Quatorzième rapport

du groupe de travail «Article 29» sur la protection des données

Justice

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 défi nies 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 M059 02/013.
Site: http://ec.europa.eu/justice/data-protection/

Commission européenne — Direction générale de la justice
De plus amples informations sur l'Union européenne sont disponibles sur l'internet via le serveur Europa (http://europa.eu).

Luxembourg: Office des publications de l'Union européenne, 2013

ISSN: 1830-6454
ISBN 978-92-79-29770-0
doi: 10.2838/29618

Quatorzième rapport du groupe de travail «Article 29» sur la protection des données

Portant sur l'année 2010

Adopté le 8 décembre 2011

TABLE DES MATIÈRES

AVANT-PROPOS DU PRÉSIDENT DU GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

Les évolutions techniques de ces dernières décennies ont apporté de nombreux avantages aux consommateurs et ont donné naissance à une culture et à un vocabulaire entièrement nouveaux, intimement liés à l'emploi de l'internet, tels que les courriers électroniques, les apps et les tweets, que les consommateurs ont adoptés et utilisent au quotidien. Ces progrès techniques, ainsi que la croissance vertigineuse du nombre de services proposés sur l'internet, entraînent une augmentation considérable du volume des données à caractère personnel collectées et traitées et imposent de mettre à jour les règles en matière de protection des données, en particulier dans le contexte d'une mondialisation croissante.

En 2010, le groupe de travail a continué à centrer son travail sur la révision du cadre juridique dans l'Union européenne et a adopté des avis ciblés en la matière, notamment sur le principe de responsabilité et sur la question complexe du droit applicable, dans la lignée de la contribution conjointe à la consultation de la Commission européenne du groupe de travail «Article 29» et du groupe de travail «Police et justice» du mois de décembre 2009 (rapport sur l'avenir de la protection de la vie privée).

Le groupe de travail a été enchanté de constater que bon nombre de ses propositions avaient été, dans une grande mesure, intégrées à la communication de la Commission européenne de novembre 2010 intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne». La Commission a demandé au groupe de travail de la conseiller à nouveau en 2011, en particulier sur des questions telles que la coopération entre les autorités chargées de la protection des données (DPA), la notification, les données sensibles et le consentement.

Les règles en matière de protection des données et de la vie privée sont en cours de révision, non seulement au niveau de l'Union européenne, mais aussi à celui du Conseil de l'Europe et de l'OCDE, ainsi qu'aux États-Unis. En 2010, dans ce pays, la Federal Trade Commission a publié un premier document de travail relatif à la protection de la vie privée du consommateur (Protecting Consumer Privacy in an Era of Rapid Change) et, à la fin de l'année, le ministère du commerce y a publié un livre vert relatif à la confidentialité des données commerciales et à l'innovation dans l'économie de l'internet (Commercial Data Privacy and Innovation in the Internet Economy: a Dynamic Policy Framework). C'est l'occasion de resserrer les liens entre l'Union européenne et les États-Unis, en vue d'assurer un haut niveau de protection des données partout dans le monde.

En fin de compte, l'aspect primordial est l'effet des nouvelles règles en matière de protection des données sur les citoyens, c'est-à-dire les personnes directement concernées par ces données.

Une plus grande transparence est vitale concernant les méthodes de collecte et de traitement des données, les personnes responsables de ces opérations et les motifs de la collecte. Insister sur l'importance de la transparence peut sembler souhaitable d'un point de vue politique, mais cela peut s'avérer contreproductif. De nos jours, les recherches montrent qu'un individu, en fonction de ses activités sociales et professionnelles, peut être enregistré dans 250 à 1 000 bases de données différentes. On peut difficilement s'attendre à ce que les personnes concernées assurent le suivi de l'ensemble des opérations de collecte et de traitement de ces données et, a fortiori, à ce qu'elles exercent leurs droits d'accès, de rectification et de suppression.

Le consentement demeure une pierre angulaire de la protection des données à caractère personnel. Toutefois, se reposer trop lourdement sur celui-ci pour justifier le traitement des données n'est pas toujours possible, dans la mesure où, en pratique, les conditions d'obtention d'un consentement éclairé ne peuvent pas toujours être réunies. Dans le monde (virtuel) d'aujourd'hui, les opérations de traitement des données sont complexes et les individus sont confrontés à des choix multiples. Lorsqu'une politique de protection de la vie privée indique que la société «partage également ses informations avec des tiers soigneusement sélectionnés», ce à quoi vous consentez en réalité demeure complètement incertain.

On pourrait dès lors soutenir que le droit fondamental à la protection des données ne peut être suffisamment garanti s'il s'appuie dans une trop grande mesure sur des actions devant être entreprises par les individus eux-mêmes pour exercer leurs droits. Dès lors, l'obligation des responsables du traitement de données de veiller à un respect effectif de la législation doit être renforcée.

De nos jours, on remarque chez les responsables du traitement des données un besoin et un intérêt croissants pour une prise de mesures efficaces en faveur d'une réelle protection des données. Maintenir une bonne réputation,

s'assurer la confiance des citoyens et des consommateurs et réduire les risques juridiques et économiques sont autant d'aspects de plus en plus cruciaux pour les responsables du traitement des données. La désignation de délégués à la protection des données et l'exécution d'analyses d'impact, deux aspects relevant du principe de responsabilité, peuvent s'avérer utiles à cet égard.

Il s'agirait, en d'autres termes, d'obliger les responsables du traitement des données à prendre les mesures nécessaires dans le but de garantir le respect des principes matériels et des obligations imposés par la loi lors du traitement des données à caractère personnel et à pouvoir, sur demande, en apporter la preuve. Les créateurs de nouveaux produits et services devraient également être contraints, dès les prémices du développement, de penser à la protection et à la sécurisation des données à caractère personnel, conformément au principe de prise en considération du respect de la vie privée dès la conception (privacy by design).

Par ailleurs, un système solide de protection des données ne peut fonctionner que s'il existe des contrôles et des contrepoids et un mécanisme solide permettant de veiller efficacement au respect des règles en vigueur. Les autorités nationales chargées de la protection des données doivent donc être dotées de compétences renforcées, suffisantes pour leur permettre de remplir leurs missions correctement et en toute indépendance. En d'autres termes, ces autorités doivent recevoir les moyens de devenir de véritables institutions chargées de faire respecter les réglementations en vigueur.

Face à la multiplication des opérations transfrontalières de traitement des données, la nécessité d'une mise en œuvre uniforme du cadre juridique dans l'UE se révèle de plus en plus pertinente, en particulier pour ce qui est des activités transfrontalières de supervision et de contrôle. Le rôle du groupe de travail «Article 29» en la matière doit être renforcé et le groupe de travail lui-même doit gagner en indépendance.

En conclusion, il s'agit de restaurer l'équilibre entre les trois principaux acteurs dans le domaine de la protection des données en Europe. Pour cela, les personnes concernées doivent être mieux informées, tout en étant déchargées; les responsables du traitement doivent assumer leurs responsabilités et rendre davantage de comptes; et les autorités chargées de la protection des données doivent recevoir davantage de pouvoirs afin de garantir le respect de la loi; elles doivent en outre être dotées des moyens nécessaires en vue d'une meilleure coopération transfrontalière.

Jacob Kohnstamm

Chapitre premier
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 à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2.

1. Questions examinées par le groupe de travail «Article 29» sur la protection des données à caractère personnel[2]

1.1 TRANSFERT DE DONNÉES VERS DES PAYS TIERS

1.1.1 Dossiers passagers/PNR

Avis 7/2010 (WP 178) sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers

Le 21 septembre 2010, la Commission européenne a présenté sa communication relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers. La Commission considère que l'utilisation des données PNR à des fins d'application de la loi s'étend et qu'elle est de plus en plus considérée comme un aspect normal et nécessaire du travail des services chargés de l'application de la loi.

Par conséquent, la Commission a décidé de définir un ensemble de critères généraux qui devraient être appliqués à tous les futurs accords PNR conclus avec des pays tiers. Cette communication comporte, en outre, une analyse de l'utilisation actuelle des données PNR et présente une liste des pays tiers avec lesquels la Commission envisage de conclure des accords à l'avenir.

Le nombre de pays demandant des données PNR étant en augmentation constante, la quantité d'accords en la matière est susceptible de croître également. La Commission a décidé qu'il était donc souhaitable de définir un cadre applicable à tous les accords PNR à venir, afin d'éviter toute insécurité juridique tant pour les compagnies aériennes que pour les États membres, ainsi que les charges administratives inutiles qu'entraîne la nécessité de respecter des corpus de règles différents, en fonction du pays tiers concerné. Le groupe de travail «Article 29» salue l'approche globale adoptée par la Commission pour répondre aux demandes à l'échelon de l'UE et pour garantir des normes solides en matière de protection des données, dans le respect intégral des droits fondamentaux.

Le groupe de travail souhaite souligner qu'il ne faut pas envisager l'échange de données PNR en dehors de son contexte. L'approche globale doit dès lors être étendue aux demandes de pays tiers concernant l'ensemble des données passagers, comme les données API, la mise en correspondance des listes des pays à surveiller et les résultats des autres activités de contrôle précoce. Cela signifie également que la Commission devrait décider, lorsqu'elle reçoit une demande pour le transfert de données relatives passagers, si des données doivent être communiquées et, le cas échéant, quel type de données, par exemple des données API, serait suffisant. Enfin, elle devrait également conclure un accord à cet effet.

En ce qui concerne les données PNR, le groupe de travail a suivi de près les négociations qui ont abouti aux accords PNR avec les États-Unis, le Canada et l'Australie, et il a rendu plusieurs avis présentant les questions posées au sujet du respect de la vie privée en liaison avec ces systèmes PNR. À ce jour, de nombreuses objections soulevées par le groupe de travail n'ont pas été considérées. La communication sur laquelle porte le présent avis constitue, toutefois, un pas dans la bonne direction, bien que plusieurs sujets de préoccupation demeurent.

CONCLUSION

Globalement, le groupe de travail se réjouit que la Commission européenne affiche une compréhension claire de la nécessité d'accorder une attention accrue à la protection des données dans les accords PNR à venir et souhaite conclure des accords juridiquement contraignants afin de garantir la sécurité juridique et l'égalité de traitement. La communication présentée le 21 septembre 2010 constitue un pas dans la bonne direction. Toutefois, il convient de s'interroger de manière approfondie sur l'utilité d'un profilage à grande échelle fondé sur les données passagers, en s'appuyant sur des éléments scientifiques et sur des études récentes.

[2] Tous les documents adoptés par le groupe de travail «Article 29» sur la protection des données figurent à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2

Le groupe de travail souligne encore une fois la nécessité d'une approche globale portant sur l'ensemble des données relatives aux passagers et pas uniquement sur les données PNR. La cohérence est indispensable compte tenu des évolutions actuelles, notamment le réexamen du cadre juridique de l'UE en matière de protection des données et la proposition de négociations avec les États-Unis portant sur un accord général relatif à la protection des données.

