, en octobre 2009.

# Slovénie

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

En Slovénie, le cadre institutionnel et juridique moderne de la protection des données (et de l'accès aux informations publiques) s'aligne depuis des années sur «l'acquis communautaire».

S'appuyant sur les dispositions spécifiques de l'article 48 de la loi sur la protection des données personnelles[22] (LPDP), le commissaire à l'information a émis plusieurs avis préliminaires sur la législation en préparation, concernant la conformité de celle-ci à la protection des données personnelles. Parmi ses principaux accomplissements, citons les amendements et annexes à la loi sur les communications électroniques[23] (LCE) adoptés fin 2009. Ces amendements incluent l'anonymisation des numéros de téléphone repris sur les factures détaillées que reçoivent les abonnés, conformément à la directive «vie privée» (2002/58/CE). Les recommandations du groupe de travail «Article 29» (WP 113) relatives aux dispositions de la directive sur la conservation des données (2006/24/CE) ont également été prises en considération. La période de conservation des données est désormais réduite à 8 mois et ne peut dépasser 14 mois. La version amendée de la LCE limite également la période de conservation des données fournies et ramène l'enregistrement de ces données d'une durée indéterminée à une période limitée à 10 ans. L'un des principaux changements apportés à la LCE consiste en la communication à la police de données de trafic et de localisation afin de protéger la vie et l'intégrité physique d'une personne et en la compétence donnée au commissaire à l'information de surveiller les dispositions relatives à l'interception légale de communications.

Les autres grands textes législatifs examinés par le commissaire à l'information en 2009 traitaient de la procédure administrative générale, de la procédure pénale, des étrangers, des passeports, des frontières de l'État, des opérations bancaires, des affaires étrangères, de la santé, de la police, de la Croix-Rouge, du code familial, du blanchiment d'argent, de la prévention du financement du terrorisme, et des archives.

## B. Jurisprudence importante

En 2009, comme lors des années précédentes, le commissaire à l'information a eu à traiter plusieurs cas dont les médias nationaux se sont largement fait l'écho.

**Partis politiques**
Le commissaire à l'information a engagé une procédure de contrôle à l'encontre de deux partis politiques slovènes, suspectés de collecte et de conservation illégales de données personnelles à des fins de campagne électorale. La plainte a été déposée par plusieurs citoyens slovènes/électeurs inscrits résidant à l'étranger, qui ont reçu des contenus de marketing direct de la part des deux partis politiques, sans leur avoir donné leur consentement pour utiliser leurs données de contact à des fins de marketing. Lors de la procédure de contrôle, les partis politiques n'ont pas pu apporter un fondement légal à la collecte des données de contact des citoyens concernés. En conséquence de la violation établie, le commissaire à l'information a imposé aux deux partis une amende de 4170 euros chacun. De surcroît, les personnes civilement responsables au sein des partis ont dû s'acquitter d'une amende de 830 euros.

**Président du tribunal de district**
Le président du tribunal de district a été reconnu responsable du paiement d'une amende de 1660 euros pour deux délits de traitement illégal de données à caractère personnel. Il s'est avéré, lors de la procédure judiciaire, que la personne responsable avait collecté, puis traité, des données relatives aux appels passés par deux employés depuis des téléphones professionnels (données de trafic). Le but du traitement de ces données de trafic n'était ni déterminé ni légal, et leur traitement ultérieur non conforme à la loi. La décision du commissaire à l'information n'est cependant pas irrévocable. Conformément aux dispositions de la loi sur les tribunaux, la Cour suprême a également enquêté sur le travail du service de gestion du tribunal de district susmentionné.

Ce dossier reflétant purement et simplement des problèmes largement répandus en matière de respect de

[22] Journal officiel de la République de Slovénie, n° 94/2007

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

la vie privée au travail, le commissaire à l'information a réitéré son point de vue quant au fait que ce domaine mérite un cadre juridique amélioré. En effet, pratiquement un tiers des cas relevant de sa compétence a trait au respect de la vie privée au travail.

**Communication illégale de données à caractère personnel entre deux compagnies d'assurances**

Le commissaire à l'information a mis à l'amende deux compagnies d'assurances et les personnes civilement responsables du traitement illégal de données à caractère personnel. Dans le cadre de la procédure, le commissaire a établi que les données personnelles de 2382 particuliers ont ainsi été communiquées sans base légale ou sans le consentement personnel des personnes concernées.

La compagnie d'assurances qui avait fourni les données personnelles a été sanctionnée pour communication illégale de données à caractère personnel et traçabilité insuffisante des données fournies. Preuves à l'appui, le commissaire à l'information a mis à jour le traitement illégal des données de 26 particuliers, ce qui a valu à la compagnie une amende de 112 590 euros, tandis que la personne civilement responsable écopait d'une amende de 20 000 euros. La compagnie a porté l'affaire devant les tribunaux. Quant à l'autre, elle s'est vu infliger une amende de 108 420 euros pour acquisition illégale de données personnelles, et les personnes civilement responsables ont écopé chacune d'une amende de 20 000 euros. Cette compagnie a pour sa part fait usage de la possibilité offerte par la loi de payer immédiatement la moitié de l'amende.

Il s'agit des amendes les plus élevées imposées par le commissaire à l'information à ce jour. Celui-ci a souligné qu'à l'avenir, une telle communication illégale de données à caractère personnel entre responsables de traitement de données en possession de données sensibles ou de vastes bases de données sera vigoureusement sanctionnée.

**Protection des données dans le secteur bancaire**

Le commissaire a effectué des contrôles systématiques de la sécurité des données à caractère personnel dans le secteur bancaire (dans six des plus grandes banques), à savoir la légalité du traitement de données personnelles dans le cadre des transferts interbancaires de données relatives à la cote de solvabilité des clients, données qui alimentent le nouveau système SISBON, et la légalité de l'accès aux données de comptes bancaires des clients. Le commissaire à l'information a pu établir qu'aucune donnée n'avait été consultée illégalement dans le cadre des transferts de données interbancaires. Cependant, il a constaté la consultation non autorisée des données de comptes bancaires de certains clients (hommes politiques) bien connus dans deux des banques inspectées. Les employés non habilités qui ont consulté les données bancaires ont été sanctionnés en vertu de la loi générale sur les délits.

**Publication du courrier électronique et des questions d'un journaliste sur le site internet du commissaire à l'information**

Le commissaire à l'information a publié sur son site internet le courrier électronique envoyé par un journaliste, contenant des questions d'ordre journalistique et l'adresse électronique professionnelle du journaliste. Le courrier en question a également été envoyé à un certain nombre d'abonnés à la liste de diffusion du commissaire à l'information. Le journaliste a déposé plainte; toutefois, le commissaire à l'information n'a constaté aucune violation de la loi sur la protection des données personnelles et n'a pas ouvert de procédure de contrôle. Le commissaire à l'information défendait le raisonnement suivant: le courrier électronique a été envoyé à l'adresse professionnelle officielle du commissaire, conçue pour réceptionner des courriers de personnes physiques et morales au sujet du travail du commissaire à l'information. Le nom, le prénom et l'adresse électronique professionnelle du journaliste ne représentaient pas, dans le cas présent, des données personnelles protégées, le journaliste agissant en sa qualité de journaliste public, dont le nom est publié sur le site officiel du média. La publication de son courrier électronique n'a dès lors pas porté atteinte à sa vie privée et à sa dignité. Quant aux questions contenues dans le courrier, elles concernaient la nature publique du travail du commissaire à l'information et, de surcroît, le contenu des communications était destiné à être publié. En conséquence, les questions du journaliste ne peuvent être considérées comme une communication personnelle protégée mais comme une information publique.

**Publication d'une décision judiciaire dans le journal**
Un extrait d'une décision judiciaire contenant les données personnelles du plaignant a été publié dans un quotidien slovène. Le commissaire à l'information y a vu une violation de la loi sur la protection des données personnelles et a infligé une amende au propriétaire du journal et à la personne civilement responsable. L'affaire est importante, car le commissaire à l'information adopte ici le point de vue selon lequel des données personnelles contenues dans un arrêt judiciaire relatif à un personnage non public représentent des données personnelles protégées. La décision judiciaire ne peut dès lors être publiée que sous une forme anonymisée. Le commissaire à l'information invoque également, dans ce cas, qu'en cas de conflit entre, d'une part, le droit à la liberté d'expression et le principe constitutionnel connexe de publicité de la procédure judiciaire et, d'autre part, le droit à la protection des données, le droit à la protection des données du personnage non public prévaut. L'intérêt public ne doit pas être confondu avec ce qui intéresse le public et la seule curiosité du public ne peut justifier des entorses au droit constitutionnel à la protection des données personnelles.

## C. Questions diverses importantes

Outre ses missions 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, 10 demandes seulement ont été reçues en 2009 (contre 16 en 2008 et jusqu'à 40 en 2007). Proportionnellement, une baisse a été constatée dans le nombre de décisions émises – 6 décisions (4 autorisations, 2 refus) contre 17 en 2008 et 35 en 2007.

La situation relative à l'octroi de permis pour la **mise en rapport de systèmes de classement** n'a pas évolué en 2009: 8 décisions ont été rendues en 2009 comme en 2008 (contre 7 en 2007) en la matière.

En 2009, 71 plaintes ont été déposées auprès du commissaire à l'information en sa qualité d'organe compétent pour statuer sur le recours introduit par une personne concernée quant à son **droit à l'information**.

À la fin 2009, les systèmes d'archivage de données personnelles de plus de 11 000 responsables de traitement de données étaient enregistrés dans le **registre public** géré par le commissaire à l'information et publié sur son site internet. Les chiffres montrent une hausse d'environ 1000 nouvelles entrées par an.

Dans le cadre de ses **activités d'inspection** (en décembre 2009, neuf inspecteurs de la protection des données étaient au service du commissaire) en 2009, le commissaire à l'information a reçu 624 demandes et plaintes concernant des soupçons d'infraction à la loi sur la protection des données à caractère personnel, dont 219 dans le secteur privé (contre 256 en 2008) et 405 dans le secteur public (contre 379 en 2008). Si l'on compare ces chiffres aux années précédentes (635 cas en 2008, 406 cas en 2007 et 231 en 2006), la hausse significative de 76 % en 2007 et 56 % en 2008 est aujourd'hui en baisse. Comme les années précédentes, la plupart des plaintes avaient trait à la collecte illicite ou disproportionnée de données à caractère personnel, à la divulgation de données personnelles à des utilisateurs non autorisés, à une vidéosurveillance illégale, à une protection insuffisante des données personnelles, à une publication illicite de ces données, etc. On recense 163 procédures ouvertes pour des infractions administratives (contre 279 en 2008 et 133 en 2007).

En 2009, le nombre de demandes d'**opinions** et de clarifications **écrites** a donné lieu à 596 réponses écrites et à 1471 réponses succinctes de la part du commissaire à l'information (ainsi que plusieurs centaines de réponses verbales par téléphone). Au regard du chiffre de 853 cas en 2008 et de 1144 cas en 2007, ces chiffres indiquent clairement que le grand public reste 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 pas non plus étrangers.

Outre la publication sur son site internet d'avis non contraignants sous la forme d'explications écrites et la publication de diverses brochures portant sur la protection des données, le commissaire a, en 2009, continué à formuler des **orientations** sur des aspects spécifiques

de la protection des données. Elles ont pour objectif de fournir des instructions et des informations pratiques au public, aux personnes concernées et aux responsables du traitement de données, sous la forme d'une foire aux questions. Les réponses apportées doivent permettre de se conformer aux dispositions obligatoires de la loi sur la protection des données personnelles et/ou de toute autre législation. L'année dernière, le commissaire a préparé et publié sur son site internet des orientations relatives au code de conduite régissant la collecte des données à caractère personnel, à la protection des données personnelles dans les médias, à l'information et à la sensibilisation des consommateurs, à l'usurpation d'identité, à la protection des données des enfants en milieu scolaire, à la prévention et à la protection contre le cyberharcèlement et, enfin, à l'ingénierie sociale.

À l'occasion de la troisième **Journée européenne de la protection des données**, qui fêtait en 2009 son troisième anniversaire, le commissaire a organisé une table ronde sur le thème du respect de la vie privée au travail. Pour la troisième fois, le commissaire a décerné les prix des bonnes pratiques en matière de protection des données personnelles aux lauréats des secteurs public et privé. Les prix d'excellence de la protection des données ont été décernés à la société Cetis d. d. et au ministère de la défense de la République de Slovénie. En outre, et pour la première fois, des récompenses ont également été attribuées aux entreprises pouvant démontrer un haut niveau de sécurité des données personnelles grâce à leur certification ISO/CEI27001 de système de gestion de la sécurité de l'information.

**Coopération internationale**

*Coopération permanente avec les organes de l'Union européenne et du Conseil de l'Europe*

En sa qualité d'instance de réglementation nationale dans le domaine de la protection des données, le commissaire à l'information coopère en permanence avec les organes compétents de l'Union européenne et du Conseil de l'Europe, cette forme de coopération internationale étant régie par la directive 95/46/CE.

En 2009, le commissaire à l'information a participé activement à cinq groupes de travail à l'échelle communautaire, concernant le contrôle de la protection des données dans différents secteurs au sein de l'Union. Il s'agit du groupe de travail sur la protection des données à caractère personnel institué en vertu de l'article 29 de la directive européenne sur la protection des données, des autorités de contrôle communes pour Europol, l'espace Schengen et le système d'information douanier, ainsi que des réunions de coordination du contrôleur européen de la protection des données avec les autorités nationales pour la protection des données personnelles et du groupe de coordination du contrôle d'Eurodac.

En 2009, le commissaire à l'information a été élu vice-président de l'autorité de contrôle commune pour Europol et, dans le cadre de la coopération policière et judiciaire, il a régulièrement assisté aux réunions du groupe de travail pour la police et la justice.

Avec l'entrée de la Slovénie dans l'espace Schengen, le commissaire à l'information est devenu l'organe indépendant de supervision du transfert de données aux fins de la Convention et ses compétences ont été étendues à la surveillance de l'article 128 de la Convention de Schengen. En 2009, il a réceptionné 55 demandes d'accès à des données personnelles, dont aucune n'a été refusée. Le commissaire à l'information n'a pas reçu de plainte quant à l'exercice du droit d'accès de premier niveau des particuliers à leurs données contenues dans le SIS.

En 2009, le commissaire à l'information a participé au groupe d'évaluation SCH-EVAL de la Bulgarie et de la Roumanie dans le cadre de leur adhésion à l'espace Schengen.

Au niveau du Conseil de l'Europe, un représentant du commissaire à l'information a participé au comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Cette année, le Conseil s'est essentiellement attelé au projet de recommandation sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel collectées et traitées dans le cadre du profilage.