Le groupe de travail insiste sur le fait que les normes et critères généraux figurant dans la communication devraient être considérés comme constituant un seuil minimal de protection des données à atteindre dans les accords PNR à venir. Toutefois, sur plusieurs points, ces normes pourraient et devraient être relevées.

Le groupe de travail invite par conséquent la Commission, le Parlement européen et le Conseil à tenir compte du présent avis lors des discussions relatives aux mandats de négociation se rapportant à de futurs accords PNR, ainsi qu'aux versions provisoires de ces accords, et à le tenir informé de la suite donnée. Le groupe de travail est bien sûr disposé à collaborer avec les institutions de l'UE si celles-ci estiment nécessaire qu'il précise ou développe sa position.

Enfin, le groupe de travail souhaiterait demander une nouvelle fois à être consulté ou invité à rendre un avis sur les éléments relatifs à la protection des données de tout accord à venir, en particulier eu égard à son rôle d'organe consultatif officiel de l'UE sur la protection des données et compte tenu du fait que les membres du groupe de travail sont les autorités nationales de contrôle des transporteurs qui devront respecter d'éventuels accords futurs. Il demande également à être régulièrement tenu au courant de l'état de la situation au cours des négociations de ces futurs accords.

1.1.2. Adéquation

Avis 6/2010 sur le niveau de protection des données à caractère personnel en République orientale de l'Uruguay

Le 20 octobre 2008, la mission de la République orientale de l'Uruguay (ci-après «l'Uruguay») auprès de l'Union européenne a adressé à la Commission européenne une lettre par laquelle le gouvernement uruguayen demandait officiellement d'engager la procédure en vue de déclarer que l'Uruguay assure un niveau de protection adéquat en matière de transfert de données à caractère personnel en provenance de l'UE/EEE, conformément à l'article 25, paragraphe 6, de la directive 95/46/CE relative à la protection des données à caractère personnel (ci-après «la directive»).

Afin de déterminer si l'Uruguay assure un niveau de protection adéquat, la Commission a chargé le Centre de recherche informatique et droit (CRID) de l'université de Namur de produire un rapport sur le sujet. Ce rapport circonstancié analyse dans quelle mesure le système juridique uruguayen respecte les exigences concernant le droit matériel et la mise en œuvre de mécanismes d'application des règles de protection des données à caractère personnel définies dans le document de travail «Transferts de données à caractère personnel vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données» (document WP12) adopté le 24 juillet 1998 par le groupe de travail institué en vertu de l'article 29 de la directive (ci-après, «le groupe de travail»). Par l'intermédiaire de l'Unité de régulation et de contrôle des données à caractère personnel (ci-après «l'URCDP») et en accord avec le conseil exécutif de l'URCDP, les autorités uruguayennes ont, le 11 février 2010, transmis leurs commentaires, en réponse aux questions soulevées dans ledit rapport.

Ce rapport, ainsi que les commentaires des autorités uruguayennes, ont été examinés par un sous-groupe spécialement constitué au sein du groupe de travail, qui a demandé au président de ce dernier d'envoyer une lettre aux autorités uruguayennes les informant des points susceptibles de nécessiter des éclaircissements supplémentaires.

Par l'intermédiaire de l'URCDP, les autorités uruguayennes ont transmis au groupe de travail un rapport circonstancié approuvé le 23 juin 2010 par le conseil exécutif de l'URCDP, dans lequel elles répondaient aux questions soulevées dans la lettre précitée. Elles ont également transmis une série de documents relatifs à la situation en matière de protection des données dans ce pays, notamment le rapport annuel 2009 et le rapport d'activités au 31 mai 2010 de l'URCDP, diverses décisions adoptées par le conseil exécutif de cet organe, ainsi que les décisions juridiques pertinentes en matière de protection des données à caractère personnel.

Ce rapport a été transmis en septembre 2010 aux membres du sous-groupe, qui l'ont analysé en accordant une attention particulière aux questions soulevées dans la lettre adressée par le président du groupe de travail aux

autorités uruguayennes. Après avoir étudié les informations susmentionnées, le sous-groupe a soumis son projet d'avis au groupe de travail.

Le 12 octobre 2010, le groupe de travail a rendu son avis, considérant que **la République orientale de l'Uruguay garantit un niveau de protection adéquat** au sens de l'article 25, paragraphe 6, 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.

Le groupe de travail insiste également sur le fait que, à la suite de la décision prise par la Commission, il suivra de près l'évolution de la protection des données en Uruguay, ainsi que l'application par l'autorité compétente en matière de protection des données (l'URCDP) des principes de protection des données visés dans le document WP12 et dans son avis.

1.1.3. Clauses contractuelles types

Liste des questions les plus fréquentes soulevées par l'entrée en vigueur de la décision 2010/87/UE de la Commission du 5 février 2010 relative aux clauses contractuelles types 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 du Parlement européen et du Conseil

Le 5 février 2010, la Commission européenne a adopté une décision mettant à jour les clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays non membres de l'UE qui n'assurent pas un niveau de protection adéquat des données (clauses contractuelles «responsable du traitement vers sous-traitant»).

La nouvelle décision 2010/87/UE réglemente les transferts de données entre responsables du traitement des données établis dans l'EEE et sous-traitants établis hors de l'EEE et énumère les conditions à remplir par la sous-traitance ultérieure de données entre ces sous-traitants et des sous-traitants ultérieurs établis hors de l'EEE.

Le 12 juillet 2010, le groupe de travail a adopté un document dressant la liste des questions les plus fréquentes soulevées par l'entrée en vigueur de ces nouvelles clauses contractuelles types le 15 mai 2010. Ce document reflète la position harmonisée des autorités européennes chargées de la protection des données.

Cette liste ne prétend pas à l'exhaustivité et pourra être mise à jour si nécessaire.

1.2. COMMUNICATIONS ÉLECTRONIQUES, INTERNET ET NOUVELLES TECHNOLOGIES

Avis 2/2010 (WP 171) sur la publicité comportementale en ligne

La publicité comportementale consiste à suivre les utilisateurs lorsqu'ils surfent sur l'internet et à constituer des profils à travers le temps, qui serviront ultérieurement à leur proposer des publicités correspondant à leurs centres d'intérêt. L'avis précise le cadre juridique applicable aux acteurs de la publicité comportementale.

Le groupe de travail souligne en particulier que les fournisseurs de réseaux publicitaires sont soumis à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», selon lequel le placement de cookies ou de dispositifs similaires dans l'équipement terminal d'un utilisateur ou l'accès à des informations par l'intermédiaire de ces dispositifs n'est autorisé qu'avec le consentement informé de l'utilisateur.

Il demande donc aux fournisseurs de réseaux publicitaires de mettre en place des mécanismes d'«opt-in» préalable qui nécessitent une action positive des personnes concernées indiquant leur acceptation que des cookies ou des dispositifs similaires soient placés sur leur équipement et que leur comportement sur l'internet soit suivi aux fins de l'envoi de publicités personnalisées.

Le groupe de travail considère qu'une acceptation unique par les utilisateurs de recevoir un cookie peut également emporter leur acceptation de lectures ultérieures du cookie et, partant, du suivi de leur navigation sur l'internet.

Comme la publicité comportementale repose sur l'utilisation d'identifiants permettant la création de profils d'utilisateurs extrêmement détaillés qui, la plupart du temps, seront considérés comme des données à caractère personnel, la directive 95/46/CE s'applique également. Le groupe de travail explique comment les fournisseurs de réseaux de publicité en ligne doivent se conformer aux obligations qu'impose cette directive, notamment en matière de droits d'accès, de rectification, d'effacement, de conservation, etc.

L'avis analyse et précise les obligations prévues par le cadre juridique applicable. Il ne prescrit toutefois pas la manière dont, sur le plan technologique, ces obligations doivent être satisfaites. En revanche, en différents domaines, le groupe de travail invite les professionnels concernés à engager un dialogue avec lui afin de proposer des solutions techniques et d'autres moyens de se conformer dans les meilleurs délais au cadre décrit dans l'avis.

1.3. CONTRÔLE DE L'APPLICATION

Rapport 01/2010 (WP 172) sur la deuxième action commune de contrôle de l'application de la législation UE: respect au niveau national par les fournisseurs de télécommunications et les fournisseurs de services Internet (FSI) des obligations découlant de la législation nationale sur la conservation des données relatives au trafic, sur la base juridique des articles 6 et 9 de la directive 2002/58/CE «vie privée et communications électroniques» et de la directive 2006/24/CE sur la conservation des données la modifiant

- Cette action de contrôle de l'application de la législation UE par le groupe de travail «article 29» a été décidée en vue de contrôler le respect des dispositions introduites par la directive 2006/24/CE, compte tenu des recommandations et des préoccupations exprimées par le groupe de travail dans ses précédents avis sur la question.
- L'application de la directive sur la conservation des données par les fournisseurs de services de communications électroniques et de services Internet est par nature associée à un niveau de risque élevé, qui exige des mesures de sécurité techniques et organisationnelles appropriées.
- Sur la base d'un questionnaire et de contrôles sur place, auxquels ont été soumis les principaux opérateurs et FSI nationaux afin de couvrir une importante partie du marché, l'action révèle un patchwork de mesures d'application, notamment en ce qui concerne les mesures de sécurité en place.
- Le groupe de travail «article 29» s'inquiète de constater que la directive ne semble pas avoir été appliquée d'une manière uniforme au niveau national. Il semble notamment qu'elle ait été interprétée par les États membres comme laissant à leur appréciation les limites de son champ d'application; en effet, la directive a-t-elle pour objet de permettre de déroger à l'obligation générale d'effacer les données relatives au trafic dès qu'elles ne sont plus nécessaires à la transmission d'une communication, ou bien de rendre obligatoire la conservation de toutes les données que les fournisseurs sont déjà autorisés à stocker aux fins de l'article 6, paragraphe 2, de la directive 2002/58? Le groupe de travail «article 29» soutient cette seconde interprétation, qui a également été retenue dans le récent arrêt de la CEJ dans l'affaire *Irlande contre Commission* (C-301/06).

Le groupe a fait les recommandations suivantes:

- Catégories de données à conserver: la liste des données relatives au trafic qui doivent être conservées à titre obligatoire doit être considérée comme exhaustive. En conséquence, aucune obligation supplémentaire de conservation de données ne peut être imposée aux fournisseurs en vertu de la directive sur la conservation des données.
- Durées de conservation: afin de parvenir à une plus grande harmonisation, il convient de réduire la durée maximale de conservation des données et de fixer une durée unique, plus courte, applicable à l'ensemble des fournisseurs de l'UE, comme l'a indiqué le groupe de travail «article 29» dans son avis WP113. Dans une perspective plus large, c'est la sécurité générale des données relatives au trafic «en soi» qui doit être reconsidérée par la Commission.