Le commissaire à l'information a également participé activement au sous-groupe «internet et technologies de l'information» sous les auspices du groupe de travail institué en vertu de la directive européenne sur la

protection des données. Le groupe de travail a adopté en 2009 deux documents importants, à savoir la recommandation sur la protection des données et les déchets d'équipements électriques et électroniques ainsi que le rapport et document d'orientation sur la tarification routière – le «Mémorandum de Sofia». Ce mémorandum est né de la recommandation du commissaire à l'information slovène. Le groupe de travail international sur la protection des données dans les télécommunications poursuit son travail dans des domaines tels que le *Deep Packet Inspection*, les données de géolocalisation, les sites de réseau social, etc.

*Autre coopération internationale*
Les représentants du commissaire à l'information ont aussi participé aux importants **événements internationaux** suivants:

Conférence de Barcelone «*High level meeting for joint proposal to draw up international standards on privacy and data protection*» (Réunion de haut niveau visant à une proposition conjointe en vue d'établir des normes internationales sur le respect de la vie privée et la protection des données);
Conférence de printemps des autorités européennes sur la protection des données personnelles, Édimbourg
2e *European Privacy Open Space and "re:publica"*, Berlin;
Conférence européenne sur la protection des données 2009, Bruxelles;
11e réunion des autorités de protection des données d'Europe centrale et orientale, Roumanie;
*Open Society Institute Meeting on Freedom of Information*, Budapest;
*Strengthening Data Protection in Israel*, Tel Aviv (projet de jumelage);
Conférence internationale des commissaires à la protection des données et de la vie privée, Oslo;
10e *Case Handling Workshop*, Limassol;
3e *Privacy Open Space Conference*, Vienne;
31e Conférence internationale des commissaires à la protection des données et à la vie privée, Madrid.

Le commissaire a par ailleurs mené une **coopération bilatérale**, principalement avec la Hongrie, la Serbie et le Monténégro.

Grâce à ces efforts et accomplissements, le commissaire jouit d'une très bonne réputation, de la confiance de l'opinion publique et d'une grande publicité auprès de celle-ci, comme en témoignent les résultats des enquêtes d'opinion publique. Selon les derniers résultats (janvier 2010) de l'enquête menée par le centre d'étude slovène de l'opinion publique, la confiance placée dans le commissaire à l'information croît de toute évidence. Parmi les autres institutions étudiées, la seule jugée plus fiable que le commissaire est la monnaie officielle, à savoir l'euro. Jouissant d'un pourcentage élevé de confiance de l'opinion publique (53,1 %), le commissaire devance haut la main toutes les autres institutions, telles que l'armée, le président de la République, le médiateur, les écoles et la police. Mentionnons également que, parmi toutes les institutions reprises dans l'enquête, le commissaire à l'information jouit du taux le plus faible de méfiance du public.

En mai 2009, sur la proposition du président de la République, l'assemblée nationale de la République de Slovénie a réélu Mme Nataša Pirc Musar pour un nouveau mandat de 5 ans au poste de commissaire à l'information, à la quasi-unanimité des suffrages.



## Espagne

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

Au cours de l'année 2009, les textes législatifs suivants relatifs à la protection des données ont été adoptés:

1. Loi n° 25/2009 du 22 décembre modifiant diverses lois pour leur adaptation à la loi 17/2009 sur le libre accès aux activités de services et à leur pratique.

   Cette loi modifie, entre autres, la loi sur la protection de la vie privée et libéralise la vente, la livraison, la mise en œuvre et la maintenance de nombreux services de sécurité, dont les systèmes de vidéosurveillance. Avant la promulgation de cette loi, l'installation de tels dispositifs n'était légale, conformément à la loi sur la protection des données, que si elle était réalisée par des sociétés certifiées par le ministère de l'intérieur. De plus, le contrat d'installation devait être notifié à la police. Ces exigences formelles ne sont plus en vigueur.

2. Loi n° 29/2009 du 30 décembre modifiant les règlements de publicité et de concurrence illégales en vue d'améliorer les droits des consommateurs et utilisateurs.

   Sans préjudice des dispositions des règles de protection des données, des services de la société de l'information et des règles de télécommunications, cette loi stipule que des communications répétées non sollicitées à des fins de marketing direct, par le biais de courriers électroniques ou de moyens équivalents, seront assimilées à une pratique déloyale, sauf dans des circonstances justifiées légalement par le respect d'une obligation contractuelle.

De plus, l'Agence espagnole de protection des données (AEPD) a poursuivi son travail en faveur d'une plus grande sécurité juridique et d'un système juridique national conforme à la loi sur la protection des données. Plus de 100 rapports ont été publiés par son service juridique, dans le respect de la loi sur la protection des données, concernant l'adoption de dispositions générales telles que:

- l'avant-projet de loi sur la lutte contre le blanchiment d'argent et le financement du terrorisme, déjà reporté à deux reprises,
- l'avant-projet de loi sur la santé en matière de sexualité et de procréation et sur l'avortement,
- l'avant-projet d'arrêté royal adoptant un ensemble minimal de données devant être intégrées aux rapports cliniques dans le système national de santé,
- l'avant-projet de dispositions portant exécution de la loi n° 11/2007 du 22 juin sur l'accès électronique des citoyens aux services publics, transposant en droit espagnol la directive 2006/123/CE.

### B. Jurisprudence importante

Avant de procéder à l'analyse des jugements spécifiques rendus par les tribunaux espagnols, il importe de mentionner qu'un nombre significatif de jugements concernant le droit à l'effacement de ses données des registres des baptêmes de l'Église catholique ont été rendus, tous s'alignant sur le jugement n° 4646/2008 de la Cour suprême du 19 septembre, abordé plus en détail dans le douzième rapport annuel du groupe de travail «Article 29» sur la protection des données. Pour cette raison, les analyses suivantes ont été menées sans tenir compte de ces jugements.

**Audience nationale**

Au cours de l'année 2009, l'Audience nationale d'Espagne a été amenée à se prononcer sur 240 recours introduits à l'encontre de décisions de l'Agence espagnole de protection des données, dont 162 ont été irrémédiablement rejetés (68 %). Parmi les requêtes retenues (17 partiellement et 61 sur tous les points), il convient de noter que beaucoup étaient fondées sur différentes interprétations des preuves, et non sur l'application de la loi. Les décisions suivantes méritent que l'on s'y arrête:

- Le jugement du 17 mars était le premier à traiter d'un recours introduit à l'encontre d'une décision de refus d'un transfert de données personnelles à destination d'un pays tiers.
- Dans son jugement du 22 avril, l'Audience a estimé que l'enregistrement d'une personne sans son consentement sur un fichier vidéo stocké sur un CD, à faire valoir comme preuve dans le cadre d'un procès, ne relève pas du champ d'application de la loi sur la

protection des données, car une telle donnée ne fait pas partie et n'est pas destinée à faire partie d'un système d'archivage.
- Dans son jugement du 9 juillet, l'Audience a estimé que la publication, par un journal, d'images d'une victime d'attaque terroriste présentant des lésions irréversibles du cerveau était disproportionnée et fait primer le droit à la protection des données sur le droit à la liberté d'information.
- Le jugement du 9 octobre précise que les systèmes d'archivage détenus par les plaignants sont soumis à la loi sur la protection des données et, partant, aux pouvoirs de contrôle de l'Agence espagnole de protection des données.
- Le jugement du 26 novembre a confirmé les sanctions infligées par l'Agence espagnole de protection des données à l'encontre d'une entreprise qui a traité les données personnelles d'un mineur sans le consentement de ses parents, pour lui offrir une carte de crédit dans le cadre d'une campagne de marketing direct.

**Cour suprême**

Pour sa part, la Cour suprême a confirmé tous les critères de l'Agence espagnole de protection des données dans 16 de ses 19 jugements portant sur les décisions de l'Agence, dont les suivants:
- Le jugement du 28 avril a conclu que la loi espagnole s'applique à un système d'archivage stocké dans un serveur situé aux États-Unis, dont les données sont traitées en vue de mener une campagne publicitaire gérée par une entreprise espagnole et ciblant des citoyens espagnols.
- Le jugement du 17 novembre a confirmé que la dérogation permettant la divulgation de données personnelles aux tribunaux ne s'applique que lorsque les tribunaux en question en font directement la demande.

**Résolutions de l'autorité espagnole de protection des données**

Le nombre d'infractions signalées à l'Agence en 2009 a entraîné une hausse de 75 % des actions entreprises, dépassant les 4100 unités (les principaux secteurs inspectés étant les télécommunications, les organismes financiers et la vidéosurveillance). Toutefois, on a pu observer, dans le cas des résolutions concernant des procédures répressives à l'encontre de sociétés privées, que le secteur des télécommunications et les institutions financières, bien qu'occupant la première et la troisième place en termes de nombre de procédures, affichent une diminution de 10,34 % et 21,26 % respectivement. Par ailleurs, la vidéosurveillance privée pour raisons sécuritaires a grimpé à la deuxième place, avec une croissance de 229,55 % par rapport à l'année précédente. En outre, dans un contexte de crise économique tel que celui que nous avons connu en 2009, on a pu observer une hausse exponentielle des actions dérivées ou liées à des réclamations pour défaillance. Les résolutions faisant état d'une infraction à la loi sur la protection des données par les administrations publiques ont crû d'environ 12,5 %.

Les pénalités infligées ont représenté la somme de 24 872 979,72 euros au total. S'il s'agit là d'une hausse de 12,99 % par rapport à l'année précédente, le chiffre se rapproche du volume de sanctions déclarées en 2006, à la différence notable que le nombre de procédures répressives résolues en 2009 est supérieur de 235 % à celui de 2006. C'est précisément cette hausse substantielle des procédures répressives et non le montant des sanctions déclarées qui explique le montant des pénalités infligées. Les pénalités mineures présentent la plus forte hausse (44,76 %), tandis que les amendes punissant des infractions graves restent stables et que les sanctions de faits très graves ont diminué de près de 6 %. Au regard du total des décisions répressives rendues, on constate une baisse notable de la responsabilité des contrevenants dans 40,72 % des cas. Si l'on analyse les données soumises, il convient de conclure que la hausse quantitative des sanctions, conséquence de l'augmentation antérieure du nombre de plaintes, n'empêche pas l'appréciation d'une meilleure conformité à la loi sur la protection des données (avec une croissance du nombre de violations de pure forme), de la réduction des violations très graves et de la diminution de la responsabilité en cas de violation.

Quoi qu'il en soit, les résolutions suivantes sont particulièrement dignes d'intérêt:
- Résolution PS/00053/2009 du 13 janvier. Le Bureau britannique du commissaire à l'information a signalé à l'AEPD qu'une entreprise espagnole pratiquait des appels commerciaux non sollicités («appels à froid») auprès de citoyens britanniques. L'entreprise en question n'était pas en mesure de prouver l'origine des

données, elle n'avait jamais eu la moindre relation contractuelle avec les personnes concernées et n'avait pas obtenu leur consentement. L'Agence lui a par conséquent infligé une amende de 60 001 euros pour violation grave de la loi sur la protection des données.

- Résolution PS/00593/2008 du 20 avril. Une base de données médicales de 140 travailleurs avait été découverte via un programme de partage de fichiers P2P. Le responsable du traitement de données, une société spécialisée dans la prévention des risques professionnels, a essayé de rejeter la faute sur un ancien employé. L'Agence lui a infligé une amende de 60 001 euros pour ne pas avoir pris les mesures de sécurité appropriées, ce qui constitue une violation très grave de la loi sur la protection des données.
- Résolution PS/00183/2009 du 14 septembre. Une billetterie en ligne offrait deux places de concert à l'utilisateur qui parvenait à envoyer une publicité spécifique le plus grand nombre de fois. L'Agence a estimé que la billetterie s'adonnait ainsi à l'envoi de communications commerciales non sollicitées, et lui a imposé une amende de 30 001 euros pour violation grave de la loi sur les services de la société de l'information.
- Résolution PS/00233/2009 du 20 octobre. Une société de télécommunications a vendu les créances en souffrance de ses clients à des entreprises tierces. La base de données contenait des créances inexistantes, incertaines ou contestées, qui étaient même ajoutées à l'historique de crédit de certaines personnes concernées. L'Agence a imposé une amende de 420 000 euros pour violation très grave de la loi sur la protection des données.
- L'intégralité des textes des résolutions adoptées par l'Agence espagnole de protection des données est disponible à l'adresse https://www.agpd.es/ (en espagnol).

## C. Questions diverses importantes

**Faciliter le respect de la loi: une garantie pour les citoyens.** L'Agence a renforcé sa politique de sensibilisation, convaincue du fait que faciliter le respect de la loi se traduira par une augmentation des garanties offertes aux citoyens. C'est ainsi que s'est tenu en janvier 2009 le 2e «atelier ouvert» annuel (*Open Session*), qui a attiré quelque 700 participants, et que le catalogue de guides pratiques a été étoffé, avec la publication de nouvelles brochures de recommandations destinées aux internautes et concernant la vidéosurveillance et la protection des données sur le lieu de travail, ainsi qu'un guide sur la vidéosurveillance et un autre relatif aux droits des garçons et des filles et aux devoirs des mères et des pères (ces deux derniers guides étant en anglais).

La ligne d'assistance se révèle toujours être un canal d'information très utile dans le cadre de la politique d'information de l'Agence. En témoigne, année après année, la hausse des consultations. Quant au service juridique, il a traité un total de 679 consultations, dont 359 (54 %) émanaient des administrations publiques et 313 (les 46 % restants) du secteur privé.

Ces politiques continuent de produire des résultats. En 2009, près de 400 000 dossiers ont été enregistrés dans le registre général de la protection des données (RGPD), soit une hausse de plus de 50 % par rapport à 2008, pour un montant total de 1 647 756 dossiers. Le système de notification simplifiée NOTA, qui facilite la notification via internet et est utilisé dans presque 90 % des notifications manuelles, a incontestablement contribué à cette augmentation. Qui plus est, l'utilisation de certificats numériques gagne du terrain, ce format étant même utilisé dans une notification sur cinq.

L'augmentation des enregistrements est plus marquée dans la sphère privée, avec une croissance de 63 %, tandis que le secteur public affiche une hausse de près de 50 % dans les dossiers des administrations locales, sachant que les dossiers municipaux dans le RGPD représentent près de 96 % de la population espagnole.

L'offre de nouveaux canaux visant à faciliter le respect de la loi a donné une impulsion positive au programme EVALÚA, un test d'auto-évaluation en ligne permettant aux entreprises et autorités locales de juger de leur conformité à la loi. Ce test répond gratuitement aux demandes régulièrement posées par les agents de traitement de données personnelles.