Mesures de sécurité techniques et organisationnelles: des mesures supplémentaires spécifiques (telles que la mise en place d'un système d'authentification solide et l'établissement d'un journal détaillé des accès) ont été détaillées, et une proposition de norme pour le transfert de données aux services répressifs a été élaborée aux fins de transferts rapides et plus fiables, permettant la collecte d'informations statistiques ainsi qu'un accès aux données responsable. À ce propos, la notion d'«infraction grave» semble devoir être clarifiée au niveau des États membres, et la liste des entités autorisées à accéder aux données devrait être communiquée à toutes les parties concernées.

1.4. RFID

Avis 5/2010 sur la proposition des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID)

Le groupe de travail analyse la proposition de l'industrie concernant la mise en œuvre de la recommandation de la Commission sur les analyses d'impact vie privée des solutions RFID.

Le groupe de travail émet des réserves sur une partie de la proposition:

- La classification des applications. Certaines applications pour lesquelles l'industrie présume qu'il n'y a pas de traitement de données personnelles sont mal classifiées et traitent des données personnelles sur la base de l'identifiant unique contenu dans le tag RFID. Pour ces applications, une analyse d'impact doit avoir lieu.
- L'absence de consultation des parties concernées dans les processus.
- Le cas des traitements de données particulières, pour lesquelles des recommandations plus précises doivent être faites.

Le groupe de travail a la conviction que les entreprises peuvent proposer un cadre amélioré sur la base des observations formulées dans le présent avis et s'engage à mettre en œuvre tous les moyens pertinents pour continuer à améliorer la proposition de cadre et parvenir à son approbation rapide.

1.5. DONNÉES À CARACTÈRE PERSONNEL

Avis 3/2010 (WP 173) sur le principe de la responsabilité

L'avis décrit les bénéfices que des mesures et pratiques concrètes internes aux entreprises et administrations peuvent apporter à la protection des données. À moins d'une réelle intégration dans les valeurs et pratiques communes d'une organisation et d'une répartition explicite des responsabilités, le respect de ces principes et obligations risque d'être compromis, et les incidents relatifs à la protection des données sont susceptibles de se perpétuer.

Pour favoriser la protection effective des données, le cadre réglementaire européen doit se doter d'outils complémentaires. À cet égard, l'avis formule une proposition concrète en vue d'établir un principe de responsabilité exigeant des responsables du traitement des données qu'ils mettent en place des mesures appropriées et efficaces pour garantir le respect des principes et obligations définis dans la directive, et qu'ils le prouvent aux autorités de contrôle qui le demandent. Cela contribuera à faire de la protection des données une réalité et aidera les autorités compétentes en la matière dans leurs missions de supervision et de mise en application.

L'avis contient en outre des suggestions visant à garantir que le principe de responsabilité offre la sécurité juridique requise, tout en laissant une certaine marge de manœuvre aux acteurs de la protection (par exemple, en leur permettant de déterminer les mesures concrètes à mettre en place selon les risques liés au traitement et les types de données traités). Il examine ensuite l'impact que pourrait avoir un tel principe sur d'autres domaines, dont les transferts de données internationaux, les exigences en matière de notification, les sanctions et, enfin, il aborde l'élaboration de programmes de certification ou de labels.

Avis 8/2010 (WP 179) sur le droit applicable

Cet avis clarifie le champ d'application de l'article 4 de la directive 95/46/CE, qui détermine quelle(s) loi(s) nationale(s) en matière de protection de données, adoptée(s) conformément à la directive, peu(ven)t s'appliquer aux traitements de données à caractère personnel. Il dégage en outre les domaines dans lesquels des améliorations sont encore possibles.

Délimiter l'application du droit de l'UE au traitement des données à caractère personnel permet de clarifier le champ d'application de la législation européenne sur la protection des données, tant dans l'Union ou l'EEE que dans un contexte international plus large. Une bonne compréhension du droit applicable contribuera à garantir simultanément la sécurité juridique pour les responsables du traitement et un cadre clair pour les individus et les autres parties prenantes. Par ailleurs, une compréhension correcte des dispositions du droit applicable devrait permettre de prévenir toute lacune dans le niveau élevé de protection des données à caractère personnel prévu par la directive 95/46/CE.

Cet avis donne également des indications et des exemples concernant: les autres dispositions de l'article 4; les obligations en matière de sécurité résultant de la législation applicable conformément à l'article 17, paragraphe 3; la possibilité pour les autorités chargées de la protection des données d'exercer les pouvoirs dont elles sont investies pour vérifier un traitement effectué sur le territoire de l'État dont elles relèvent et intervenir à ce sujet, même si le droit applicable est celui d'un autre État membre (article 28, paragraphe 6).

L'avis suggère en outre qu'il serait utile de clarifier le libellé de la directive et d'améliorer la cohérence entre les différentes parties de l'article 4 lors de la révision du cadre général régissant la protection des données.

Dans cette optique, la simplification des règles de détermination du droit applicable consisterait à revenir au principe du pays d'origine: tous les établissements d'un même responsable du traitement dans l'UE appliqueraient la même législation (celle du lieu du principal établissement), indépendamment du territoire sur lequel ils seraient situés. Cependant, cela ne pourrait être acceptable que moyennant une harmonisation générale des législations nationales, y compris les obligations en matière de sécurité.

On pourrait appliquer des critères supplémentaires lorsque le responsable du traitement est établi en dehors de l'UE, en vue de garantir l'existence d'un lien suffisant avec le territoire de l'UE et d'éviter que des responsables du traitement établis dans des pays tiers ne puissent utiliser ce dernier pour exercer des activités illégales de traitement de données. Les critères qui pourraient être envisagés dans cette optique sont, d'une part, le ciblage des personnes, entraînant l'application du droit de l'UE en matière de protection des données lorsque l'activité qui implique le traitement de données à caractère personnel cible des personnes résidant dans l'UE et, d'autre part, le critère des moyens, repris sous une forme résiduelle et limitée, qui couvrirait les cas limites (données concernant des personnes ne résidant pas dans l'UE, responsables du traitement sans lien avec l'UE) dans lesquels il existe une infrastructure de traitement de données sur le territoire de l'Union.

.

CONCLUSIONS

Cet avis vise à clarifier le champ d'application de la directive 95/46/CE et, en particulier, de son article 4. Toutefois, il met également en évidence une série de domaines dans lesquels des améliorations sont encore possibles.

1.6. CODE OF CONDUITE

Avis 4/2010 (WP 174) sur le code de conduite européen de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct

L'article 27, paragraphe 3, de la directive, qui porte sur les codes de conduite communautaires, est libellé comme suit: *«Les projets de codes communautaires, ainsi que les modifications ou prorogations de codes communautaires existants, peuvent être soumis au groupe visé à l'article 29. Celui-ci se prononce, entre autres, sur la conformité des projets qui lui sont soumis avec les dispositions nationales prises en application de la présente directive. S'il l'estime opportun, il recueille les observations des personnes concernées ou de leurs représentants. La Commission peut assurer une publicité appropriée aux codes qui ont été approuvés par le groupe.»*

Afin de faciliter l'application de cette disposition, le groupe de travail a adopté, en septembre 1998, un document clarifiant la procédure à suivre par les parties intéressées pour la soumission de codes de conduite communautaires et pour l'évaluation subséquente de ces codes par le groupe de travail, conformément aux articles 27 et 29 de la directive 95/46/CE[3]. Ce document résume les grandes étapes de la procédure à suivre dans ce contexte.

En juin 2003, le groupe de travail a adopté un avis sur le code de conduite européen de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct: le code est conforme à l'article 27 de la directive sur la protection des données et apporte suffisamment de valeur ajoutée à la directive, dans la mesure où il cible bien les questions et les problèmes de protection des données dans le secteur du marketing direct et propose des solutions suffisamment claires aux difficultés susceptibles d'apparaître[4]. Le groupe de travail a donc considéré qu'il répondait aux exigences de l'article 27 de la directive.

Le groupe de travail a toutefois souligné qu'un code général tel que celui-ci ne permettait pas, par définition, de résoudre l'ensemble des problèmes spécifiques aux activités en ligne et a, par conséquent, invité la FEDMA à élaborer une annexe traitant ces questions. Cette annexe devrait notamment porter sur la protection des enfants, qui sont particulièrement vulnérables lors d'opérations en ligne, comme souligné par le document du BEUC (l'organisation européenne des consommateurs), consulté par le groupe de travail.

Par une lettre datée du 16 décembre 2005, la FEDMA a présenté au groupe de travail «Article 29» un document contenant une «annexe au code sur la protection des données et le marketing direct» (ci-après «l'annexe»). Selon la FEDMA, cette annexe a pour objet de couvrir les problèmes particuliers soulevés par le marketing en ligne. À l'instar du code de la FEDMA, l'intention n'est nullement de remplacer la réglementation nationale ni d'y porter atteinte, ni

[3] Travaux futurs sur les codes de conduite: document de travail concernant la procédure d'examen des codes de conduite communautaires par le groupe de travail, adopté le 10 septembre 1998, WP 13.

[4] Avis 3/2003, document WP 77, disponible à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp77_fr.pdf.

d'approcher des domaines qui ne sont à l'heure actuelle pas couverts par la législation de l'UE. L'annexe vise à fournir aux opérateurs transfrontaliers des lignes directrices sur la manière de se comporter dans le cadre d'opérations de marketing en ligne.

En juin 2010, la FEDMA a envoyé une version définitive de l'annexe relative au marketing en ligne, qui est à présent conforme à la directive 95/46/CE et apporte une valeur ajoutée suffisante.

CONCLUSION

Le groupe de travail se félicite du fait que l'annexe relative au marketing en ligne du code de conduite européen de la FEDMA sur l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct soit conforme à la directive 95/46/CE, à la directive 2002/58/CE actuellement applicable, ainsi qu'à la législation nationale en vigueur[5]. Cette annexe traite de nombreux aspects importants du secteur en ligne (par exemple, les campagnes de recrutement de nouveaux membres par des membres existants, la protection des enfants et la possibilité de se désabonner) et, dès lors, elle apporte une valeur ajoutée aux directives en proposant des solutions claires aux questions qui se posent dans le secteur du marketing en ligne. Elle satisfait donc aux exigences énoncées à l'article 27 de la directive 95/46/CE. Toutefois, la transposition dans les législations nationales de la directive 2002/58/CE, telle que modifiée par la directive 2009/136/CE, pourrait exiger une modification de l'annexe, notamment en ce qui concerne les *cookies* et les logiciels espions, afin de garantir sa conformité avec les nouvelles dispositions. Le groupe de travail recommande à la FEDMA d'examiner les adaptations à apporter à l'annexe du code de conduite à partir du 25 mai 2011, afin de garantir sa conformité avec le cadre juridique découlant de la directive 2002/58/CE telle que modifiée par la directive 2009/136/CE et avec les dispositions nationales de transposition.