**Internet: à nouveaux services, nouveaux défis.** L'examen de l'utilisation libre que les utilisateurs font des services internet dépend des conditions fixées unilatéralement par le fournisseur de services. Il convient dès

lors de donner la priorité aux politiques actives visant à établir une relation avec les fournisseurs de ces services. À cet égard, l'AEPD a communiqué les recommandations de l'étude préparée en collaboration avec INTECO sur Facebook et Tuenti, lesquelles insistent sur l'amélioration des politiques de respect de la vie privée en vue de fournir des informations claires et compréhensibles, ainsi que sur la nécessité de mettre en place des politiques de respect de la vie privée par défaut et d'effacer tout le contenu du profil dès la demande de désinscription.

En 2009, 156 procédures ont été menées dans le cadre de procédures préliminaires spécifiquement liées aux services fournis via internet. La nouveauté est que 18 de ces procédures ont été lancées suite à 31 plaintes concernant des utilisateurs des réseaux sociaux Facebook et Tuenti, la majorité ayant trait à la diffusion de photos de tiers sans leur consentement.

La majorité des actions restantes concernait aussi la diffusion non autorisée de données personnelles par le biais d'internet: 37 renvoient à des blogs ou forums, 13 à des services d'hébergement de vidéos – Youtube pour l'essentiel – et 38 à d'autres types de site internet, comme des sites d'entreprise, des recueils de rapports juridiques et des sites personnels. Vingt-huit autres réclamations concernaient des sites publicitaires, des services de rencontre en ligne ou des services de courrier électronique. Dans la plupart des cas, il était question de la diffusion non autorisée de données.

En outre, 10 des actions introduites avaient trait à des incidents de divers types liés à des achats en ligne ou à des opérations commerciales électroniques. Enfin, signalons cinq procédures préliminaires conduites dans le cadre de services de moteur de recherche et du placement d'informations personnelles dans des répertoires ou moteurs de recherche de personnes.

**Mineurs: une protection nécessaire compte tenu de leur présence grandissante sur le web.** L'utilisation des réseaux sociaux s'est imposée comme un passage quasi obligé dans le développement social des mineurs, qui se voient offrir un nouveau moyen de contact avec le monde extérieur. Cependant, ils risquent, dans une très large mesure, de présenter un déficit de base quant à savoir comment exercer un réel contrôle sur leurs informations.

Les réglementations de protection des données interdisent aux mineurs de moins de quatorze ans de s'inscrire sur un réseau social sans le consentement de leurs parents. Pour l'Agence, le respect de cette obligation est une priorité. En fait, le contrôle de l'accès des mineurs était une exigence sans cesse formulée lors des réunions organisées avec les responsables concernés de Tuenti et Facebook.

En réponse aux demandes de l'AEPD, Tuenti a présenté un système de vérification de l'âge qui analyse les profils d'utilisateurs suspects et effacent ceux qui ne peuvent prouver leur âge. De même, il a entrepris de renforcer les processus d'élimination des profils existants et de développer des systèmes de vérification des nouveaux profils suspects. Il a par ailleurs publié des informations concernant la modification de la politique de respect de la vie privée, en configurant par défaut le niveau maximum de protection pour les utilisateurs de moins de 18 ans. L'Agence a également demandé aux responsables de Facebook de relever l'âge limite de 14 ans pour les utilisateurs espagnols.

Il est cependant nécessaire d'intégrer une formation adéquate sur la protection des données et le respect de la vie privée aux manuels scolaires et, dans le même ordre d'idées, les administrations publiques et les écoles doivent mettre à la disposition des élèves des technologies qui limitent l'accès aux services web par les enfants de moins de 14 ans. Dans ce contexte, le document d'identité électronique s'avère être l'un des outils les plus efficaces pour certifier l'âge sur internet. L'Agence accorde une extrême importance à la mise en œuvre d'initiatives adéquates pour munir les plus de 14 ans des moyens numériques leur permettant de prouver qu'ils ont l'âge requis pour consentir au traitement de leurs données.

**Vidéosurveillance: vivre avec des garanties.** La vidéosurveillance pour des raisons sécuritaires est devenue une réalité omniprésente. Chaque année, on observe une croissance significative des dossiers de vidéosurveillance, comme en 2009, où les dossiers enregistrés dans le registre général de protection des données ont

augmenté d'environ 240 % (soit plus de 37 000 dossiers) dans la sphère privée. Dans le secteur public, il s'agit d'une croissance de 60 % (soit 578 dossiers supplémentaires).

L'étude 2009 du CIS (centre espagnol de recherches sociologiques) en témoigne: 68,7 % des citoyens sont favorables à l'installation de dispositifs de vidéosurveillance, contre 10 % qui s'y opposent. Il n'empêche qu'un nombre croissant de plaintes sont déposées concernant des violations de la loi sur la protection des données dans le cadre de la vidéosurveillance, entraînant une hausse de 230 % des procédures répressives abouties.

Quant aux caméras permettant la transmission d'images par le biais d'internet, l'AEPD a constaté, dans le cadre d'une inspection sectorielle, que la majorité d'entre elles permettent d'identifier les personnes filmées. Principale irrégularité constatée, les mécanismes du contrôle d'accès aux images sont souvent désactivés par le fabricant ou nécessitent un nom d'utilisateur et un mot de passe par défaut. Le manque de diligence qui caractérise le contrôle d'accès entraîne une vulnérabilité qui permet l'accès de tiers en laissant la caméra en mode *«open door»*. Un train de recommandations est proposé, dont la nécessité de permettre le contrôle d'accès aux images au moyen de noms d'utilisateur et de mots de passe. À la suite de l'inspection, sept procédures répressives ont été ouvertes et conclues.

**Secteur de l'emploi: trouver l'équilibre entre droits et devoirs.** L'éventail de traitements de données personnelles menés dans le secteur de l'emploi a incité l'AEPD à rédiger un guide sur la protection des données dans les entreprises, afin de répondre aux aspects pratiques que ces dernières rencontrent régulièrement. Le guide suggère des critères de conformité aux règlements de protection des données à caractère personnel et formule des recommandations spécifiques sur le traitement des données spécialement protégées, plus particulièrement les données liées aux soins de santé et à l'affiliation syndicale, ainsi que sur les garanties à respecter dans le cadre de la prévention des risques professionnels.

Bien qu'ils ne traitent pas nécessairement de données personnelles, le guide intègre aussi des recommandations concernant la mise en œuvre de systèmes internes de déclenchement d'alerte (*«whistleblowing»*) au sein de l'entreprise, tout en garantissant la protection des employés. Le chapitre consacré aux contrôles exercés par l'employeur présente les règles applicables aux contrôles biométriques, à la vidéosurveillance sur le lieu de travail ou à l'utilisation d'outils technologiques fournis par l'employeur, ainsi qu'au contrôle de l'absentéisme au travail.

**Flux internationaux de données: entre flexibilité et mondialisation.** Les transferts internationaux de données à partir de l'Espagne se sont mondialisés pour atteindre aujourd'hui les quatre coins du globe. Le nombre d'autorisations a augmenté de 25 %, les États-Unis représentant le premier pays de destination, malgré une baisse du nombre de transferts. On constate une croissance impressionnante de 100 % vers les pays d'Amérique latine (132 autorisations), tandis que l'Asie maintient un volume constant d'autorisations (115). Sur le continent africain, les transferts internationaux se concentrent sur le Maroc (19) et la République d'Afrique du Sud (3). Quant à l'Australie, elle apparaît comme une destination émergente.

La recherche de procédures plus flexibles pour l'autorisation de transferts internationaux a engrangé des succès en 2009. L'AEPD a autorisé le premier transfert basé sur des règles d'entreprise contraignantes (REC) et a participé, dans le cadre d'une procédure coordonnée, à la défense de dix requêtes de ce type de garantie devant d'autres autorités de l'Union européenne.

On peut affirmer, en bref, que nous assistons à une augmentation constante des flux internationaux de données, mettant l'accent sur la délocalisation des services et des procédures d'autorisation plus flexibles. Cette réalité nous place devant l'urgence de dégager des normes contraignantes devant garantir la protection de la vie privée dans un monde globalisé.

**2009: Madrid, capitale mondiale du respect de la vie privée. La résolution de Madrid: lieu de rencontre pour une réglementation mondiale.** En 2009, l'AEPD a organisé la 31e Conférence internationale des commissaires à la protection des données et à la vie privée – le plus grand forum mondial dédié à la vie privée et le lieu de rencontre des commissaires à la protection des données et à la vie privée des quatre coins du monde, ainsi que

des représentants d'organes publics et privés et de la société civile – faisant de Madrid l'épicentre mondial de la vie privée du 2 au 6 novembre. La Conférence a réuni plus d'un millier de personnes issues de 83 pays.

Inaugurée par Leurs Altesses Royales le Prince et la Princesse des Asturies, la conférence a investi le Palais des Congrès de Madrid, sous le slogan «*Privacy: today is tomorrow*» (La vie privée: aujourd'hui, c'est déjà demain). Une centaine d'intervenants ont participé à plus de vingt sessions, dont le ministre espagnol de l'intérieur Alfredo Pérez Rubalcaba, la secrétaire d'État américaine à la sécurité intérieure Janet Napolitano, l'inventeur du téléphone mobile Martin Cooper, le co-inventeur de la famille de protocoles internet TCP/IP Vinton Cerf, et le ministre marocain de l'industrie, du commerce et des nouvelles technologies Ahmed Reda Chami. Mais la plus grande réussite de cette manifestation réside dans les avancées réalisées en vue d'un instrument juridique universel et contraignant en matière de vie privée, contribuant à une meilleure protection des droits et libertés individuels dans notre monde globalisé, fruit d'un très vaste consensus social et institutionnel.

L'adoption de la «résolution de Madrid» marque une avancée majeure dans le sens de la «proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles». Cette proposition vise, en premier lieu, à promouvoir à l'échelle internationale le droit à la protection des données et à la vie privée, en offrant un modèle de réglementation capable de garantir un haut degré de protection et pouvant être adopté dans chaque pays. Elle vise ensuite à faciliter le flux international de données personnelles et à contribuer à triompher des obstacles existants.

Bien qu'elle n'ait pas la valeur d'un accord international ou d'un règlement de force exécutoire, cette convention n'en demeure pas moins un texte de référence tout à fait légitimé par la grande participation de la communauté internationale de la protection des données et de la vie privée à sa préparation, mais aussi par l'inclusion d'éléments présents dans tous les systèmes valides de protection des données actuellement en vigueur et par le soutien qu'elle a reçu de tous les commissaires présents à la Conférence internationale. Par conséquent, la promotion et la diffusion de ce texte parmi les organisations privées, les experts et les organismes publics nationaux et internationaux feront partie des priorités de l'AEPD au cours de l'année 2010.

## 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 suédois 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 personnelles 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 suédois 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 (PTS) 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 en avril 2004. L'Agence de protection des consommateurs (Konsumentverket) est chargée de veiller au respect de la loi relative aux pratiques de marketing.

La ***directive sur le respect des droits de propriété intellectuelle*** (IPRED, *Intellectual Property Rights Enforcement Directive*) a été transposée en droit suédois par le biais de divers amendements à des lois nationales, entrés en vigueur le 1er avril 2009. Ces amendements facilitent l'enquête sur des cas suspects de partage illégal de fichiers. L'une de ses spécificités réside dans le fait que les organisations chargées de protéger la propriété intellectuelle – dès lors qu'elles soupçonnent qu'une personne a été impliquée dans des partages de fichiers de pair à pair – peuvent s'adresser à un tribunal et demander que les fournisseurs d'accès internet divulguent les informations en leur possession sur le propriétaire de l'adresse IP en question. Quelques procès ont déjà eu lieu et une affaire est actuellement en instance devant la Cour d'appel de Svea.

Au 1er décembre 2009, l'Établissement radio de la défense nationale (FRA) s'est lancé progressivement dans la collecte de renseignements par câble, en vertu de la ***loi de surveillance des signaux***, entrée en vigueur le même jour. Cette nouvelle loi habilite le FRA à collecter des renseignements soit par voie aérienne, c.-à-d. ciblant les signaux radio, soit par câble. Jusqu'à l'entrée en vigueur de la nouvelle loi, aucun renseignement ne pouvait être collecté par câble. Or, une part croissante du trafic international, qui véhicule les informations intéressantes, est désormais transmise par câble, rendant nécessaire l'introduction d'une législation neutre sur cette technologie. Le Conseil de l'inspection des données est responsable du contrôle du traitement des données personnelles entrepris par le FRA. Le 12 mars 2009, le gouvernement a décidé de confier au Conseil de l'inspection des données la tâche spéciale de superviser les activités sous l'angle du respect de la vie privée. Le Conseil est assisté par un groupe consultatif composé de membres du Riksdag (le Parlement suédois). Il transmettra ses conclusions au gouvernement en décembre 2010.

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 en mars 2009.

Comme nous le signalions déjà l'année dernière, une commission d'enquête a été mise sur pied en 2006 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 l'aspect de l'enregistrement des prescriptions. La ***loi sur les données des pharmacies*** est entrée en vigueur en juillet 2009 et le monopole d'Apoteket AB a été aboli.

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'a toujours pas été transposée en droit suédois. À ce jour, rien n'indique quand le gouvernement soumettra un projet de loi au Riksdag (le Parlement suédois).

Fin novembre 2009, la Suède a signé le ***paquet Télécom de l'Union européenne*** dont les règles visent à renforcer les droits des consommateurs dans leurs relations avec des opérateurs de téléphonie et internet. Il revient à présent au gouvernement de présenter un projet de loi sur ce «paquet télécom», qui sera mis en œuvre au plus tard au printemps 2011.

En mai 2009, une commission d'enquête a soumis un rapport sur la ***protection de la vie privée dans le cadre de la vie professionnelle.*** La commission propose une nouvelle loi devant préciser et renforcer la protection de l'employé. Cette loi ne concernerait que des mesures mises en œuvre par les employeurs et destinées aux employés. Les examens médicaux et les différents types de surveillance sont autant d'exemples de questions que pourrait couvrir la loi proposée. La commission appelle à consulter différents acteurs du grand public, dont le Conseil de l'inspection des données. Le gouvernement n'a pas encore pris de décision quant à sa volonté de soumettre un projet de loi.

En février 2008, le gouvernement a mis sur pied une commission d'enquête chargée de passer en revue la législation en matière de vidéosurveillance et d'y consacrer un rapport. Ce dernier, intitulé ***Une nouvelle loi sur la vidéosurveillance,*** a été présenté au gouvernement en octobre 2009. Actuellement, la vidéosurveillance est régie par deux lois différentes, dont le champ d'application dépend de l'objet de la vidéosurveillance. Parmi les utilisateurs potentiels de la vidéosurveillance, beaucoup jugent cette situation complexe. La commission propose donc en premier lieu d'adopter une loi unique régissant tous les types de vidéosurveillance. Dans ce contexte, il est également proposé que le Conseil de l'inspection des données puisse jouer un rôle central dans le contrôle de l'application de la nouvelle loi. Celle-ci est appelée à prendre effet en janvier 2011.