Afin de veiller à ce que les autorités nationales chargées de la protection des données soient dûment informées du fonctionnement pratique du code, le comité «Protection des données» de la FEDMA rédigera un rapport annuel pour le groupe de travail sur l'application du code. Si ce rapport soulève des questions, le groupe de travail prendra contact avec la FEDMA de façon à les examiner.

Le groupe de travail encourage la FEDMA à promouvoir cette annexe du code de conduite relative au marketing en ligne d'une manière volontariste dans le secteur du marketing direct, afin que les personnes concernées soient suffisamment informées de son existence et de son contenu. Il encourage également la FEDMA à poursuivre ses travaux dans ce domaine en vue d'accroître encore le niveau de protection des particuliers. Le groupe de travail accordera une attention particulière aux rapports annuels sur l'application du code qui seront présentés par le comité «Protection des données» de la FEDMA.

[5] La législation nationale peut imposer des exigences supplémentaires.

Chapitre deux

Principaux développements dans les États membres

2. Main Developments in Member States

AUTRICHE

A. Résumé des activités et actualités

Une nouvelle version de la **loi sur la protection des données** est entrée en vigueur le 1er janvier 2010. Les principales nouveautés concernent les règles en matière de vidéosurveillance, l'instauration d'une obligation de notification des cas graves de violation de la loi sur la protection des données (notification des cas de violation de données à caractère personnel) et la simplification de la notification des cas d'utilisation des données grâce au recours à une procédure de notification en ligne.

Les dispositions relatives à la procédure simplifiée de notification n'étaient pas encore d'application pendant la période de référence, d'une part parce que les conditions techniques n'étaient pas encore remplies et d'autre part parce que ces dispositions ne deviendront applicables qu'en cas de promulgation et d'entrée en vigueur d'un nouveau règlement portant sur le registre de traitement des données. Ce règlement devait être promulgué au plus tard le 1er janvier 2012.

On peut considérer de façon générale que la réglementation explicite des activités de vidéosurveillance dans le cadre de la loi sur la protection des données a largement sensibilisé la population quant au fait que les opérations de vidéosurveillance constituaient effectivement des cas d'utilisation de données à caractère personnel. En conséquence, le nombre de notifications reçues par la Commission de la protection des données à ce sujet a augmenté.

Un **amendement au règlement-type et standard** du chancelier fédéral a toutefois eu pour effet d'exclure certaines opérations de vidéosurveillance de l'obligation de notification à la Commission de la protection des données. Il s'agit plus précisément de la vidéosurveillance pratiquée par des banques, des bijouteries, des antiquaires, des orfèvres et joailliers, des bureaux de tabac et des stations-services, ainsi que de celle pratiquée par les détenteurs de propriétés privées bâties («maisons unifamiliales»).

La Commission de la protection des données s'est montrée critique envers un projet de **modification de la loi relative à la juridiction administrative** en 2010, qui prévoyait la dissolution de certaines administrations autonomes (dont la Commission de la protection des données) et le transfert de leurs activités jurisprudentielles vers de nouveaux tribunaux administratifs restant à créer. La Commission de la protection des données a tout particulièrement insisté sur le fait que les activités relevant de l'article 28 de la directive 95/46/CE devraient être transférées à une nouvelle autorité, dans la mesure où ces activités ne pouvaient pas être prises en charge par des tribunaux administratifs, ceux-ci n'étant habilités qu'à prendre des décisions de type judiciaire.

En 2010, la Commission de la protection des données a publié, dans le cadre de ses travaux de **sensibilisation** en matière de protection des données, une **brochure** intitulée ***Du bestimmst*** («C'est toi qui décides») s'adressant prioritairement aux jeunes et les informant des risques encourus lors de l'utilisation des nouvelles technologies (en particulier l'internet et les réseaux sociaux), en rapport avec la législation sur la protection des données. Cette brochure est particulièrement populaire auprès des écoles et fait systématiquement l'objet de nouvelles commandes auprès de la Commission de la protection des données.

La manifestation organisée dans le cadre de l'édition 2010 de la **Journée européenne de la protection des données** a été mise sur pied en collaboration avec le Conseil de la protection des données et la chancellerie fédérale et était avant tout consacrée aux innovations juridiques en matière de protection des données liées au traité de Lisbonne.

Organisation	Commission autrichienne de la protection des données
Président et/ou collège	Président: Dr Anton Spenling. Membre administrateur: Dr Eva Souhrada-Kirchmayer. Membres du collège: Dr Anton Spenling, Dr Eva Souhrada-Kirchmayer, M. Helmut Hutterer, Dr Claudia Rosenmayr-Klemenz, Dr Klaus Heissenberger, Mme Daniela Zimmer.
Budget	Pas de budget propre; le financement est assuré par le budget de la Chancellerie fédérale.
Personnel	20 postes à temps plein (18 temps pleins et 4 temps partiels).
Activités générales	
Décisions, avis, recommandations	61 décisions formelles (plaintes), 10 avis formels, 22 autorisations (transferts de données vers des pays tiers, recherche et enquêtes), 5 recommandations formelles.
Notifications	7 569
Examens préalables	3 977 (notifications soumises à un examen préalable).
Demandes émanant des personnes concernées	Par écrit: 913 (plaintes non comprises). Par téléphone: environ 22 500.
Plaintes émanant des personnes concernées	Plaintes ayant mené à une décision formelle: 94. Plaintes ayant mené à un éclaircissement ou à une recommandation: 298.
Conseils sollicités par le Parlement ou le gouvernement	Cette fonction relève de la compétence de deux autres institutions: le Datenschutzrat (Conseil de la protection des données) et le service juridique du gouvernement, qui dépend de la Chancellerie fédérale.
Autres renseignements relatifs aux activités générales	5 757 000 identifiants ont été délivrés par l'autorité d'enregistrement de l'administration en ligne, laquelle fait partie de l'autorité autrichienne chargée de la protection des données (DPA autrichienne). Cette autorité est responsable de la gestion sectorielle des identités au sein du système autrichien d'administration en ligne. Elle est également chargée de contrôler ce système de gestion.
Activités d'inspection	
Contrôles, enquêtes	14, la plupart en matière de vidéosurveillance.
Activités de sanction	
Sanctions	Aucune. La DPA autrichienne ne peut imposer de sanctions. La DPA a signalé une infraction à l'autorité administrative régionale compétente pour imposer des sanctions.

Amendes	Aucune. La DPA autrichienne ne peut infliger d'amendes.
DPD	
Chiffres relatifs aux DPD	Néant. Le droit autrichien ne prévoit pas de DPD.

B. Informations sur la jurisprudence

La Commission de la protection des données a donné suite à une réclamation portant sur une surveillance radar mise en place par une commune. Ce radar avait été installé afin de surveiller la circulation routière, ce qui, de l'avis de la Commission, relevait d'une fonction régalienne des pouvoirs publics. En l'espèce, la commune ne disposait toutefois pas des compétences légales pour prendre de telles mesures de police de la route; cela aurait nécessité un transfert de compétences reposant sur un règlement régional, ce qui n'était pas le cas. La décision a été (une nouvelle fois) contestée par la commune devant la Cour administrative, qui a toutefois rejeté ce recours.

Une réclamation déposée par une étudiante contre la commission électorale auprès de l'Union des étudiants de l'université de Vienne pour une violation du droit de confidentialité des données à caractère personnel dans le cadre de la participation à l'élection électronique (*e-Voting*) des représentants des étudiants a été rejetée. Le système de vote prévoyait un encodage séparé des données liées à l'identité et au vote proprement dit. Comme l'a expliqué la Commission de la protection des données, de nombreuses dispositions techniques avaient été prises pour éviter tout recoupement de ces données. Le système de vote électronique répondait par ailleurs aux dispositions de la loi relative à l'Union des étudiants et étudiantes.

Un plaignant a déposé un recours contre le «Parlement de la République d'Autriche» en invoquant une violation du droit d'information parce que sa demande de renseignements introduite auprès d'un parlementaire autrichien, par ailleurs membre d'une commission d'enquête, n'avait pas eu de suite. Les activités exercées dans le cadre d'une commission d'enquête parlementaire relevant de la fonction législative, ce dossier ne relevait pas des compétences de la Commission; la plainte a donc été rejetée.

Google Street View a été enregistré début 2010 auprès de la Commission de la protection des données. Lorsque l'on a appris, au printemps 2010, que Google Inc. avait également, au cours des voyages de reconnaissance organisés dans le cadre de son programme *Street View*, rassemblé des données WLAN (WiFi) et enregistré le contenu de certains courriels, la Commission de la protection des données a initié une procédure de contrôle à l'encontre de Google Inc. Google a ensuite effacé les contenus enregistrés.

Le membre administrateur de la Commission, agissant *ex officio* sur la base d'un soupçon de mise en péril d'intérêts légitimes à la confidentialité, a interdit à Google de continuer à utiliser toutes les données collectées dans le cadre de son programme *Street View*. On ne savait notamment pas très bien la nature exacte du lien entre l'obtention de données WLAN, non concernées par la déclaration auprès de la Commission de protection des données, et *Street View*. Cette décision a été contestée par Google Inc. auprès de la Commission de la protection des données, Google affirmant par ailleurs que plus aucune donnée WLAN n'avait entre-temps été collectée lors des voyages de reconnaissance *Street View*. Comme il est apparu par la suite, lors de la procédure d'enquête, que la collecte des données WLAN servait un autre but que l'application *Google Street View* et ne devait par conséquent pas être considérée comme relevant de l'utilisation notifiée sous le nom de «*Street View*», la décision du membre administrateur a été levée.

Une «procédure de vérification de l'enregistrement» a simultanément été lancée. Celle-ci est autorisée lorsque l'on a connaissance de circonstances justifiant une suspicion de vice d'enregistrement. Entre-temps, la notification a été améliorée et *Google Street View* a été enregistré. Parallèlement, la Commission de la protection des données a émis plusieurs recommandations à l'intention de Google Inc. À la fin de l'année 2010, une procédure de contrôle portant sur l'utilisation des données WLAN par Google Inc. était toujours en cours.

BELGIQUE

A. Résumé des activités et actualités

Atelier de traitement des dossiers 2010

En mars 2010, l'autorité belge chargée de la protection des données (la Commission de la protection de la vie privée) a accueilli le 21e atelier de traitement des dossiers au *Square* à Bruxelles. Les participants, principalement des experts juridiques de DPA européennes, ont abordé les thèmes suivants: la recherche scientifique, le marketing direct et la mobilité.

La DPA belge a contribué aux discussions sur la recherche scientifique grâce à une présentation intitulée «Trouver l'équilibre entre la liberté scientifique et la protection des données», qui a soulevé les questions suivantes: la légitimité de déposer et de stocker des données à caractère personnel dans des archives publiques et privées, les conditions possibles d'accès à ces archives et, enfin, les données à caractère personnel anonymes, encodées et non encodées.