Le gouvernement a présenté un projet de loi proposant des ***amendements à la loi constitutionnelle***. Une nouvelle disposition induirait une protection contre les atteintes graves impliquant la supervision ou la cartographie de la situation personnelle des individus. Les amendements devraient entrer en vigueur en janvier 2011.

Nous rapportions déjà l'année dernière l'existence de problèmes liés aux informations en matière de crédits, du fait que ces informations sont divulguées sur des sites internet sous le couvert d'une protection constitutionnelle de l'information et des déclarations (un amendement à la loi fondamentale sur l'expression de 2003). Cet amendement permettait de divulguer des informations de crédit à tout un chacun sur des sites internet, sans avoir à respecter les règles strictes de la ***loi sur les informations en matière de crédits***. Cette situation avait donné lieu à des violations de la vie privée et à de nombreuses plaintes. Le Conseil de l'inspection des données a, à plusieurs reprises, écrit au gouvernement au sujet de ces problèmes. Le ministre de la justice a annoncé la soumission d'un projet de loi au printemps 2010.

En décembre 2009, le gouvernement a mis sur pied une commission d'enquête chargée de présenter une proposition réorganisant les ***activités de lutte contre le dopage***. L'une de ses tâches consiste à examiner les possibilités de créer une organisation nationale antidopage indépendante, dont la responsabilité serait partagée par l'État et l'organisation centrale des sports. Il conviendra également d'examiner la possibilité d'y associer d'autres parties prenantes susceptibles de collaborer aux activités antidopage. La commission rendra son rapport au gouvernement en octobre 2010.

## B. Jurisprudence importante

### Arrêt de la Cour administrative suprême suédoise sur les adresses IP

Une affaire devant élucider si les numéros IP peuvent constituer des données personnelles a finalement abouti en 2009. Une organisation privée voulant garantir ses intérêts de droit d'auteur avait utilisé un logiciel spécial pour retrouver les internautes s'adonnant à du partage de fichiers. En 2005, le Conseil de l'inspection des données avait conclu que, dans le cas présent, la collecte et le

traitement de numéros IP s'apparentaient au traitement de données personnelles. Appel a été interjeté contre la décision du Conseil devant le tribunal administratif du comté et la Cour administrative d'appel, qui ont confirmé tous deux la position du Conseil. Saisie d'un recours, la Cour administrative suprême a décidé en avril 2009 de le rejeter. L'arrêt de la Cour administrative d'appel prévaut donc, et la décision du Conseil de l'inspection des données selon laquelle un numéro IP peut être une donnée personnelle reste valide.

Dans le rapport de l'année dernière, le Conseil de l'inspection des données exposait une affaire impliquant des ***systèmes de billetterie basés sur les techniques RFID utilisant des cartes à puce.*** En 2006 et 2008, le Conseil a effectué des contrôles concernant les nouveaux systèmes de billetterie des sociétés de transport utilisant des cartes à puce qui laissent des traces électroniques (systèmes basés sur les techniques RFID). Le Conseil de l'inspection des données a décidé que les données personnelles enregistrées lorsque les passagers utilisent leur billet électronique ne peuvent être conservées que pendant 60 jours, après quoi elles ne doivent plus permettre une identification du passager. L'une des sociétés concernées a fait appel de la décision, arguant que les informations relatives aux voyageurs devaient être assimilées à des documents officiels et, par conséquent, devaient être conservées en l'absence de règles de suppression spécifiques, conformément à la loi sur les archives. Le tribunal administratif du comté a rejeté la décision du Conseil en janvier 2009 et a renvoyé l'affaire. Se fondant sur l'applicabilité de la loi sur les archives, le Conseil de l'inspection des données a conclu en l'absence d'obligation de supprimer les informations ou de les rendre anonymes. Il a cependant réitéré son point de vue quant au fait que les informations détaillées sur le mode d'utilisation des transports publics par les particuliers ne peuvent être conservées pendant une durée indéfinie. Par conséquent, en juin 2009, le Conseil a adressé un courrier au gouvernement dans lequel il pointe la nécessité d'une nouvelle législation à cet égard.

L'année dernière, le Conseil de l'inspection des données a également donné des informations concernant ***la vidéosurveillance dans les écoles***. Cette initiative se justifiait suite aux résultats d'un questionnaire en ligne lancé en 2008, dont il ressortait que la vidéosurveillance dans les écoles 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 alors inspecté sept écoles et découvert que la vidéosurveillance des élèves durant les heures de cours était 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 dressé une liste de points à contrôler en vue d'aider les écoles à déterminer quand la vidéosurveillance est acceptable. Un appel a été introduit à l'encontre des décisions du Conseil d'octobre 2008 devant le tribunal administratif du comté, qui s'est prononcé en septembre 2009. Les appels ont été rejetés et les décisions du Conseil confirmées. Cependant, deux des cinq décisions font l'objet d'un recours devant la Cour administrative d'appel, où les affaires sont toujours en instance. En 2009, le Conseil de l'inspection des données a visité quatre nouvelles écoles et découvert que le traitement de données comporte toujours une série de lacunes et que les écoles ont des connaissances insuffisantes, voire inexistantes, quant à la conservation des données personnelles des élèves. Il n'existe pas de procédure pour la suppression des données dont la conservation ne se justifie plus.

## C. Questions diverses importantes

### Le procès Pirate Bay

Le procès intenté à l'encontre des quatre individus qui se cachaient derrière le site de partage populaire *«The Pirate Bay»* a débuté en février 2009 devant le tribunal de district de Stockholm. Le tribunal a rendu son verdict en avril. Les quatre cofondateurs de *«The Pirate Bay»* ont été condamnés à un an de prison et à une amende de 3 000 000 euros, dont ils sont conjointement et solidairement redevables. Les médias du monde entier ont suivi le procès et commenté la décision. *The Guardian* a écrit dans ses colonnes: «Le consortium de médias et de labels musicaux à l'origine des poursuites judiciaires savourera sa victoire des années durant. La décision est historique, incontestablement, mais elle apporte plus de questions que de réponses.» Les accusés ont interjeté appel de la sentence devant la Cour d'appel de Svea (*Svea hovrätt*), et l'affaire est en instance.

Au printemps 2009, le Conseil de l'inspection des données a invité des représentants de certains des plus grands ***sites*** suédois ***de réseau social***, dans le but d'élaborer des recommandations sur les conditions d'utilisation et le traitement des plaintes. En novembre, le résultat de cette collaboration a été présenté, sous l'intitulé «***Secure your site – Guidelines for member conditions as regards sites for young people***» (Sécurisez votre site – Lignes directrices relatives aux conditions d'adhésion aux sites pour les jeunes).

Au cours de l'année 2009, le Conseil de l'inspection des données a été saisi de plusieurs cas portant sur la ***publication de données à caractère personnel sur internet***. Trois d'entre eux concernaient des sites qui publiaient, par exemple, les noms et adresses de personnes condamnées pour différents ***crimes sexuels***. Le Conseil a transmis les dossiers à la police. Une autre plainte déposée auprès du Conseil de l'inspection des données avait trait à un site sur lequel des ***individus pouvaient classer et commenter des entreprises***, voire, parfois, des particuliers. Le Conseil a estimé que le site était responsable dans une certaine mesure et que le traitement n'était pas conforme à la loi sur la protection des données personnelles. Les informations ont été supprimées du site et le dossier est clos. En août 2009, les autorités policières de Skåne, au sud de la Suède, ont annoncé leur intention de ***publier sur internet des photos issues de caméras de surveillance*** afin d'obtenir l'aide du grand public pour identifier des suspects. Depuis lors, des photos d'enquêtes concernant, par exemple, des agressions, des fraudes ou des vols, ont été publiées. Leur publication a suscité de nombreuses réactions et le comité de la police nationale suédoise a sollicité l'avis du Conseil de l'inspection des données sur cette publication. Ce dernier a répondu que ce type de publication devait rester exceptionnel et que les conditions préalables à une publication devaient être régies par une loi. L'avis du Conseil a dès lors été transmis au ministère de la justice.

Le Conseil de l'inspection des données a également produit un nouveau rapport, intitulé ***Respect de la vie privée en 2009***, qui, comme l'année dernière, contient un aperçu complet des nouvelles lois, propositions, décisions et techniques publiées au cours de l'année en relation avec la protection de la vie privée.

**Réunion des commissaires nordiques à la protection des données**

Le Conseil de l'inspection des données a accueilli en mai 2009 la réunion bisannuelle des commissaires des pays nordiques. La réunion, organisée à Stockholm, a rassemblé des participants du Danemark, 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 sur la protection des données.

### B. Jurisprudence importante

**Conservation des rapports de police**
En 2008, le commissaire a émis des avis d'exécution à l'attention de cinq corps de police, leur ordonnant de supprimer les anciennes condamnations pénales de l'ordinateur national de la police (PNC).

Cette mesure a été prise suite à notre enquête menée après les plaintes de cinq personnes qui avaient été condamnées ou qui avaient reçu un avertissement de la police sans être condamnées par la suite d'un quelconque délit.

Dans chaque cas, le commissaire a écrit aux corps de police concernés, leur enjoignant de supprimer les informations en question du PNC, ou de les «rétrograder», c.-à-d. de les conserver sur le PNC, mais à un endroit accessible uniquement par les policiers. Chaque corps de police a accepté de «rétrograder» l'information, mais pas de la supprimer.

En conséquence, le commissaire a distribué des avis d'exécution aux directeurs de chacun des corps de police. Chaque avis exigeait de supprimer l'information relative à la condamnation de l'individu en question du PNC.

Les directeurs ont interjeté appel devant l'*Information Tribunal*, qui entend les recours introduits contre les avis du commissaire à l'information, en vue d'annuler les avis d'exécution du commissaire. En d'autres termes, les directeurs de la police ont cherché à pouvoir conserver les données de condamnation en question sur le PNC.

Le tribunal a confirmé les avis d'exécution émis par le commissaire et requis des directeurs de police qu'ils suppriment les informations pertinentes au sujet de ces cinq individus.

Les cinq directeurs de police ont été autorisés à interjeter appel devant la Cour d'appel, qui a statué que les corps de police n'avaient pas besoin de supprimer les informations et que la conservation des dossiers par leurs soins n'enfreignait pas la loi sur la protection des données. Le jugement peut être consulté à l'adresse:
www.bailii.org/ew/cases/EWCA/Civ/2009/1079.html

Nous pensons que ce jugement soulève d'importantes questions, pas seulement pour ces individus et tant d'autres au sujet desquels sont conservées des informations de condamnations très mineures et anciennes, mais aussi quant à l'interprétation de la loi sur la protection des données en pratique. Il remet aussi sérieusement en question l'applicabilité de l'article 8 de la Convention européenne des droits de l'homme aux données de condamnation détenues par la police. Nous avons interjeté appel devant la Cour suprême et espérons que notre pourvoi sera accepté et que ces questions pourront y être examinées.

### C. Questions diverses importantes

**Janvier**
Nous avons lancé la *«Personal Information Promise»* à l'occasion de la Journée européenne de la protection des données. La «promesse» est un engagement clair des dirigeants d'organisations, qui déclarent qu'ils font grand cas des informations personnelles qui leur sont confiées et qu'ils mettront en place les ressources appropriées pour y veiller. Fin 2009, un millier d'organisations avaient signé la promesse.

Nous avons conclu à la violation de la loi sur la protection des données personnelles par le ministère de l'intérieur après la perte par un sous-traitant d'une carte mémoire non cryptée contenant les données personnelles sensibles de milliers de personnes en 2008. Les informations perdues se rapportaient à des individus prestant une peine privative

de liberté et à d'autres condamnés antérieurement pour des délits pénaux.

**Mars**
Nous avons saisi une base de données clandestine contenant les données personnelles de 3213 ouvriers du bâtiment et émis un avis d'exécution à l'encontre du propriétaire de la base de données, un certain M. Ian Kerr, agissant au nom de *The Consulting Association*. Les données ont été utilisées par plus de 40 entreprises de construction afin d'examiner la candidature des candidats à l'embauche. Ian Kerr a été condamné par la suite à une amende de 5000 livres sterling, plus les frais de justice, et nous avons émis des avis d'exécution à l'encontre de 14 entreprises de construction pour violation de la loi sur la protection des données personnelles. Certaines avaient payé des milliers de livres sterling pour obtenir injustement les données personnelles d'ouvriers de la construction.

Nous avons tenu notre deuxième conférence des agents de protection des données à Manchester, qui a attiré quelque 300 délégués. Cet événement a eu des répercussions en termes de sensibilisation à la protection des données, à la suite de récentes pertes de données, et de partage d'idées et d'expériences sur la manière de relever les défis auxquels sont confrontés les agents de protection des données.

**Avril**
En 2008, nous avons chargé RAND Europe de dresser un bilan de la directive européenne sur la protection des données. Le projet a évalué les forces et faiblesses des dispositifs européens de protection des données et, partant, la loi britannique sur la protection des données. Le projet de rapport final a été présenté à la conférence des commissaires européens à la protection des données, organisée par le commissaire à l'information à Édimbourg en avril 2009, et publié en mai.

**Juin**
Nous avons publié notre code de bonnes pratiques en matière d'avis relatifs à la vie privée. Le code a été conçu de manière à aider les organisations à élaborer des avis clairs en matière de vie privée et à s'assurer qu'elles collectent les données personnelles de manière honnête et transparente.

Nous avons également accueilli notre nouveau commissaire, Christopher Graham, qui nous a rejoints au terme du mandat de Richard Thomas.

**Octobre**
Notre redevance de notification est passée de 35 à 500 livres sterling pour certaines grandes organisations. Les organisations concernées sont celles affichant un chiffre d'affaires de 25,9 millions de livres sterling ou plus et employant au moins 250 personnes. Le nouveau taux s'applique également aux organes publics employant au moins 250 personnes.

**Novembre**
Le projet de loi sur les coroners et la justice a reçu la sanction royale et est devenu une loi du Parlement. Par conséquent, nous aurons le pouvoir d'auditer les départements gouvernementaux sans leur consentement, en leur remettant un avis d'évaluation. Nos nouveaux pouvoirs d'audit doivent entrer en vigueur en avril 2010.

Nous avons publié le guide sur la protection des données, qui livre des orientations claires en matière d'application pratique de la loi. Les différentes parties prenantes lui ont réservé un accueil chaleureux.

**Décembre**
Nous avons lancé une consultation publique relative à notre avant-projet de code de pratiques en ligne sur les informations personnelles à l'occasion de notre conférence à Manchester du 9 décembre. L'avant-projet de code formule des recommandations claires et complètes pour gérer en bonne et due forme les données personnelles et offrir aux particuliers le degré adéquat de choix et le contrôle de ces données. Il doit aider les organisations grâce à une présence en ligne pour traiter des questions liées à l'insécurité juridique en adoptant de bonnes pratiques. Notre but est de publier le code finalisé aux alentours du mois de mai 2010.