«Vie privée et recherche scientifique: de l'obstruction à la construction»

Les 22 et 23 novembre 2010, l'autorité belge chargée de la protection des données a organisé un congrès international intitulé «Vie privée et recherche scientifique: de l'obstruction à la construction», dédié aux aspects relatifs à la vie privée et à la protection des données dans la recherche scientifique. Cet événement, organisé dans le contexte de la présidence belge du Conseil de l'UE, avait pour ambition de lancer un dialogue entre les DPA, les universités nationales et internationales et la communauté scientifique concernant les bonnes pratiques en matière de recherche médicale et de recherche historique. Le 22 novembre, des formations ont été organisées afin d'informer les participants sur des points pertinents en matière de législation relative à la protection des données et de sujets médicaux et historiques plus spécialisés, de manière à ce que tous disposent des informations nécessaires pour la participation aux ateliers de discussion organisés le 23 novembre, qui ont permis de tirer plusieurs conclusions. Davantage d'informations sur le congrès, sur ses résultats et sur les activités ultérieures sont disponibles sur le site web du congrès (http://www.privacyandresearch.be).

Questions clés - recommandations et avis

En 2010, la DPA belge a publié des documents officiels dans les domaines suivants: la télébillettique (recommandation n° 01/2010), les tierces parties de confiance (recommandation n° 02/2010), la technologie de cartographie mobile (recommandation n° 05/2010), la lutte contre le dopage (avis n° 08/2010), la levée du secret bancaire (avis n° 10 et 11/2010), la lutte contre le mariage simulé (avis n° 12/2010) et la divulgation de données de communications électroniques aux services de renseignement et de sécurité (avis n° 23/2010). Tous ces documents, ainsi que tous les avis, recommandations et autorisations adoptés en 2010 sont disponibles en français et en néerlandais sur le site web de la DPA belge, sous la rubrique «Décisions»: (http://www.privacycommission.be/en/decisions/commission/).

«Je décide», un site web de sensibilisation consacré aux jeunes et à la vie privée

Étant donné la situation vulnérable dans laquelle se trouvent régulièrement les jeunes en tant qu'utilisateurs fréquents des nouvelles technologies et après avoir consulté divers intervenants du monde éducatif, la DPA belge a entrepris de mettre en place un site web spécial, lancé en janvier 2010, visant quatre groupes cibles: les enfants, les jeunes, les parents et les professionnels du monde éducatif. Le but de ce site (en français, http://www.jedecide.be, et en néerlandais, http://www.ikbeslis.be) est de promouvoir l'utilisation des nouvelles technologies par les jeunes, tout en sensibilisant ces derniers aux avantages et inconvénients que présentent ces outils.

Organisation	Autorité belge responsable de la protection des données (Commission de la protection de la vie privée)
Président et/ou collège	M. Willem Debeuckelaere La composition du collège est disponible sur http://www.privacycommission.be.
Budget	Subvention de l'État fixée à 5 516 000 EUR pour 2010. Recettes propres: 60 000 EUR, accord spécial de la Chambre des représentants de Belgique pour l'octroi de 354 112,37 EUR supplémentaires pour l'organisation d'une conférence scientifique, de l'atelier de traitement des dossiers et des inspections Schengen.
Personnel	56 personnes
Activités générales	
Décisions, avis, recommandations	Commission: 25 avis, 1 recommandation, 1 recommandation en traitement ultérieur. Comités sectoriels: 32 avis, 209 autorisations individuelles, 4 autorisations générales, 121 associations avec autorisations générales.
Notifications	Total: 11 269 notifications pour 11 269 nouvelles opérations de traitement, 261 modifications d'opérations de traitement existantes, 73 corrections d'opérations de traitement existantes, 376 annulations d'opérations de traitement existantes.
Examens préalables	s. o.
Demandes émanant des personnes concernées	Reçues: 2 399 demandes d'information de seconde ligne (back office) et 3 008 demandes de première ligne (front office) Traitées: 1 983 demandes d'information de seconde ligne et 3 008 demandes de première ligne.
Plaintes émanant des personnes concernées	Reçues: 348. Traitées: 190.
Conseils sollicités par le Parlement ou le gouvernement	87
Activités d'inspection	
Contrôles, enquêtes	Affaires ouvertes: 85. Affaires traitées: 47.
Activités de sanction	
Sanctions	s. o.
Amendes	s. o.

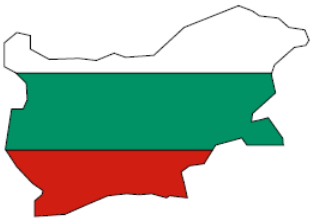
DPD	
Chiffres relatifs aux DPD	La fonction de délégué à la protection des données à caractère personnel est prévue par l'article 17 de la loi belge sur la protection des données à caractère personnel, mais il n'existe encore aucun arrêté royal mettant en œuvre cet article. Ce document est actuellement en discussion au ministère de la justice.

B. Informations sur la jurisprudence

Un arrêt de la cour d'appel de Gand s'est révélé particulièrement intéressant pour la DPA belge:

Le 30 juin 2010, la cour d'appel de Gand a dit pour droit que le portail Yahoo, son moteur de recherche et son service de messagerie électronique ne pouvaient être contraints de communiquer les données à caractère personnel des utilisateurs de ses services de messagerie électronique à la justice belge. Dans le contexte d'une enquête en matière de cybercriminalité, les inspecteurs de la *Federal Computer Crime Unit* (une unité spécialisée de la police fédérale belge) ont surveillé un groupe d'escrocs utilisant des adresses de courrier électronique Yahoo. Ces escrocs se servaient de données bancaires secrètes de sociétés pour commander des ordinateurs et d'autres équipements numériques. Yahoo a refusé de fournir aux autorités belges les données à caractère personnel liées à ces adresses de courrier électronique, en invoquant que le droit belge n'était pas applicable en l'espèce, Yahoo ne possédant pas de filiale en Belgique, et qu'aucune donnée à caractère personnel n'était stockée sur le territoire belge. En outre, Yahoo a invoqué un traité conclu entre les États-Unis et la Belgique requérant une intervention des autorités américaines pour ce type de demandes. Un tribunal belge de première instance n'a toutefois pas accepté les arguments de Yahoo et, en mars 2009, a condamné la société à une amende de 55 000 EUR, assortie d'une astreinte de 10 000 EUR pour chaque jour de non-transmission des données. Cette condamnation a ensuite été annulée par la cour d'appel de Gand.

BULGARIE



A. Résumé des activités et actualités

A.1 Modifications de la législation

À la fin de l'année 2010, la loi relative à la protection des données à caractère personnel a été modifiée et complétée à deux principaux égards: d'une part, en ce qui concerne le renforcement des compétences institutionnelles de la Commission pour la protection des données à caractère personnel (CPDP) et, d'autre part, en matière de garantie d'accès des individus à leurs données à caractère personnel.

Ces modifications législatives ont accordé davantage de compétences à la CPDP aux fins suivantes:

- to assist in the implementation of state policy in the field of protection of personal data;
- to participate in the activities of international organisations concerning personal data protection;
- to participate in the negotiations and conclusion of bilateral and multilateral agreements on personal data protection;
- to organise and coordinate the training of personal data controllers in the field of personal data protection.

La seconde modification législative, qui assure un accès gratuit aux données à caractère personnel, fait suite à une recommandation formulée dans le cadre de l'évaluation de l'état de préparation de la Bulgarie pour rejoindre l'espace Schengen.

A.2 Activités liées à l'accession de la Bulgarie à l'espace Schengen

Conformément aux mesures arrêtées dans le «plan d'action national Schengen», qui détaille les activités à entreprendre par les pouvoirs publics bulgares pour faire en sorte que le pays soit prêt à rejoindre l'espace Schengen, la CPDP a lancé en 2010 une campagne d'information en vue de sensibiliser le public aux droits des personnes concernées dans l'espace Schengen. La campagne d'information comprenait, outre la promotion du site web de la CPDP sur les organes de presse en ligne les plus consultés et les sites des institutions publiques, l'impression et la distribution de **40 000 prospectus** (20 000 en bulgare et 20 000 en d'autres langues) disponibles dans divers endroits stratégiques. Il s'agit de la seule mesure du «plan d'action national Schengen» visant directement la société civile sans se limiter à améliorer la capacité administrative du pays.

Sur le front des inspections, la CPDP a contrôlé en 2010 **neuf transporteurs aériens** pour des questions liées au traitement des données à caractère personnel des voyageurs et a commencé à organiser le contrôle de responsables du traitement des données à caractère personnel jouant un rôle clé dans le cadre du N.SIS. Pour ce qui est de la mise en œuvre des règles régissant le traitement des données à caractère personnel dans le SIS, les experts de la CPDP désignés pour traiter les questions Schengen ont suivi une formation (organisée par le ministère de l'intérieur) sur le fonctionnement du système d'information Schengen.

À la fin de l'année 2010, la CPDP a lancé une procédure pour la création d'un registre de l'UE pour les informations classifiées (déjà existant) et d'une procédure d'accès aux réseaux et systèmes d'information automatisés.

A.3 Avis sur des questions clés

En 2010, la Commission pour la protection des données à caractère personnel a été consultée et a publié des avis sur de nombreux sujets. Les avis suivants présentent un intérêt public certain: les exigences techniques minimales et les documents nécessaires à l'approbation d'un transfert des données relatives à un enfant en attente d'adoption dans les pays tiers; la maintenance d'un site web consacré à des enfants disparus qui sont des citoyens bulgares et, enfin, la communication d'un registre de «vidéosurveillance» lors du traitement de données dans le cadre d'activités de vidéosurveillance.

Organisation	
Président et/ou collège	Commission composée d'une présidente, M[me] Veneta Shopova, et de quatre membres: M. Krassimir Dimitrov, M. Valentin Enev, M[me] Mariya Mateva et M. Veselin Tselkov.
Budget	Budget attribué: 2 650 000 BGN (devise bulgare), budget exécuté: 2 393 350 BGN.
Personnel	Effectif total de 67 personnes: • 49 fonctionnaires et • 18 agents contractuels.
Activités générales	
Décisions, avis, recommandations	La commission a publié: 115 actes administratifs en lien avec des plaintes portées à sa connaissance; 22 instructions contraignantes (adressées aux responsables du traitement des données dans les secteurs de la santé, des télécommunications, du commerce et des services, du transport et de l'administration publique); 46 avis (à la demande des responsables du traitement des données, à propos de l'application de la loi sur la protection des données à caractère personnel et en lien avec les actes normatifs soumis à une procédure de consultation interinstitutionnelle); et 35 décisions autorisant le transfert de données à caractère personnel vers des pays tiers.
Notifications	86 664 responsables de la protection des données ont été ajoutés au registre de la CPDP.
Examens préalables	1 432
Demandes émanant des personnes concernées	844
Plaintes émanant des personnes concernées	221, la plupart concernant le secteur «télécommunications et société de l'information» ou les «services financiers, de crédit, de crédit-bail et d'assurance».
Conseils sollicités par le Parlement ou le gouvernement	La CPDP a émis des avis sur des actes législatifs d'ordre primaire et dérivé concernant le registre du commerce, les documents d'identité bulgares, l'accès à la base de données nationale sur la population, le système d'information du marché intérieur et le fonctionnement du N.SIS, ainsi que des avis sur des accords bilatéraux dans le domaine de la coopération policière et judiciaire.
Autres renseignements relatifs aux activités générales	La CPDP a organisé 6 séances de formation pour les responsables des données à caractère personnel, axées sur l'application des dispositions arrêtées par la loi sur la protection des données à caractère personnel. Les groupes cibles étaient les représentants des collectivités et des administrations locales, les représentants du service diplomatique national, les directeurs de centres d'éducation (l'Institut des Balkans pour le travail et la politique sociale, l'Union nationale des jurisconsultes), ainsi que les

	étudiants. De plus, la CPDP a lancé et mené une campagne d'information destinée à sensibiliser davantage le public aux droits des individus dans l'espace Schengen.
Activités d'inspection	
Contrôles, enquêtes	Nombre total de contrôles: 1 537 (principalement dans les secteurs de la santé, du commerce et des services, de l'éducation, des services sociaux, du tourisme, etc.).
Activités de sanction	
Sanctions	La CPDP a formulé 1 511 conclusions et 36 déclarations de constatation de violation administrative.
Amendes	Des frais et sanctions d'ordre patrimonial ont été imposés pour un montant de 129 500 BGN.
DPD	
Chiffres relatifs aux DPD	s. o.
Président et/ou collège	Commission composée d'une présidente, M[me] Veneta Shopova, et de quatre membres: M. Krassimir Dimitrov, M. Valentin Enev, M[me] Mariya Mateva et M. Veselin Tselkov.

B. Informations sur la jurisprudence

s.o.

C. Autres informations importantes

En 2010, la Commission pour la protection des données à caractère personnel a été saisie de plaintes concernant, pour la plupart, des violations du droit des individus à être informés du traitement de données les concernant sur l'internet. Les fournisseurs de services du secteur «télécommunications et société de l'information» (concernant la divulgation d'informations à des tiers aux fins de recouvrement de créances) étaient les premiers visés par ces plaintes, avant le secteur «services financiers, crédit, crédit-bail et assurances».

Concernant ce dernier secteur, il convient de mettre en avant une affaire concernant la divulgation des données d'une entreprise présentes dans le registre du commerce, y compris des données à caractère personnel qui, selon la CPDP, dépassaient les objectifs pour lesquels le registre a été créé. Par ailleurs, les informations divulguées n'ont pas été traitées conformément aux modalités de recevabilité.

Nous avons également constaté une augmentation du nombre de plaintes concernant le traitement de données à caractère personnel par des responsables du traitement et par des fournisseurs de services de marketing direct.

De nombreuses plaintes ont été introduites auprès de la Commission pour la protection des données à caractère personnel par des personnes s'étant vu refuser l'accès à des informations personnelles les concernant ou s'étant heurtées à un refus tacite de communication desdites données. La CPDP a également constaté des cas de violation des principes de proportionnalité et de traitement des données à des fins concrètes et licites. Elle a également constaté des cas de traitement de données violant certaines des conditions de recevabilité applicables.

Dans le cadre de la transposition finale de la directive 2006/24/CE en droit bulgare en mai 2010, la Commission pour la protection des données à caractère personnel s'est vu conférer un pouvoir légal de surveillance de l'aspect

sécuritaire des données à conserver relatives au trafic. Outre ses compétences en vertu de la loi sur la protection des données à caractère personnel, la CPDP est habilitée, en vertu de la loi sur les communications électroniques à: 1) exiger, dans le cadre de ses compétences, la communication d'informations par les gestionnaires de réseaux et/ou fournisseurs de services publics de communications électroniques; et 2) formuler des instructions contraignantes requérant une exécution immédiate.

CHYPRE

A. Résumé des activités et actualités

Au mois de mai 2010, M^me^ Panayiota Polychronidou a été désignée au poste de commissaire à la protection des données à caractère personnel. Elle succède ainsi à M^me^ Goulla Frangou, qui a occupé cette fonction pendant deux mandats.

Nos services ont, par ailleurs, été à l'origine d'un avant-projet de loi visant à modifier la loi 138(I)/2001 afin de permettre une meilleure mise en œuvre des dispositions de la directive 95/46/CE et un contrôle plus efficace de l'application de la législation nationale en matière de protection des données à caractère personnel.

Dans le cadre de nos efforts de sensibilisation et à l'occasion des activités organisées pour la Journée européenne de la protection des données à caractère personnel, nos services ont consacré 15 000 EUR à la distribution, le 28 janvier, de 42 000 dépliants informatifs à quatre journaux différents couvrant environ 93 % du tirage quotidien. Le même jour, notre personnel a distribué des dépliants et des tasses de café arborant le logo de la «Journée européenne de la protection des données, le 28 janvier» aux visiteurs des centres de service aux citoyens (guichets uniques) et a répondu aux questions des citoyens sur la protection des données à caractère personnel.

À la suite d'un rapport de l'inspecteur général constatant qu'un certain nombre de personnes s'étaient vu délivrer des permis de conduire professionnels par le département du transport routier (RTD) alors qu'elles bénéficiaient d'allocations ou d'autres prestations d'incapacité de travail des services de sécurité sociale (SIS) pour des raisons médicales, parmi lesquelles la cécité, nos services ont été consultés afin de déterminer comment les services concernés pourraient échanger des informations dans le respect des dispositions légales sur la protection des données, afin d'éviter tout nouvel octroi d'un permis de conduire professionnel à des personnes médicalement inaptes. Compte tenu de la législation actuelle régissant les compétences du SIS et du RDT, ainsi que d'un avis pertinent émis par le Procureur général de la République déclarant que l'émission d'un permis de conduire professionnel ne constitue en rien une preuve d'utilisation de ce permis, la commissaire a informé les parties requérantes que de tels incidents pouvaient être évités en échangeant les informations nécessaires grâce au regroupement de leurs systèmes de fichiers électroniques, moyennant une autorisation accordée par la commissaire en vertu de la section 8 de la loi. Cela permettrait au RTD, lorsqu'il reçoit une demande de permis de conduire professionnel, de vérifier, à l'aide de la méthode de recherche HIT/NO HIT (concordance/non-concordance), si le demandeur en question reçoit ou non, pour des raisons médicales, une allocation ou d'autres prestations d'incapacité de travail de la part des services de sécurité sociale (SIS). En cas de concordance, le directeur du RTD pourrait alors s'enquérir auprès des SIS des renseignements relatifs aux raisons médicales invoquées par le demandeur pour recevoir cette allocation ou ces prestations et, si nécessaire, rediriger ce dernier vers le conseil médical du RTD, afin de contrôler si les raisons médicales en question peuvent ou non justifier le refus d'un permis de conduire professionnel. En outre, la commissaire a indiqué que des limitations techniques devaient être mises en place, en vue de garantir que les utilisateurs du système au RTD n'accèdent qu'aux informations relatives aux personnes ayant déposé une demande de permis de conduire professionnel et non aux bénéficiaires d'allocations et de prestations qui n'ont introduit aucune demande de permis de conduire professionnel.

Organisation	Services du commissaire à la protection des données à caractère personnel
Président et/ou collège	M[me] Panayiota Polychronidou
Budget	Budget attribué: 318 091 EUR. Budget exécuté: 235 487 EUR.
Personnel	7 agents administratifs. 2 agents informaticiens. 5 secrétaires. 2 agents auxiliaires.
Activités générales	
Décisions, avis, recommandations	Nombre d'avis: 39 questions de fond.
Notifications	Nombre de notifications: 222.
Examens préalables	Nombre d'examens préalables: s. o.
Demandes émanant des personnes concernées	Nombre de demandes: s. o.
Plaintes émanant des personnes concernées	Nombre de plaintes: 804.
Conseils sollicités par le Parlement ou le gouvernement	Nombre de conseils sollicités: 16 des 39 avis ont été émis en réponse à des questions émanant d'organismes publics.
Autres renseignements relatifs aux activités générales	Autorisations de regroupement de systèmes de fichiers: 32. Autorisations de transmission de données à caractère personnel à des pays tiers: 33. Autorisations de traitement de données sensibles dans le domaine du droit du travail: 0.
Activités d'inspection	
Contrôles, enquêtes	Nombre de contrôles: 19 (18 dans le secteur bancaire et 1 dans l'unité «Asile»). En 2010, notre bureau a poursuivi les contrôles initiés en 2009 des 18 banques commerciales actives à Chypre. Dans le cadre de ces contrôles, les banques ont répondu à un questionnaire type et divers formulaires destinés aux clients ont été examinés. Dans les cas où les formulaires requéraient des consommateurs des données à caractère personnel et violaient ainsi le principe de proportionnalité, la commissaire a recommandé leur modification, afin de les rendre conformes à la loi. En

	se fondant sur les conclusions tirées des questionnaires, la commissaire a publié des lignes directrices concernant principalement les listes noires, les critères justifiant le recours à différentes périodes de conservation, en particulier pour les données des banques sur leurs clients anciens et actuels, ainsi que l'exactitude des données. Dans le cadre d'un contrôle décidé au mois de décembre 2010 par le groupe de coordination de contrôle d'Eurodac, notre bureau a demandé à l'unité «Asile» de compléter et de renvoyer un questionnaire préparé à cet effet par le groupe, destiné à vérifier les pratiques nationales en matière de suppression anticipée et de vérification de l'âge des demandeurs d'asile mineurs, ainsi que le respect par l'unité des dispositions applicables du règlement (CE) nº 2725/2000.
Activités de sanction	
Sanctions	14
Amendes	12 amendes (montant total de 17 000 EUR).
DPD	
Chiffres relatifs aux DPD	s. o.

RÉPUBLIQUE TCHÈQUE

A. Résumé des activités et actualités

En 2010, l'Office de la protection des données à caractère personnel («OPDP» ou «l'Office») a fêté sa 11e année d'existence et de travail, ainsi que le premier anniversaire de la présidence renouvelée pour cinq ans de M. Igor Němec.

L'événement le plus important de cette année a été la ***Conférence des commissaires européens à la protection des données et à la vie privée***, organisée à Prague par l'OPDP les 29 et 30 avril 2010. Sous le leitmotiv ambitieux «Peser le passé en pensant à l'avenir», la conférence s'est décomposée en quatre sessions: «L'internet des choses, la surveillance omniprésente dans l'espace et le temps», «Les enfants sur la toile des réseaux», «La protection des données à caractère personnel à la croisée des chemins», «Le secteur public: partenaire respecté ou secteur privilégié en ce qui concerne le traitement des données?». Ces quatre sessions ont en outre été complétées par un débat d'experts sur le profilage ethnique. Quatre résolutions ont été adoptées dans divers domaines: les scanners corporels à des fins de sécurité dans les aéroports, l'accord envisagé entre l'Union européenne et les États-Unis sur des normes de protection des données dans le domaine de la coopération policière et judiciaire en matière pénale, l'avenir de la protection des données et de la vie privée, ainsi que la mise en place d'actions communes de sensibilisation et d'éducation des jeunes au niveau européen et international (pour de plus amples détails, consulter http://www.uoou.cz/uoou.aspx?menu=125&submenu=614&loc=690&lang=en).