Vous trouverez de plus amples détails sur nos activités au cours de l'année 2009 dans nos rapports annuels pour 2008/09 et 2009/10, publiés sur notre site www.ico.gov.uk.

# Chapitre 3

# UNION EUROPÉENNE ET ACTIVITÉS COMMUNAUTAIRES

## 3.1. COMMISSION EUROPÉENNE

*Conférence[24]: «Données personnelles - plus d'utilisation, plus de protection?» 19-20 mai 2009*

La Commission européenne a organisé une conférence sur l'utilisation et la protection des données personnelles afin d'examiner les nouveaux défis pour le respect de la vie privée.

Comment protéger les données personnelles dans le contexte de la mondialisation et de la mobilité accrue et au regard des technologies modernes de communication et d'information et des nouvelles politiques? Quelles données sont consultées et échangées par les autorités publiques et les entreprises privées? Quelle est l'efficacité réelle des règles actuelles sur les transferts internationaux de données personnelles à l'ère de l'informatique dématérialisée (*«cloud computing»*)? Quelles sont les attentes des particuliers, des entreprises et de la société dans son ensemble? Ces thèmes et d'autres questions d'actualité ont été abordés lors d'une conférence sur l'utilisation, l'échange et la protection des données personnelles dans l'Union européenne, que la Commission européenne a organisée à Bruxelles les 19 et 20 mai 2009.

Les personnes intéressées, les chefs d'entreprise, les associations de consommateurs, les universitaires, les autorités de contrôle de la protection des données et les pouvoirs publics des États membres de l'Union européenne et des pays tiers étaient invités à y participer. Jacques Barrot, vice-président de la Commission européenne chargé de la justice, de la liberté et de la sécurité, figurait au rang des intervenants.

La conférence a donné l'occasion aux différentes parties prenantes d'exprimer leurs opinions et leurs questions sur les nouveaux défis relatifs à la protection des données et sur la nécessité d'une stratégie efficace pour la gestion des informations dans l'Union européenne. Cette manifestation s'inscrivait dans le cadre de la consultation lancée par la Commission sur la manière de développer le droit fondamental à la protection des données personnelles et de le faire respecter dans les faits, notamment dans le domaine de la liberté, de la justice et de la sécurité.

*Atelier sur les atouts économiques des technologies renforçant la protection de la vie privée – 12 novembre 2009[25]*

La Commission européenne a lancé une étude sur les atouts économiques des technologies renforçant la protection de la vie privée. L'atelier a été l'occasion de présenter le rapport[26] intermédiaire de l'étude, actuellement menée par London Economics. Il a également offert à un vaste panel d'acteurs concernés la possibilité de partager leur expérience des technologies renforçant la protection de la vie privée. Nous espérions que les participants nous livreraient des exemples pratiques du fonctionnement ou dysfonctionnement des technologies renforçant la protection de la vie privée, et de la manière dont leur déploiement peut bénéficier à chacun d'entre nous. Cet atelier a été conçu à l'attention des acteurs des technologies renforçant la protection de la vie privée (développeurs, déployeurs, pouvoirs publics, utilisateurs/consommateurs). Dans un souci de préserver un environnement de travail pratique, la participation à l'atelier a été limitée à 50 experts.

*Consultation publique sur le cadre juridique pour le droit fondamental à la protection des données à caractère personnel[27]*

La consultation sur le cadre juridique pour le droit fondamental à la protection des données à caractère personnel a été ouverte au public du 9.7.2009 au 31.12.2009. L'objectif de la consultation était de confronter les points de vue sur les nouveaux défis qui attendent la protection des données à caractère personnel afin de maintenir un cadre juridique efficace et complet devant protéger les données personnelles des particuliers au sein de l'Union européenne. Les enjeux étaient les suivants: a) échanger des opinions sur les nouveaux défis qui attendent la protection des données personnelles, particulièrement à la lumière des nouvelles technologies et de la mondialisation, b) échanger des opinions sur la

[24] http://ec.europa.eu/justice_home/news/events/events_2009_en.htm

[25] http://ec.europa.eu/justice_home/news/events/events_2009_en.htm

[26] http://ec.europa.eu/justice_home/news/events/workshop_pets_2009/report_en.pdf

[27] http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

capacité du cadre juridique actuel à relever ces défis et c) échanger des opinions sur les futures actions nécessaires pour relever les défis identifiés. Dans le cadre de cette consultation publique, 168 réponses ont été reçues de la part de citoyens, d'organisations (enregistrées et non enregistrées) et d'autorités publiques.

*Directive vie privée et communications électroniques*

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 (la directive vie privée et communications électroniques) a été révisée dans le cadre du processus de révision du paquet de réformes des télécommunications, qui comprend cinq directives européennes (directive-cadre, directive «accès», directive «autorisation», directive «service universel» et directive «vie privée et communications électroniques»). Un nouveau règlement instituant l'Organe des régulateurs européens des communications électroniques (ORECE) a rejoint le paquet de réformes des télécommunications.

La vie privée et la protection des données à caractère personnel seront renforcées à travers les nouvelles règles introduisant la notification obligatoire des violations des données personnelles – la première loi du genre au sein de l'Union européenne. Cela signifie que les fournisseurs de communications seront obligés d'informer les autorités et leurs clients des manquements à la sécurité de leurs données personnelles. Cette nouvelle donne devrait inciter davantage les fournisseurs de réseaux et services de communications à mieux protéger leurs données à caractère personnel.

En outre, les règles relatives à la vie privée et à la protection des données sont renforcées, par exemple sur l'utilisation de «cookies» et de dispositifs similaires. Les internautes seront mieux informés au sujet des cookies et du sort réservé à leurs données personnelles. Ils auront également plus de facilité à contrôler leurs informations personnelles dans la pratique. Sans oublier que les fournisseurs de services internet acquerront aussi le droit de protéger leurs activités et leurs clients par le biais d'actions juridiques à l'encontre des «spammeurs».

La nouvelle directive vie privée et communications électroniques doit être transposée en droit national d'ici mai 2011.

## 3.2. COUR DE JUSTICE EUROPÉENNE

*Ordonnance de la Cour (huitième chambre) du 19 février 2009 (demande de décision préjudicielle du Oberster Gerichtshof (Autriche)) - LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH) (Affaire C-557/07)*[28]

Dispositif de l'arrêt:
Le droit communautaire, notamment l'article 8, paragraphe 3, de la directive 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle, lu en combinaison avec l'article 15, paragraphe 1, de 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 (directive vie privée et communications électroniques), ne s'oppose pas à ce que les États membres établissent une obligation de transmission à des personnes privées tierces de données à caractère personnel relatives au trafic pour permettre d'engager, devant les juridictions civiles, des poursuites contre les atteintes au droit d'auteur. Toutefois, le droit communautaire exige que les États membres, lors de la transposition des 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 marché 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, 2002/58 et 2004/48, veillent à se fonder sur une interprétation de celles-ci qui permette d'assurer un juste équilibre entre les différents droits fondamentaux en présence. Par ailleurs, les autorités ainsi que

[28] JO C 113 du 16.05.2009, p.14.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:113:0014:0014:EN:PDF

les juridictions des États membres doivent, lors de la mise en œuvre des mesures de transposition desdites directives, non seulement interpréter leur droit national d'une manière conforme à ces dernières, mais également veiller à ne pas se fonder sur une interprétation de ces directives qui entrerait en conflit avec les droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité.

Un fournisseur d'accès, qui se limite à procurer aux utilisateurs l'accès à l'internet, sans proposer d'autres services tels que, notamment, des services de courrier électronique, de téléchargement ou de partage des fichiers, ni exercer un contrôle de droit ou de fait sur le service utilisé, doit être considéré comme un «intermédiaire» au sens de l'article 8, paragraphe 3, de la directive 2001/29.

*Arrêt de la Cour (troisième chambre) du 7 mai 2009 (demande de décision préjudicielle du Raad van State (Pays-Bas)) – College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer Pays-Bas (Affaire C-553/07)*[29]

Dispositif de l'arrêt:
L'article 12, sous a), 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, impose aux États membres de prévoir un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé. Il appartient aux États membres de fixer un délai de conservation de cette information ainsi qu'un accès corrélatif à celle-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention et de recours prévus par la directive 95/46, et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement.

Une réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêt et obligation en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement. Il appartient à la juridiction nationale d'effectuer les vérifications nécessaires.

## 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 communautaires dans le cadre du traitement des données à caractère personnel.

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

- contrôler le traitement des données à caractère personnel par les institutions et organes communautaires 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 nationales et avec les organismes de contrôle de l'ancien «troisième pilier» de l'UE afin de renforcer la cohérence dans la protection des données à caractère personnel (coopération).

[29] JO C 153 du 04.07.2009, p.10
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:153:0010:0010:EN:PDF

[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.

*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. Des avis plus détaillés à l'attention de l'administration communautaire peuvent aussi prendre la forme d'avis sur des mesures administratives ou de publication d'orientations thématiques.

Tous les organes et institutions communautaires doivent compter au moins un délégué à la protection des données. En 2009, le nombre de **délégués à la protection des données** a grimpé à 45. Une supervision efficace passe immanquablement par une interaction régulière avec ces personnes et leur réseau.

Le **contrôle préalable** des traitements à risque est resté la principale activité du CEPD en 2009, dans le cadre de sa mission de supervision. Il a ainsi adopté plus de 110 avis de contrôle préalable sur des données relatives à la santé, à l'évaluation du personnel, au recrutement de candidats, à la gestion du temps, à l'enregistrement des appels téléphoniques, aux outils de performance et aux enquêtes de sécurité. Ces avis sont publiés sur le site internet du CEPD et leur mise en œuvre fait l'objet d'un suivi systématique.

La mise en œuvre du règlement par les organes et institutions est également **systématiquement contrôlée** par une évaluation régulière d'indicateurs de performance, associant tous les institutions et organes communautaires. Dans la foulée de l'exercice de printemps 2009, le CEPD a publié un rapport qui démontre que les institutions européennes ont bien progressé dans le respect des règles de protection de données. Cependant, on observe dans la plupart des agences un moindre degré de conformité.

Dans ce contexte, le CEPD a mené quatre **inspections** sur site dans différents organes et institutions. Ces inspections font systématiquement l'objet d'un suivi et seront renforcées dans un futur proche. En juillet 2009, le CEPD a adopté un manuel de procédure d'inspection et en a publié les principaux aspects sur son site internet.

En 2009, le nombre total de **plaintes** a grimpé à 111, mais seules 42 ont été jugées recevables. La plupart des plaintes irrecevables abordaient des questions de niveau national qui échappent à la compétence du CEPD. Les cas recevables concernaient des violations présumées de la confidentialité, une collecte de données excessive ou l'usage illégal de données par le responsable du traitement. Dans huit cas, le CEPD a conclu à la violation des règles de protection des données.

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. Une variété de questions ont été soulevées, notamment concernant les transferts de données à destination de pays tiers ou d'organisations internationales, le traitement de données en cas de pandémie, la protection des données dans le cadre du service d'audit interne et la mise en œuvre des dispositions du règlement (CE) n° 45/2001.

Le CEPD a adopté des **lignes directrices** relatives au traitement de données personnelles à des fins de recrutement ainsi qu'aux données de santé sur le lieu de travail. En 2009, le CEPD a également organisé une consultation publique sur les lignes directrices relatives à la vidéosurveillance, en insistant notamment dans ce contexte sur les principes clés de «Privacy by Design» – selon lequel les TIC sont conçues et développées en tenant compte de la vie privée et des exigences de protection des données depuis la création même de la technologie, et ce à tous les stades de son développement – et de responsabilisation.

*Consultation*

Plusieurs événements significatifs ont contribué à rapprocher la perspective d'un nouveau **cadre juridique pour la protection des données**. La concrétisation de cette perspective figurera en belle place dans l'agenda du CEPD dans les années à venir.

Fin 2008, l'adoption d'un cadre juridique général pour la protection des données dans le domaine de la coopération policière et judiciaire en matière pénale au niveau communautaire, bien que n'apportant pas pleine

satisfaction, a franchi un pas important dans la bonne direction.

En 2009, un deuxième développement majeur fut l'adoption de la directive révisée «vie privée et communications électroniques» dans le cadre d'un paquet plus vaste. Ce fut là aussi un premier pas sur la voie de la modernisation du cadre juridique pour la protection des données.

En plus d'avoir rendu contraignante la Charte des droits fondamentaux pour les organes et institutions ainsi que pour les États membres agissant dans le champ de la législation communautaire, l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, a également signé l'introduction d'une base générale pour un cadre juridique complet dans l'article 16 du TFUE.

En 2009, la Commission a également initié une consultation publique sur l'avenir du cadre juridique pour la protection des données. Le CEPD a collaboré étroitement avec ses collègues pour entourer cette consultation de toutes les synergies nécessaires et a profité de diverses occasions pour souligner la nécessité d'une protection des données plus complète et efficace au sein de l'Union européenne.

Le CEPD a poursuivi la mise en œuvre de sa **politique de consultation** générale et a émis un nombre record d'avis législatifs sur différents sujets. Cette politique défend une approche proactive, s'accompagnant d'un inventaire régulier des propositions législatives requérant un avis, et de la possibilité de commentaires informels lors des phases préparatoires des propositions législatives. La plupart des avis rendus par le CEPD ont été débattus dans l'enceinte du Parlement et du Conseil.

En 2009, le CEPD a suivi avec un grand intérêt les développements qui ont entouré le **programme de Stockholm** et sa vision pour les cinq prochaines années dans le domaine de la justice et des affaires intérieures. Le CEPD a donné des conseils sur le développement du programme et a participé aux travaux préparatoires du modèle européen d'information.

D'autres travaux dans ce domaine concernaient la révision des règlements Eurodac et Dublin, la création d'une agence pour la gestion opérationnelle des systèmes d'information à grande échelle et une approche cohérente de la supervision dans le domaine.

Dans le contexte de la **vie privée et des communications électroniques et de la technologie**, hormis la révision générale susmentionnée, le CEPD s'est attelé à des questions relatives à la directive sur la conservation des données, à l'utilisation de tags RFID ou à des systèmes de transport intelligents, ainsi qu'au rapport RISEPTIS intitulé *«Trust in the Information Society»* (Confiance dans la société de l'information).

À l'ère de la **mondialisation**, le CEPD s'est attelé au développement de normes mondiales, au dialogue transatlantique sur la protection des données et aux données répressives, ainsi qu'aux questions de mesures restrictives à l'égard de terroristes présumés et de certains pays tiers.