Dans le cadre de la préparation de projets de loi, le gouvernement est tenu par la loi de consulter l'Office. Par conséquent, une grande partie des activités législatives de l'OPDP ont porté, en 2010, sur des projets de ***législations spécifiques*** avec des conséquences sur la vie privée et la protection des données à caractère personnel. L'une des principales tâches de l'Office a été de participer au travail d'un groupe d'experts sur l'élaboration d'une *loi relative au traitement des échantillons d'ADN humain.* La République tchèque est toujours largement dépourvue d'une législation spécifique sur les bases de données policières conservant des renseignements sur l'ADN, même si le traitement de telles données par la police peut aujourd'hui être régulé dans une grande mesure par un simple ordre du président de la police. De même, le pays manque également d'une législation spécifique solide sur l'utilisation des *systèmes de surveillance par caméra*. L'Office a émis un commentaire dans ce domaine, portant sur un avant-projet de loi qui n'a pas été finalisé en 2010. L'Office a estimé plus approprié de ne légiférer que sur les cas d'utilisation de caméras dans les locaux et lieux accessibles au public faisant fréquemment l'objet de problèmes et de discussions.

En 2010, le début de la mise en œuvre de la directive 2009/136/CE s'est avéré d'une importance fondamentale du point de vue de la compétence de l'Office et de ses activités, en particulier dans le domaine des communications électroniques et des services liés à la société de l'information. L'Office a présenté plusieurs commentaires au sujet de la loi sur les communications électroniques (pour laquelle il supervise également les aspects relatifs à la protection des données à caractère personnel).

Parmi une quantité d'autres avant-projets commentés, celui de modification de la loi sur le casier judiciaire revêt une importance particulière.

À la fin de l'année 2010, l'Office a reçu une demande d'avis sur l'avant-projet de ***stratégie gouvernementale de lutte contre la corruption*** pour la période 2010-2012, qui comprend diverses mesures législatives en lien direct avec la protection des données à caractère personnel. De manière générale, l'Office a fait remarquer que les différentes mesures devaient respecter les principes de protection des données à caractère personnel et être donc formulées avec minutie, afin de permettre le traitement et la divulgation de données à caractère personnel dans les seuls objectifs spécifiés. Il a en outre indiqué que ces mesures ne devaient être rendues disponibles qu'aux seuls organismes dûment autorisés, conformément à des procédures précises et dans une mesure strictement nécessaire à la lutte contre les pratiques de corruption. Des objections particulières ont été soulevées, par exemple sur l'instauration d'un *registre des délits,* au regard duquel l'Office a signalé que les raisons justifiant la centralisation complète des données relatives aux délits dans les divers domaines de la vie humaine n'étaient pas parfaitement claires. L'Office a également indiqué que le régime d'enregistrement de données aussi sensibles devait inclure des garanties appropriées, similaires à celles utilisées dans le modèle strict des casiers judiciaires. D'autres remarques

ont également été formulées concernant les *tests de fiabilité* pour les personnes travaillant pour les pouvoirs publics et le *registre central des factures*.

En 2009, l'OPDP a reçu de nouvelles compétences, ainsi que de nouvelles missions, lancées et développées en 2010: créer (d'ici à juin 2012) et puis diriger le système d'information ORG (ORG IS) dans le cadre du système de registres de base lié au ***programme d'administration en ligne***. Le système d'information ORG, cofinancé par l'UE, sera employé comme convertisseur d'identité, en remplaçant le numéro national d'identité universellement utilisé qui repose sur la date de naissance par un système d'identifiants ne représentant rien de particulier et différents selon les programmes individuels ou les groupes de programmes.

Les montants provenant du budget de l'État affectés spécifiquement aux tâches susmentionnées relatives au programme d'administration en ligne (programme ORG IS) ne sont pas compris dans les sommes reprises dans le tableau récapitulatif ci-dessous.

Organisation	
Président et/ou collège	Igor Němec, président de l'OPDP
Budget	Dépenses totales: environ 97 000 000 CZK, soit environ 3 900 000 EUR.
Personnel	97 personnes: 61,5 % possédant un diplôme universitaire, 51 % de femmes.
Activités générales	
Décisions, avis, recommandations	2 avis (sur des transferts de données vers l'étranger, sur des aspects relatifs à la protection des données à caractère personnel dans le cadre de prestations de détectives privés). 10 points de vue sur des sujets d'actualité, publiés sur l'internet ou dans des bulletins (par exemple sur l'ADN).
Notifications	4 037
Examens préalables	64 (procédures liées à des notifications).
Demandes émanant des personnes concernées	3 822 questions et demandes de consultation par les citoyens.
Plaintes émanant des personnes concernées	1 039 plaintes et requêtes au titre de la loi sur la protection des données à caractère personnel. 2 834 plaintes et requêtes liées à des communications commerciales non sollicitées.
Conseils sollicités par le Parlement ou le gouvernement	217
Autres renseignements relatifs aux activités générales	317 consultations pour des personnes morales. 219 consultations pour des personnes physiques gérant une entreprise.
Activités d'inspection	
Contrôles, enquêtes	106 contrôles liés à la loi sur la protection des données à caractère

	personnel. 163 procédures de contrôle liées à des communications commerciales non sollicitées.
Activités de sanction	
Sanctions	209 sanctions financières pour un montant total de 254 000 EUR, dont 19 600 EUR pour des communications commerciales non sollicitées. En général, les sanctions financières sont accompagnées d'injonctions.
Amendes	(Voir également ci-dessus, sous «sanctions financières».) Les amendes les plus élevées ont été imposées dans le secteur public (registres centraux des médicaments, des étudiants, de la population: respectivement 92 000, 32 000 et 16 000 EUR). Dans le secteur privé, les amendes les plus importantes n'ont pas dépassé 7 200 EUR par affaire (hôtels, caméras dans les magasins et établissements d'hébergement, etc.).
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

The Czech Republic is not a typical country for legislation based on case-law, in the sense of precedent decisions by courts.

In personal data protection legislation, the jurisdiction of courts is quite important anyway because law courts have a role of second instance for complaints against the decisions of the OPDP (first instance is the President of the Office) and anybody can also bring a case before the court directly.

In 2010 there were 18 new actions lodged in the field of personal data protection. Seven actions against the Office´s decisions were dismissed by the court and six decisions of the Office were cancelled by the court.

As an example, the following are the three typical judgements, all of them regarding a complaint against the Office´s decision, where the actions were dismissed:

- the judgement of the Municipal Court in Prague (11 Ca 433/2008-89) on the privacy protection versus protection of ownership issue, related to a camera system in a hotel;
- the judgement of the Municipal Court in Prague (9 Ca 4/2008-33) on the processing of personal data by a travel agency;
- the judgement of the Supreme Administrative Court (1 As 93/2009-121) related (in general) to the nature of control and administrative procedures.

C. Autres informations importantes

En 2010, l'OPDP a enregistré moins de demandes pour ***des autorisations de transfert de données à caractère personnel vers des pays tiers.*** Cette tendance s'explique surtout par le fait que les responsables ont utilisé de manière croissante des instruments créés par la Commission européenne afin d'assurer une protection adéquate dans les pays tiers, principalement des clauses contractuelles types et le régime de la «sphère de sécurité» (" Safe Harbour ") aux États-Unis. Le plus souvent, les responsables se reposent toutefois sur les dispositions de la loi sur la protection des données autorisant les transferts sur la base du consentement ou des instructions de la personne concernée. Dans ce cas, l'autorisation de l'Office reste nécessaire.

Sur le front des *activités de coopération internationale*, l'Office a continué à participer aux tâches du groupe de travail «Article 29» sur la protection des données, ainsi qu'à celles de plusieurs de ses sous-groupes. M. Igor Němec, le président de l'OPDP, a été élu vice-président du groupe de travail «Article 29» lors de sa 77e session, en octobre 2010.

L'Office et, en particulier, ses experts, ont été invités à rejoindre diverses équipes internationales dans le cadre de projets financés par l'UE, dans des pays qui mettent en place ou qui développent leur système de protection des données à caractère personnel. L'un des juristes de l'Office, M. Jiri Mastalka, a occupé la fonction d'expert de référence dans un projet en Albanie. De plus, l'Office a désigné quatre experts à court terme pour un projet similaire dans l'ancienne République yougoslave de Macédoine. Des constatations pratiques issues des procédures de contrôle de l'Office ont été présentées à des collègues bulgares lors d'un atelier de deux jours organisé à Prague. Les experts de l'Office ont également coopéré avec des collègues polonais et hongrois dans le cadre d'un projet commun financé par le programme «Leonardo da Vinci» de l'UE.

L'OPDP a centré ses *activités de sensibilisation* et ses communications aux médias sur des prestations quotidiennes dynamiques et sur la mise à disposition d'informations actualisées, grâce à son site web, ainsi qu'au moyen de conférences de presse. L'intérêt des journalistes pour les conférences de presse s'est révélé très satisfaisant: de 20 à 25 journalistes ont assisté aux conférences et une grande diversité de médias y étaient représentés, parmi lesquels des agences, des médias électroniques et la presse écrite. Trente à soixante articles et reportages relatifs à la protection des données à caractère personnel ont été publiés dans les médias dans la foulée des conférences de presse, et ce dans un délai de trois jours après l'événement. Dans les annexes des communiqués de presse, l'Office fournit régulièrement des informations sur les enquêtes clôturées en raison de l'ouverture de procédures administratives en vue d'imposer des amendes.

Lors de sa conférence de presse hivernale, traditionnellement organisée à l'occasion de la Journée de la protection des données, l'Office a lancé le quatrième concours pour les enfants et les jeunes, intitulé «C'est ma vie privée, interdiction d'y regarder et d'y fouiller!», qui avait cette année pour objectif d'attirer l'attention des enfants et des jeunes sur les risques liés aux communications sur l'internet et à l'utilisation des réseaux sociaux.

DANEMARK

A. Résumé des activités et actualités

Organisation	
Président et/ou collège	La gestion des affaires quotidiennes de la DPA est assurée par le secrétariat, dirigé par un directeur. Les affaires particulièrement intéressantes (environ 15 par an) sont présentées au Conseil pour décision. Le Conseil est présidé par un juge de la Cour suprême.
Budget	20 300 000 DKK.
Personnel	Environ 35 personnes.
Activités générales	
Décisions, avis, recommandations	s. o. (compris dans les chiffres fournis ci-dessous).
Notifications	2 660
Examens préalables	2 660
Demandes émanant des personnes concernées	2 018 (demandes et plaintes).
Plaintes émanant des personnes concernées	s. o.
Conseils sollicités par le Parlement ou le gouvernement	383
Autres renseignements relatifs aux activités générales	52 affaires liées à la sécurité.
Activités d'inspection	
Contrôles, enquêtes	64
Activités de sanction	
Sanctions	Chaque année, la DPA danoise critique divers responsables du traitement des données pour leur non-respect de la loi sur le traitement des données à caractère personnel.
Amendes	Amendes dans trois affaires.
DPD	

Chiffres relatifs aux DPD	s. o. (Ceci n'est pas une option en vertu de la législation danoise.)