D'autres sujets n'ont pas manqué de susciter l'intérêt du CEPD, comme la **santé publique** – dont les soins de santé transfrontaliers, la santé électronique et la pharmacovigilance – et l'**accès du public aux documents** – comme la révision du règlement (CE) n° 1049/2001 sur l'accès du public aux documents et divers procès portant sur la relation entre accès du public et protection des données.

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

Mention spéciale doit être faite de la contribution commune sur le *«Future of Privacy»* en réponse à la consultation de la Commission européenne sur un cadre juridique communautaire pour la protection des données, et de la consultation de la Commission sur l'impact des scanners corporels dans le domaine de la sécurité aéronautique.

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 avec les autorités nationales de protection des données. Le groupe de coordination de la supervision d'Eurodac, composé d'autorités nationales de protection des données et du CEPD, s'est réuni à trois reprises et s'est concentré sur la mise en œuvre du programme de travail adopté en décembre 2007.

L'un des principaux résultats fut l'adoption en juin 2009 d'un second rapport d'inspection consacré à deux sujets: le droit à l'information des demandeurs d'asile et les méthodes d'évaluation de l'âge des jeunes demandeurs d'asile.

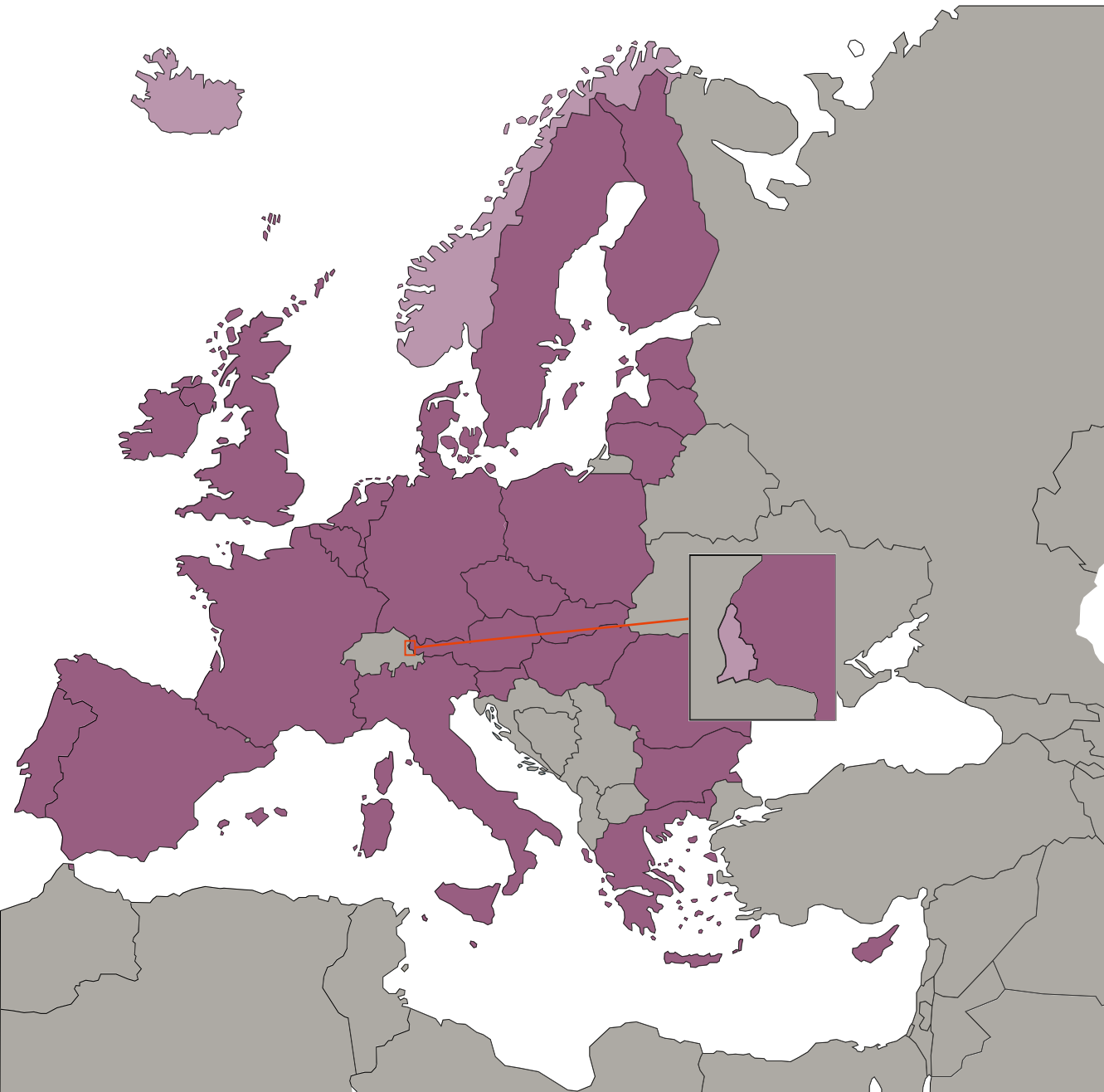
Le CEPD a poursuivi son étroite collaboration avec les autorités de protection des données dans le cadre de l'ancien «troisième pilier» – la **coopération policière et judiciaire** – et avec le groupe de travail sur la police et la justice. En 2009, cette coopération a couvert la participation au débat sur le programme de Stockholm et l'évaluation de l'impact de la décision-cadre du Conseil sur la protection des données.

La coopération au sein des **forums internationaux** s'est poursuivie, notamment dans le cadre de la 31e Conférence internationale des commissaires à la protection des données et de la vie privée, organisée à Madrid, qui a accouché d'un ensemble de normes mondiales pour la protection des données.

Le CEPD a également organisé un atelier sur les réponses à apporter aux infractions à la sécurité dans le cadre de l'«initiative de Londres», lancée à l'occasion de la 28e Conférence internationale en novembre 2006, dans le but de renforcer la sensibilisation à la protection des données et de la rendre plus efficace.

# 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 2009, 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 ou ayant une incidence sur la protection des données. En voici les plus importants:

1. Loi n° 37/2009 modifiant la loi n° 54/2006 sur l'assurance chômage. – La loi n° 37/2009 a permis de renforcer l'autorité de l'inspection du travail pour collecter des données. Si l'inspection du travail possédait d'ores et déjà l'autorité de collecter des données, nécessaire à la mise en œuvre de la loi n° 54/2006, auprès des autorités fiscales, des autorités d'assurance médicale et sociale, du centre de soutien à l'enfance et des fonds de pension, la loi n° 37/2009 lui a également conféré l'autorité de collecter des données auprès des écoles de l'enseignement secondaire supérieur et universitaire. À cet égard, l'inspection du travail a obtenu les listes des étudiants de ces écoles, l'inscription à une école pouvant affecter le droit à bénéficier d'allocations de chômage.

2. Loi n° 48/2009 modifiant la loi n° 110/2000 sur les biobanques. – La loi sur les biobanques contient des dispositions sur la protection des données à caractère personnel pour ce qui est de la collecte, de la conservation et de l'utilisation d'échantillons biologiques. À l'origine, tous les échantillons devaient être conservés à l'abri des marqueurs d'identification personnelle. La loi n° 48/2009 a changé la donne. Désormais, une distinction est faite entre échantillons de recherche et échantillons cliniques. Les premiers sont conservés sans identification personnelle, et le lien entre échantillons et identification personnelle se fait conformément aux règles de l'APD (actuellement règle n° 918/2001). Les échantillons cliniques, pour leur part, peuvent être marqués à l'aide de marqueurs d'identification personnelle, mais sont conservés de manière à ne pas être perdus ou endommagés, et sont rendus inaccessibles aux personnes non autorisées. La loi n° 48/2009 a pour objet d'éliminer le risque de mauvaise identification des échantillons cliniques, pouvant ainsi mettre en danger la sécurité des patients.

3. Loi n° 55/2009 relative aux dossiers médicaux. – Cette loi stipule l'obligation de conserver les dossiers médicaux. Elle poursuit l'objectif d'introduire des règles concernant les dossiers médicaux afin d'offrir aux patients les meilleurs services de santé possibles à tout moment, tout en garantissant la protection des données médicales. Dans la mesure du possible, les dossiers médicaux doivent être introduits sous forme électronique. La loi autorise les institutions de soins de santé et les praticiens indépendants à mettre en rapport leurs systèmes d'information de santé contenant les dossiers médicaux des patients ou à utiliser un système d'information commun. Les patients ont le droit de s'opposer au partage de leurs données dans des systèmes d'information mis en rapport. Les patients peuvent également interdire l'accès à leurs données dans un système d'information conjoint, en tout ou en partie, en dehors de l'établissement de soins ou du cabinet d'un praticien où sont enregistrés les dossiers. Les patients peuvent décider, pendant leur traitement, de refuser l'accès de leur dossier médical relatif au traitement à autrui, à l'exception de la personne qui introduit les données, du superviseur des dossiers médicaux et, le cas échéant, d'autres praticiens spécifiés. S'il s'avère nécessaire, dans le cadre du traitement, que d'autres praticiens de soins de santé puissent accéder aux données médicales en question, le patient en est informé, de même que tout refus d'autoriser l'accès nécessaire aux dossiers médicaux peut être assimilé, dans certaines circonstances, à un refus de traitement. La conformité aux dispositions de la loi est, en premier lieu, contrôlée par les responsables des systèmes d'information de santé et, en second lieu, par le directeur médical de la santé et l'APD. Si un contrôle révèle une réelle probabilité de violation des droits au respect de la vie privée d'un patient, le délit est transmis à la police.

4. Loi n° 146/2009 modifiant la loi n° 142/2008 relative à une enquête sur les circonstances ayant mené à l'effondrement des banques islandaises en 2008, sur les causes de cet effondrement et sur les événements connexes. – La loi n° 146/2009 introduit des clauses sur la procédure à suivre par le Parlement islandais (Althing) pour réagir au rapport de la commission d'enquête spéciale, désignée par l'Althing conformément à la loi n° 142/2008. La loi contient des dispositions sur les bases de données créées dans le cadre des activités de la commission. Ces bases de données intègrent des données très fournies sur des

particuliers. Certaines ont été publiées dans le rapport de la commission soumis en avril 2010 (la plupart concernant des hommes d'affaires, des politiciens et des hauts fonctionnaires), puisque les données étaient supposées faire la lumière sur l'effondrement des banques islandaises. Toutefois, le volume des données n'est pas considéré être d'une valeur telle qu'elle impose leur publication. La loi n° 146/2009 inclut dès lors des dispositions protégeant ces données de façon à ne pas les rendre accessibles aux personnes dont l'accès n'est pas légitime. En vertu de la loi, l'accès à des fins de recherche peut être considéré comme légitime. Toutefois, le traitement à des fins de recherche n'entraîne pas la publication de données personnellement identifiables.

## B. Jurisprudence importante

Aucune.

## C. Questions diverses importantes

L'un des hauts faits de l'année 2009 en matière de protection des données a été un projet de recherche mené par la Banque nationale d'Islande, dans le cadre duquel des données importantes sur la situation financière d'individus, émanant de nombreuses parties telles que des banques et autres organismes financiers, l'inspection du travail, les fonds de pension et l'administration de l'assurance sociale, ont été reliées entre elles. L'objectif de mettre en rapport ces données s'inscrivait dans une volonté de mieux comprendre l'impact de la crise financière en Islande sur les individus et les ménages, afin d'être mieux armé pour combattre la crise. L'APD a autorisé la liaison sous réserve de l'adoption de mesures de sécurité techniques et organisationnelles, dont l'anonymisation des données. Si les données n'étaient pas traitées, l'ordinateur sur lequel elles étaient stockées était conservé par l'APD. Comme stipulé dans les permis, le disque dur de l'ordinateur contenant toutes les données a été détruit début 2010.

Le 28 avril, l'APD a rendu une décision relative à l'utilisation de données dans la base de données centrale des produits médicinaux en Islande, gérée depuis 2003 par l'inspection de la santé, conformément à la loi. L'article 27 de la loi n° 93/1994 sur les produits médicinaux, telle que modifiée par la loi n° 89/2003, énonce les finalités autorisant l'utilisation de la base de données, c.-à-d. essentiellement des fins administratives, dont l'enquête sur une consommation abusive présumée de médicaments créant une accoutumance. Un individu avait demandé une prescription pour un tel médicament. Le médecin en charge de ce patient s'est enquis auprès de l'inspection de la santé de la consommation médicamenteuse de l'individu et a reçu des réponses révélant que l'individu en question avait des antécédents d'usage de médicaments créant une accoutumance. L'individu n'a été informé de cette utilisation de la base de données que par la suite et a déposé plainte auprès de l'APD. Dans la décision susmentionnée, l'APD a conclu que la transmission des informations sur le plaignant n'était pas conforme à l'article 27 de la loi sur les produits médicinaux et que l'inspection de la santé n'avait, par conséquent, pas agi légalement en transmettant lesdites informations au médecin.

Le 16 décembre 2009, l'APD a émis une décision sur le traitement de données contenues dans des adresses IP par l'inspection du travail. Les personnes souhaitant bénéficier d'allocations de chômage envoient chaque mois un avis électronique à l'inspection confirmant qu'ils sont sans emploi. Selon l'interprétation que fait l'inspection de la législation en matière de chômage, les chômeurs doivent rester en Islande (et donc être prêts à travailler à court terme) pour être habilités à recevoir les allocations. L'adresse IP d'un avis électronique envoyé à l'inspection contenait des informations révélant que l'individu en question n'était pas en Islande. L'inspection lui a envoyé un courrier lui apprenant qu'elle possédait des informations sur son séjour hors d'Islande, mais ne spécifiait pas comment elle les avait obtenues. L'individu a déposé plainte auprès de l'APD, qui a conclu, dans la décision susmentionnée, qu'il aurait été de bon ton d'indiquer sur le site internet de l'inspection du travail que les adresses IP étaient collectées et que les données contenues dans ces adresses étaient traitées en vue de découvrir si un individu séjournait hors d'Islande.

## Liechtenstein

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

L'une des missions centrales de l'Office pour la protection des données (ou DSS, pour *Datenschutzstelle*) 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 2009, le DSS a rendu un avis sur 34 projets de loi à divers stades du processus législatif. Dans le cadre de la proposition de loi, il faudra aborder plus en détail les points suivants, qui touchent à des aspects importants de la législation sur la protection des données.

L'année dernière déjà, notre rapport détaillait les deux révisions partielles de la loi sur la protection des données (ou DSG, pour *Datenschutzgesetz*). La première est entrée en vigueur au 1er janvier 2009[31], et la seconde au 1er juillet 2009[32]. Dans le même temps, le règlement pour la protection des données (ou DSV, pour *Datenschutzverordnung*) a également été adapté, et sa nouvelle version est elle aussi applicable depuis juillet 2009[33]. Le DSV prévoit, plus particulièrement, la création d'une nouvelle institution, en la personne d'un préposé à la protection des données tant au sein des entreprises que des administrations[34]. Cette nouvelle fonction vise à responsabiliser davantage les propriétaires de bases de données. Par ailleurs, cette nouvelle règle est aussi considérée comme un atout concurrentiel pour les entreprises. Les personnes privées ou entreprises qui désignent un responsable de la protection des données «maison» bénéficient de certaines facilités. Ainsi, dans certaines conditions, elles ne sont plus tenues de signaler leurs bases de données. Quant aux entreprises, elles peuvent même ne plus être tenues d'élaborer un règlement concernant le traitement de leurs bases de données automatisées. Pour pouvoir bénéficier de ces divers avantages prévus par la loi, les responsables du traitement des données doivent être signalés au DSS, qui publiera leur nom dans une liste publique.

Dans la pratique, les principales nouveautés ont trait à la plus grande indépendance du DSS[35], au transfert de données à l'étranger et à la vidéosurveillance. Concernant le transfert de données transnational, on relèvera surtout l'obligation, désormais, de faire approuver certains accords de protection des données reposant sur une convention unique ainsi que les règlements d'ordre intérieur contraignants des entreprises en matière de protection des données[36]. En l'absence, dans le pays étranger concerné, d'une législation garantissant une protection adéquate des données, les accords doivent d'abord faire l'objet d'une autorisation de la part du gouvernement, sur avis du DSS. L'Office est ainsi invité à indiquer si les garanties ou les règlements uniformes en matière de protection des données sont garants d'une protection adéquate au sens de la DSG du Liechtenstein. Lors de l'octroi de l'autorisation, le gouvernement est tenu de respecter l'avis du DSS.

L'introduction d'une base juridique générale concernant la vidéosurveillance dans l'espace public[37] a mobilisé une large part des ressources du DSS au cours de l'année de référence. L'utilisation d'un système de vidéosurveillance dans l'espace public est, depuis le 1er juillet 2009, soumise à autorisation du DSS. En règle générale, cette autorisation doit être obtenue avant la mise en service de l'équipement. Pour les systèmes existants, une période de transition a été prévue. Celle-ci se terminera à la fin de l'année. Concernant la procédure d'autorisation, des formulaires de demande en ligne, des aides à la saisie et un guide complet ont dû être élaborés à l'avance. Par ailleurs, il a fallu informer le public des nouvelles dispositions. Il convient de noter qu'il n'existe une obligation d'autorisation que lorsque des personnes sont identifiables au moyen des données obtenues, que les données sont traitées et qu'il s'agit d'un espace public. À l'inverse, les images enregistrées dans un cercle strictement privé ou familier, les transmissions d'images qui s'effectuent uniquement en temps réel et les enregistrements par webcam ne permettant pas l'identification de personnes, ne sont pas soumis à autorisation.

[31] LGBl. 2008 n° 273.LGBl. 2008 n° 273.

[32] LGBl. 2009 n° 46.

[33] LGBl. 2009 n° 209.

[34] Art. 4a, 13a, 23 par. 2 du DSV.

[35] Pour plus de détails, voir la contribution du Liechtenstein au 12e rapport annuel du groupe Art. 29 sur la protection des données, p. 132, ainsi que le rapport d'activité du délégué à la protection des données de la Principauté du Liechtenstein, 2008, 10.1.

[36] Art. 8 par. 3 de la DSG, en relation avec l'art. 6 du DSV.

[37] Art. 6a de la DSG, en relation avec l'art. 27 du DSV.

Un autre projet de loi de premier plan concernait également la révision de la loi sur les communications (KomG), qui n'a pas pu être clôturé au cours de l'année de référence:

Le Liechtenstein a introduit des dispositions en matière de conservation des données de trafic dans la KomG dès 2006, bien que la directive 2006/24/CE ne fasse pas encore partie, à ce jour, de l'Accord sur l'EEE, et qu'il n'existe donc aucune obligation de la transposer en droit national. Ces dispositions ont été critiquées à plusieurs reprises et par plusieurs camps. À cet égard, la conservation des données de trafic pendant une durée de six mois - en accord avec le groupe Art. 29 sur la protection des données - est considérée comme une atteinte considérable aux droits et libertés des citoyens et à leur sphère privée. Cette fois, le gouvernement s'est appuyé sur ces critiques pour réviser ces dispositions dans le sens d'un plus grand respect des citoyens et des libertés fondamentales, et pour définir des normes strictes concernant la consultation et l'utilisation des données conservées[38]. Par ailleurs, un contrôle global de la protection et de la sécurité des données par le DSS est prévu.

## B. Jurisprudence

Rien de particulier à signaler.

## C. Problèmes spécifiques majeurs

Les préparatifs de l'adhésion du Liechtenstein aux Accords de Schengen et de Dublin, qui battaient déjà leur plein au printemps, ont été poursuivis et intensifiés[39]. Ainsi, le DSS a déjà été saisi de dossiers juridiques relatifs au développement de l'acquis de Schengen, et notamment à la transposition de l'«Initiative suédoise» en droit national (décision-cadre 2006/960/JI). Pour sa préparation à l'évaluation de la protection des données, le Liechtenstein a pu compter sur l'expérience d'autres États Schengen. Sans compter qu'une évaluation par sondage a déjà été réalisée au cours de l'année de référence, laquelle a permis de recenser les expériences positives. Dans ce contexte, l'accent a été mis sur l'indépendance et la structure de l'Office pour la protection des données, sur ses missions juridiques et sur ses compétences en matière de contrôle, ainsi que sur les droits des citoyens. Toutefois, au centre des préparatifs figuraient aussi un questionnaire ébauchant les conditions-cadres de «l'examen de Schengen», ainsi que l'élaboration de documentations.

Bien que le Liechtenstein n'ait encore accès à aucune donnée, sa participation aux réunions de différentes instances et notamment de l'autorité de contrôle commune de Schengen, en qualité d'observateur, lui a permis d'obtenir de précieuses informations sur le mode de fonctionnement et de travail de Schengen.

Parmi les missions centrales de l'Office pour la protection des données figurent en outre l'information et la sensibilisation de l'opinion publique à la protection des données. À cet égard, c'est le site web du DSS qui reste le principal vecteur d'information. Toutefois, sa lettre d'information, qui traite chaque mois d'un nouveau thème d'actualité, constitue elle aussi une source d'information considérable pour le grand public.

Au cours de l'année de référence, l'Office pour la protection des données a, pour la première fois, réalisé un sondage en ligne. Au total, ce sont quatre rubriques de questions relatives à la protection des données (Généralités, Informations, Confiance, Comportement) qui étaient proposées aux visiteurs. Du côté des médias, on a pu constater un grand intérêt pour les résultats de cette enquête. Une des conclusions de ce sondage est qu'une majorité des répondants ne s'estiment pas suffisamment informés de leurs droits. Ils souhaitent également davantage d'informations sur le sujet «Internet et protection des données». Ces résultats ont été pris en compte, et une formation a été organisée pour les collaborateurs de l'administration du Liechtenstein.

À l'occasion de la journée européenne de la protection des données du 28 janvier, le DSS a organisé, en collaboration avec l'Institut d'économie et d'informatique de l'Université du Liechtenstein, une manifestation publique intitulée « Denn sie wissen nicht, was sie tun?! - Soziale Netzwerke unter der Lupe» («Car ils ne savent pas ce

[38] Rapport et demande n° 110/2009, p. 113.

[39] Cf. Rapport d'activité 2008, 10.1.

qu'ils font ?! - Les réseaux sociaux passés à la loupe»)[40]. L'objectif de cet événement consistait à sensibiliser l'opinion publique à la thématique de la protection des données.

L'Office pour la protection des données a commandé deux expertises visant à clarifier certaines questions juridiques. Celles-ci concernaient les exceptions au secret médical ainsi que les tensions entre le secret professionnel et l'entraide administrative, avec une mention particulière aux méthodes d'interprétation *lex specialis* et *lex posterior*. Cette dernière expertise contient des constats importants, qui doivent encore être évalués.

[40] http://www.llv.li/amtsstellen/llv-dss-datenschutztag/llv-dss-datenschutztag-archiv.htm.

## Norvège

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

Le 9 janvier, le Storting (Parlement norvégien) a adopté un amendement à la loi relative aux données à caractère personnel. La section 26 a été remplacée par une nouvelle loi régissant le marketing direct, habilitant le médiateur des consommateurs à agir dans l'intérêt du public chaque fois que celui-ci est exposé à du marketing illicite et non éthique. L'ancienne section 26 conférait ce pouvoir à l'Inspection des données.

Au début de l'année 2009, un accord a été finalisé entre l'Inspection des données et l'agence nationale de recouvrement, lequel autorise l'Inspection à collecter à l'avenir les amendes infligées et à infliger des amendes.

Comme mentionné dans le dernier rapport annuel, le Storting a adopté une nouvelle loi sur la recherche médicale, entrée en vigueur le 1er juin 2009. L'Inspection des données n'est plus compétente pour autoriser les projets de recherche médicale. Néanmoins, elle conserve le pouvoir de mener des audits sur les responsables du traitement de données afin de veiller à leur conformité à la loi sur la recherche médicale.

Le règlement sur les données à caractère personnel a été étoffé d'un nouveau chapitre 9 régissant l'«examen des boîtes de réception de courrier électronique, etc.». Le règlement codifiait la pratique officielle de l'Inspection norvégienne des données dans ces matières. Le plus important est que les employeurs doivent suivre un protocole spécifique pour consulter les boîtes de réception personnelles de courrier électronique de leurs employés et accéder à leur espace personnel dans les réseaux informatiques. Le règlement stipule clairement qu'une partie de l'espace des employés dans l'entreprise doit rester à l'abri de toute surveillance et connexion.

La loi relative aux données à caractère personnel doit être révisée et l'Inspection des données a suggéré des modifications mineures destinées à aligner la loi sur les développements technologiques et sociétaux.

### B. Jurisprudence importante

Aucune.

### C. Questions diverses importantes

**Directive sur la conservation des données**
L'année 2009 a été dominée par le débat sur la directive sur la conservation des données. L'Inspection des données a insisté sur le fait que la directive marque une rupture avec la tradition actuelle d'enregistrement et de conservation des données de communications. À notre sens, la directive est contraire aux principes, libertés et droits de l'homme légaux et fondamentaux. Une transposition de la directive en droit norvégien implique que de grandes quantités de données relatives aux communications et mouvements des citoyens norvégiens seront enregistrées et conservées pendant une longue période. L'une des questions politiques cruciales est de savoir si le Parlement doit exercer nos droits de réserve prévus dans l'accord EEE.

Dans le débat sur cette directive, ses partisans arguent que la conservation de données n'affectera en rien la vie privée, car l'utilisation de l'information sera encadrée de conditions strictes et claires. Le projet de consultation sur la transposition de la directive en droit norvégien souligne que l'information ne sera pas consultée par la police, sauf en cas de suspicion concrète et d'autorisation d'un tribunal.

La protection de la vie privée dans la tradition juridique occidentale ne doit pas seulement prémunir contre un usage ultérieur des informations collectées, mais aussi contre la vaste collecte d'informations personnelles. Une conservation systématique des informations dans l'hypothèse où elles s'avéreraient nécessaires dans le cadre d'une future enquête peut porter préjudice à la présomption d'innocence, qui est un principe important du système juridique norvégien.

**Conclusions sérieuses au sein du Registre du cancer**
À l'occasion d'une réunion entre le Registre du cancer et l'Inspection de données norvégienne à l'automne 2008, il est apparu que le Registre du cancer lui-même doutait du fait que l'enregistrement d'informations sur des femmes en bonne santé ayant participé à un

programme de mammographie ait une base légale. L'Inspection des données a examiné la matière et découvert que, depuis 2002, le Registre de cancer a traité les données d'approximativement 600 000 femmes sans le consentement de celles-ci, et ce conformément aux exigences réglementaires du Registre du cancer.

**Proposition d'établissement d'un registre national des maladies cardiovasculaires**

Le département de la santé a proposé d'établir un registre central des maladies cardiovasculaires, qui contiendra des informations obligatoires et directement identifiables. Cela signifie que le registre comprendra des informations directement identifiables, sans le consentement des patients et sans la possibilité pour ceux-ci de refuser leur enregistrement.

Le registre mentionné n'est que l'une des différentes bases de données centrales de recherche et constituera un «modèle» pour les registres similaires d'autres groupes de maladies. L'Inspection des données insiste dès lors sur l'importance de réfléchir soigneusement à la base légale pour l'établissement de tels registres. Elle souligne que la principale base légale de l'enregistrement doit être le consentement, d'autant plus quand l'information consignée sera directement identifiable. Les listes qui ne reposent pas sur l'obtention du consentement doivent dès lors recourir à des pseudonymes, ou autrement faire l'objet d'une protection spéciale.

**Propositions de nouvelles exemptions au devoir de confidentialité du personnel de santé**

Le département de la santé a proposé, dans son message annuel, une nouvelle disposition à la section 29 b de la loi relative au personnel médical, prévoyant une exemption à la confidentialité sur le client/patient à des fins d'assurance qualité, d'administration, de planification ou de gestion des services de santé.

L'Inspection des données s'inquiète des toutes nouvelles exemptions obligatoires applicables à la confidentialité du personnel de santé. La proposition du département octroiera un très large mandat susceptible, à terme, de miner significativement la confidentialité du personnel de santé. Les patients pourraient risquer de perdre la maîtrise de leurs informations en matière de santé.

**Audit – billetterie électronique**

Au printemps 2009, l'Inspection des données a réalisé trois audits de sociétés de transport public. L'objet central des inspections était le traitement de données à caractère personnel en lien avec la billetterie électronique, à savoir les cartes de voyage électroniques.

À l'avenir, il est important pour le public de pouvoir voyager librement dans la société sans avoir à laisser de traces électroniques de leur parcours ainsi que de la date et de l'heure de leur déplacement. L'évaluation de l'autorité de la protection des données est un préalable à la réelle liberté de mouvement et à la protection de la vie privée.

Il est important que les voyageurs soient capables d'utiliser des systèmes de transport public ordinaires n'enregistrant pas d'informations sur leurs mouvements. Dans le cas des billets électroniques personnels, un point essentiel résidait dans la crainte que la société de transport ne collecte et ne conserve plus d'informations que ce qui était strictement nécessaire. L'Inspection des données a enjoint les sociétés de supprimer, immédiatement ou peu de temps après le paiement du trajet, les informations liées au voyage et susceptibles de permettre une identification.

# Chapitre 5

## Membres et observateurs du Groupe de travail «Article 29» relatif à la protection des données

# MEMBRES DU GROUPE DE TRAVAIL ART. 29 RELATIF À LA PROTECTION DES DONNÉES EN 2009

| **Autriche** | **Belgique** |
|---|---|
| Mme Waltraut Kotschy<br>Commission autrichienne de la protection des données<br>(Datenschutzkommission)<br>Ballhausplatz 1 - AT - 1014 Wien<br>Tél: +43 1 531 15 / 2525<br>Fax: +43 1 531 15 / 2690<br>E-mail: dsk@dsk.gv.at<br>Site web: http://www.dsk.gv.at/ | M. Willem Debeuckelaere<br>Commission de la protection de la vie privée<br>Rue Haute, 139 - BE - 1000 Bruxelles<br>Tél: +32(0)2/213.85.40<br>Fax : +32(0)2/213.85.65<br>E-mail: commission@privacycommission.be<br>Site web: http://www.privacycommission.be/ |
| **Bulgarie** | **Chypre** |
| M. Krassimir Dimitrov<br>Commission de protection des données à caractère personnel<br>(Комисия за защита на личните данни)<br>1 Dondukov - BG - 1000 Sofia<br>Tél: +359 2 915 3501<br>Fax: +359 2 915 3525<br>E-mail: kzld@government.bg<br>kzld@cpdp.bg<br>Site web: http://www.cdpd.bg | Mme Goulla Frangou<br>Commissaire à la protection des données à caractère personnel<br>(Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)<br>1, Iasonos str.<br>Athanasia Court, 2nd floor - CY - 1082 Nicosia<br>(P.O. Box 23378 - CY - 1682 Nicosia)<br>Tél: +357 22 818 456<br>Fax: +357 22 304 565<br>E-mail: commissioner@dataprotection.gov.cy<br>Site web: http://www.dataprotection.gov.cy |
| **République tchèque** | **Danemark** |
| M. Igor Nemec<br>Bureau de la protection des données à caractère personnel<br>(Úřad pro ochranu osobních údajů)<br>Pplk. Sochora 27 - CZ - 170 00 Praha 7<br>Tél: +420 234 665 111<br>Fax: +420 234 665 501<br>E-mail: posta@uoou.cz<br>Site web: http://www.uoou.cz/ | Mme Janni Christoffersen<br>Agence danoise de protection des données<br>(Datatilsynet)<br>Borgergade 28, 5th floor - DK - 1300 Koebenhavn K<br>Tél: +45 3319 3200<br>Fax: +45 3319 3218<br>E-mail: dt@datatilsynet.dk<br>Site web: http://www.datatilsynet.dk |

| **Estonie** | **Finlande** |
|---|---|
| M. Viljar Peep<br>Bureau estonien de la protection des données<br>(Andmekaitse Inspektsioon)<br>Väike - Ameerika 19 - EE - 10129 Tallinn<br>Tél: +372 6274 135<br>Fax: +372 6274 137<br>E-mail: info@dp.gov.ee<br>Site web: http://www.dp.gov.ee | M. Reijo Aarnio<br>Médiateur chargé de la protection des données<br>(Tietosuojavaltuutetun toimisto)<br>Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki<br>(P.O. Box 315)<br>Tél: +358 10 36 166700<br>Fax: +358 10 36 166735<br>E-mail: tietosuoja@om.fi<br>Site web: http://www.tietosuoja.fi |
| **France** | **Allemagne** |
| M. Alex Türk<br>Président<br>Président de la Commission nationale de l'informatique et des libertés – CNIL<br>Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02<br>Tél: +33 1 53 73 22 22<br>Fax: +33 1 53 73 22 00<br><br>M. Georges de La Loyère<br>Commission nationale de l'informatique et des libertés - CNIL<br>Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02<br>Tél: +33 1 53 73 22 22<br>Fax: +33 1 53 73 22 00<br>E-mail: laloyere@cnil.fr<br>Site web: http://www.cnil.fr | M. Peter Schaar<br>Commissaire fédéral à la protection des données et du droit à l'information<br>(Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)<br>Husarenstraße 30 - DE -53117 Bonn<br>Tél: +49 (0)1888 7799-0<br>Fax: +49 (0)1888 7799-550<br>E-mail: postsTélle@bfdi.bund.de<br>Site web: http://www.bfdi.bund.de<br><br>M. Alexander Dix<br>(représentant des États allemands / Bundesländer)<br>Commissaire à la protection des données et à la liberté d'information de Berlin<br>(Berliner Beauftragter für Datenschutz und Informationsfreiheit)<br>An der Urania 4-10 – DE – 10787 Berlin<br>Tél: +49 30 13 889 0<br>Fax: +49 30 215 50 50<br>E-mail: mailbox@datenschutz-berlin.de<br>Site web: http://www.datenschutz-berlin.de |

| **Grèce** | **Hongrie** |
|---|---|
| M. Christos Yeraris<br>Autorité hellénique pour la protection des données à caractère personnel<br>(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)<br>1-3, avenue Kifisias<br>115 23 GR – Athènes<br>Tél: +30 210 6475608<br>Fax: +30 210 6475789<br>E-mail: christosyeraris@dpa.gr<br>Site web: http://www.dpa.gr | M. András Jóri<br>Commissaire parlementaire à la protection des données<br>(Adatvédelmi Biztos)<br>Nador u. 22 - HU - 1051 Budapest<br>Tél:+36 1 475 7186<br>Fax: +36 1 269 3541<br>E-mail: adatved@obh.hu<br>Site web: http://abiweb.obh.hu/abi/ |
| **Irlande** | **Italie** |
| M. Billy Hawkes<br>Commissaire à la protection des données<br>(An Coimisinéir Cosanta Sonraí)<br>Canal House, Station Rd, Portarlington, IE -Co.Laois<br>Tél: +353 57 868 4800<br>Fax:+353 57 868 4757<br>E-mail: info@dataprotection.ie<br>Site web: http://www.dataprotection.ie | M. Francesco Pizzetti<br>Autorité italienne de protection des données<br>(Garante per la protezione dei dati personali)<br>Piazza di Monte Citorio, 121 - IT - 00186 Roma<br>Tél: +39 06.69677.1<br>Fax: +39 06.69677.785<br>E-mail: garante@garanteprivacy.it<br>f.pizzetti@garanteprivacy.it<br>Site web: http://www.garanteprivacy.it |
| **Lettonie** | **Lituanie** |
| M$^{me}$ Signe Plumina<br>Inspection nationale des données<br>(Datu valsts inspekcija)<br>Blaumana str. 11/13 – 15, Riga, LV-1011, Latvia<br>Tél: +371 6722 31 31<br>Fax: +371 6722 35 56<br>E-mail: signe.plumina@dvi.gov.lv<br>info@dvi.gov.lv<br>Site web: http://www.dvi.gov.lv | M. Algirdas Kunčinas<br>Inspection de protection des données<br>(Valstybinė duomenų apsaugos inspekcija)<br>A.Juozapaviciaus str. 6 / Slucko str. 2,<br>LT-01102 Vilnius<br>Tél: +370 5 279 14 45<br>Fax: + 370 5 261 94 94<br>E-mail: ada@ada.lt<br>Site web: http://www.ada.lt |

| **Luxembourg** | **Malte** |
|---|---|
| M. Gérard Lommel<br>Commission nationale pour la Protection des Données - CNPD<br>41, avenue de la Gare - L - 1611 Luxembourg<br>Tél: +352 26 10 60 -1<br>Fax: +352 26 10 60 – 29<br>E-mail: info@cnpd.lu<br>Site web: http://www.cnpd.lu | M. Joseph Ebejer<br>Commissaire à la protection des données<br>Bureau du commissaire à la protection des données<br>(Office of the Data Protection Commissioner)<br>2, Airways House<br>High Street<br>Sliema SLM 1549<br>Malte<br>Tél: +356 2328 7100<br>Fax: +356 23287198<br>E-mail: joseph.ebejer@gov.mt<br>Site web: http://www.dataprotection.gov.mt |
| **Pays-Bas** | **Pologne** |
| M. Jacob Kohnstamm<br>Autorité néerlandaise de protection des données<br>(College Bescherming Persoonsgegevens - CBP)<br>Juliana van Stolberglaan 4-10, P.O Box 93374<br>2509 AJ Den Haag<br>Tél: +31 70 8888500<br>Fax: +31 70 8888501<br>E-mail: info@cbpweb.nl<br>Site web: http://www.cbpweb.nl<br>http://www.mijnprivacy.nl | M. Michał Serzycki<br>Inspecteur général pour la protection des données à caractère personnel<br>(Generalny Inspektor Ochrony Danych Osobowych)<br>ul. Stawki 2 - PL - 00193 Warsaw<br>Tél: +48 22 860 70 86<br>Fax: +48 22 860 70 90<br>E-mail: Sekretariat@giodo.gov.pl<br>Site web: http://www.giodo.gov.pl |
| **Portugal** | **Roumanie** |
| M. Luís Novais Lingnau da Silveira<br>Commission nationale de protection des données<br>(Comissão Nacional de Protecção de Dados - CNPD)<br>Rua de São Bento, 148, 3º<br>PT - 1 200-821 Lisboa<br>Tél: +351 21 392 84 00<br>Fax: +351 21 397 68 32<br>E-mail: geral@cnpd.pt<br>Site web: http://www.cnpd.pt | M$^{me}$ Georgeta Basarabescu<br>Autorité nationale de contrôle du traitement des données à caractère personnel<br>(Autoritatea Națională de Supraveghere a Prelucrării DaTélor cu Caracter Personal)<br>Olari Street no. 32, Sector 2, RO - Bucharest<br>Tél: +40 21 252 5599<br>Fax: +40 21 252 5757<br>E-mail: georgeta.basarabescu@dataprotection.ro<br>international@dataprotection.ro<br>Site web: http://www.dataprotection.ro |

| **Slovaquie** | **Slovénie** |
|---|---|
| M. Gyula Veszelei<br>le Bureau de protection des données à caractère personnel de la République slovaque<br>(Úrad na ochranu osobných údajov Slovenskej republiky)<br>Odborárske námestie 3 - SK - 81760 Bratislava 15<br>Tél: +421 2 5023 9418<br>Fax: +421 2 5023 9441<br>E-mail: statny.dozor@pdp.gov.sk<br>Site web: http://www.dataprotection.gov.sk | M[me] Natasa Pirc Musar<br>Commissaire à l'information<br>(Informacijski pooblaščenec)<br>Vosnjakova 1, SI - 1000 Ljubljana<br>Tél: +386 1 230 97 30<br>Fax: +386 1 230 97 78<br>E-mail: gp.ip@ip-rs.si<br>Site web: http://www.ip-rs.si |
| **Espagne** | **Suède** |
| M. Artemi Rallo Lombarte<br>Agence espagnole de protection des données<br>(Agencia Española de Protección de Datos)<br>C/ Jorge Juan, 6<br>ES - 28001 Madrid<br>Tél: +34 91 399 6219/20<br>Fax: + 34 91 445 56 99<br>E-mail: director@agpd.es<br>Site web: http://www.agpd.es | M. Göran Gräslund<br>Inspection des données<br>(Datainspektionen)<br>Fleminggatan, 14<br>(Box 8114) - SE - 104 20 Stockholm<br>Tél: +46 8 657 61 57<br>Fax: +46 8 652 86 52<br>E-mail: datainspektionen@datainspektionen.se<br>goran.graslund@datainspektionen.se<br>Site web: http://www.datainspektionen.se |
| **Royaume-Uni** | **Contrôleur européen de protection des données** |
| M. Christopher Graham<br>Bureau du commissaire à l'information<br>Wycliffe House<br>Water Lane, Wilmslow, SK9 5AF GB<br>Tél: +44 1625 545700<br>Fax: +44 1625 524510<br>E-mail: Veuillez remplir le formulaire sur notre site internet<br>Site web: http://www.ico.gov.uk | M. Peter Hustinx<br>Contrôleur européen de la protection des données<br>(CEPD)<br>60, rue Wiertz, BE - 1047 Brussels<br>Office: rue Montoyer, 63, BE - 1047 Brussels<br>Tél: +32 2 283 1900<br>Fax: +32 2 283 1950<br>E-mail: edps@edps.europa.eu<br>Site web: http://www.edps.europa.eu |

# OBSERVATEURS DU GROUPE DE TRAVAIL ART. 29 SUR LA PROTECTION DES DONNÉES EN 2009

| **Islande** | **Norvège** |
|---|---|
| M^me^ Sigrun Johannesdottir<br>Autorité de protection des données<br>(Persónuvernd)<br>Raudararstigur 10 - IS - 105 Reykjavik<br>Tél: +354 510 9600<br>Fax: +354 510 9606<br>E-mail: postur@personuvernd.is<br>Site web: http://www.personuvernd.is | M. Georg Apenes<br>Bureau de protection des données<br>(Datatilsynet)<br>P.O.Box 8177 Dep - NO - 0034 Oslo<br>Tél: +47 22 396900<br>Fax: +47 22 422350<br>E-mail: postkasse@datatilsynet.no<br>Site web: http://www.datatilsynet.no |
| **Liechtenstein** | **République de Croatie** |
| M. Philipp Mittelberger<br>Commissaire chargé de la protection des données<br>Bureau de protection des données<br>(Datenschutzstelle, DSS)<br>Kirchstrasse 8, Postfach 684 – FL -9490 Vaduz<br>Tél: +423 236 6090<br>Fax: +423 236 6099<br>E-mail: info@dss.llv.li<br>Site web: http://www.dss.llv.li | M. Franjo Lacko<br>Directeur<br><br>M^me^ Sanja Vuk<br>Chef du département des affaires juridiques<br>Agence croate de protection des données à caractère personnel<br>(Agencija za zaštitu osobnih podataka - AZOP)<br>Republike Austrije 25, 10000 Zagreb<br>Tél. +385 1 4609 000<br>Fax +385 1 4609 099<br>E-mail: azop@azop.hr or info@azop.hr<br>Site web: http://www.azop.hr/default.asp |
| **Ancienne République yougoslave de Macédoine** | |
| M^me^ Marijana Marusic<br>Direction de protection des données à caractère personnel<br>(ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ)<br>Samoilova 10, 1000 Skopje, RM<br>Tél: +389 2 3244 760<br>Fax: +389 2 3244 766<br>Site web: www.dzlp.mk , info@dzlp.gov.mk | |

**Secrétariat du groupe de travail art. 29**

M^me^ Marie-Hélène Boulanger
Chef d'unité
Commission européenne
Unité de protection des données
Direction générale de la justice
Bureau: LX46 01/190 - BE - 1049 Bruxelles
Tél: +32 2 295 12 87
Fax: +32 2 299 8094
E-mail: Marie-Helene.Boulanger@ec.europa.eu
Site web: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

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.

DS-AA-11-001-FR-C doi:10.2838/39464

ISBN 978-92-79-19985-1