B. Informations sur la jurisprudence

Pouvoirs publics et communications par SMS

En 2009, la DPA danoise a été contactée par la municipalité de Copenhague au sujet de l'envoi de messages textuels (SMS) par la municipalité sur les téléphones portables des citoyens. Au départ, la municipalité souhaitait rappeler aux citoyens leurs rendez-vous avec l'administration locale.

La DPA danoise a déclaré qu'à son avis, toute communication transitant par le réseau de téléphonie mobile ne constituait pas une méthode de communication sûre et que les pouvoirs publics ne pouvaient donc pas envoyer d'informations sensibles et/ou confidentielles sur le téléphone portable d'un citoyen.

À cette règle générale, la DPA danoise a ajouté, en 2010, une exception, sous réserve du respect de certaines instructions:

- seuls des rappels et autres messages de service peuvent être envoyés par ce canal;
- le citoyen doit avoir préalablement accepté cette forme de communication;
- les numéros d'identification personnels ne peuvent apparaître dans ces messages;
- les destinataires ne peuvent recevoir que des informations qui les concernent eux-mêmes ou leurs enfants; et
- des mesures techniques doivent garantir que le numéro de téléphone utilisé pour la communication est le bon.

Les pouvoirs publics danois ont mis au point un système technique, appelé *nemsms,* qui fait partie intégrante de leur système de communication.

Informatique en nuage

En 2010, la DPA danoise a reçu une question de la municipalité d'Odense à propos de l'utilisation de la suite bureautique en ligne Google Apps comprenant un agenda et des fonctionnalités de traitement des documents.

La municipalité d'Odense souhaitait que les enseignants utilisent cette solution pour l'enregistrement d'informations au sujet de l'organisation des cours, de l'évaluation de la planification des cours et du développement éducationnel individuel des élèves. De plus, les professeurs auraient utilisé ces applications pour prendre des notes sur les cours et sur la coopération des élèves, de même que pour préparer les lettres destinées aux parents au sujet de leurs enfants. La municipalité désirait aussi utiliser cette solution pour planifier et envoyer les invitations aux réunions, ainsi que pour diffuser des renseignements relatifs aux activités scolaires.

Un tel usage aurait impliqué la manipulation d'informations sensibles, notamment des données sur la santé des élèves, sur des problèmes sociaux graves, ainsi que sur d'autres questions purement privées.

La DPA danoise a abordé le dossier lors d'une réunion du Conseil de la protection des données.

La DPA a décelé, dans divers domaines, des problèmes liés aux exigences imposées par la loi sur le traitement des données à caractère personnel et par le décret sur la sécurité. Aussi ne s'est-elle pas rangée à l'avis de la municipalité d'Odense, selon lequel des données confidentielles et sensibles concernant les étudiants et les parents pouvaient être traitées dans les applications Google.

Les problèmes soulevés étaient les suivants:

- la transmission de données à des pays tiers;
- des informations générales sur la sécurité du traitement liées à l'utilisation des applications Google par la municipalité d'Odense;
- les exigences imposées par la loi sur le traitement des données à caractère personnel en cas d'appel aux services d'un sous-traitant extérieur;

- la suppression des données à caractère personnel;
- la transmission et la connexion au système;
- le contrôle des tentatives rejetées d'accès aux données; et
- la journalisation.

La DPA danoise est disposée à reconsidérer le dossier et à modifier son avis si la municipalité d'Odense poursuit ses efforts et s'emploie à apporter des solutions aux problèmes identifiés.

C. Autres informations importantes

Dans son treizième rapport annuel, la DPA danoise avait fait savoir qu'un nouveau projet de loi sur une vidéosurveillance obligatoire dans les taxis allait être déposé au parlement. La DPA peut à présent annoncer que cette loi a été adoptée par le parlement danois le 22 avril 2010 et entrera en vigueur le 1er juillet 2010.

ESTONIE

A. Résumé des activités et actualités

En Estonie, la législation en matière de protection des données à caractère personnel couvre tous les secteurs de la société. Elle vise également toutes les personnes privées qui traitent des données à caractère personnel appartenant à des tiers en dehors de la sphère privée (par exemple, sur l'internet). Toutes les institutions, de même que toutes les personnes qui, selon le droit privé, remplissent des fonctions publiques ou utilisent des fonds publics, sont réputées être détentrices d'informations publiques.

L'Inspection estonienne de la protection des données (EDPI) est un petit organisme dont l'effectif se limite à 17 personnes. Cela soulève inévitablement des questions, notamment concernant l'influence que nous pouvons exercer dans notre domaine de compétence indépendamment de nos indicateurs quantitatifs. Ces dernières années, nous avons ainsi apporté des changements radicaux à notre stratégie d'action.

Notre première décision a été d'accélérer nos activités de réaction (enregistrement, demandes d'explications et examen des plaintes), afin de pouvoir nous concentrer davantage sur des activités de supervision de notre propre initiative et d'autres actions proactives. Nous livrons ci-dessous quelques exemples de mesures prises à cet égard.

- De 2008 à 2009, nous avons lancé une action majeure pour encourager les détenteurs de données à caractère personnel sensibles à respecter l'obligation de notification. Grâce à cette initiative, la surveillance nécessaire dans ce domaine est désormais moindre.
- La ligne d'assistance téléphonique diminue notre charge de travail. En effet, répondre à de simples questions par téléphone est plus rapide que de correspondre par écrit.
- Nous avons introduit une procédure de contrôle simplifiée pour les problèmes les moins compliqués.
- Nous utilisons différents niveaux de mesures basés sur le risque en réaction aux infractions.

Contrôler le volume du travail de réaction nous permet d'agir en tant que régulateur stratégique:

- nous intervenons de notre propre initiative lorsque les risques sont plus élevés et que l'intervention a un impact plus important;
- nous utilisons de nouvelles formes de supervision, telles que la surveillance comparative extensive et les audits, qui nous permettent d'avoir une vue d'ensemble;
- au lieu d'une «formation au détail», nous nous concentrons sur la préparation de lignes directrices et d'une «formation globale»;
- nous améliorons l'efficacité de la coopération; et
- nous améliorons l'efficacité de notre travail médiatique.

Le tableau ci-dessous illustre une partie des activités menées par l'EDPI ces dernières années. Le volume des missions d'explication et de conseil (demandes d'explications, ligne d'assistance téléphonique) s'est stabilisé comparé aux années précédentes. Cependant, le nombre de plaintes et de contestations a doublé. Nous sommes d'avis que cette augmentation n'est pas due à une détérioration soudaine de la situation, mais au fait que les gens sont mieux informés de leurs droits.

Le nombre de décisions prononcées a presque triplé, d'une part en raison de l'augmentation du nombre de plaintes et de réclamations et, d'autre part, en raison de l'adoption de la nouvelle forme de supervision que représente la surveillance comparative. Des dizaines ou des centaines d'objets surveillés sont examinés en une seule séance de surveillance et nous réagissons aux manquements graves par des recommandations et des décisions. Nous avons organisé trois séances de surveillance en 2009 et six en 2010.

Les audits de conformité et d'adéquation constituent un autre nouvel outil de supervision; nous avons lancé quatre audits en 2010. Ils nous permettent d'obtenir une vue d'ensemble du respect des exigences en matière de protection des données à caractère personnel par de grands systèmes d'information particulièrement sensibles. Ces audits se fondent sur une méthodologie internationale.

Depuis la fin du mois de janvier 2010, la notification des traitements de données à caractère personnel concerne majoritairement l'internet. Les filtres d'erreurs automatiques et les formulaires standardisés par type de soumission facilitent les opérations de l'expéditeur comme du destinataire. Les injonctions transmises à ceux qui ignorent l'obligation d'enregistrement sont également standardisées. Pour ces raisons, nous avons transféré à notre service administratif la mission de notification, ce qui permet à nos services spécialisés de se concentrer sur des tâches plus spécifiques.

L'année passée, nous avons publié à cinq reprises des directives sur la protection des données à caractère personnel et sur les informations publiques: Publication des données sur les défauts de paiement, Utilisation des données à caractère personnel lors des campagnes électorales, Transfert de données vers des pays étrangers, Lignes directrices pour les détenteurs d'informations qui sont des personnes morales de droit privé et Lignes directrices générales sur l'aspect public de l'information.

Organisation	
Président et/ou collège	Dr Viljar Peep
Budget	551 190 EUR
Personnel	17 fonctionnaires.
Activités générales	
Décisions, avis, recommandations	
Notifications	5 directives sur la protection des données et la liberté d'information.
Examens préalables	468 notifications d'opérations de traitement de données à caractère personnel sensibles.
Demandes émanant des personnes concernées	s. o.
Plaintes émanant des personnes concernées	893 demandes écrites et 1 061 demandes téléphoniques.
Conseils sollicités par le Parlement ou le gouvernement	592 plaintes et contestations.
Autres renseignements relatifs aux activités générales	21 avis sur des projets de lois.
Activités d'inspection	
Contrôles, enquêtes	
Activités de sanction	139 approbations de bases de données dans le secteur public

Sanctions	
Amendes	
DPD	5 séances de surveillance comparative, 6 audits et 58 contrôles sur place.
Chiffres relatifs aux DPD	

B. Informations sur la jurisprudence

La question de la vie privée dans les relations de travail

Ces dernières années, la question des données à caractère personnel des travailleurs a été la priorité de l'EDPI. Cette question couvre la collecte et l'utilisation des données des chercheurs d'emploi, des salariés et des anciens salariés, ainsi que les vérifications des antécédents des travailleurs.

On en trouve les fondements juridiques dans la loi estonienne sur les contrats de travail, qui dispose qu'un employeur préparant un contrat de travail ne peut demander à la personne concernée que des informations présentant pour lui un intérêt légitime. Lors de la relation d'emploi, l'employeur doit respecter la vie privée de ses salariés et vérifier la bonne exécution de leurs obligations d'une manière qui ne viole pas leurs droits fondamentaux. La loi estonienne sur la protection des données à caractère personnel contient également des principes généraux (limitation de la finalité, proportionnalité, etc.).

Toutefois, il ne s'agit que de principes généraux. Lorsque nous avons entamé une discussion sur leur mise en œuvre pratique, le seul avis plus ou moins clair et unanime était que les salariés ne pouvaient pas être surveillés à l'aide de caméras installées dans les toilettes et dans les salles de douches.

Des centaines de questions pratiques ont été soulevées au cours du débat, notamment: comment le passé des chercheurs d'emploi et des salariés peut-il être vérifié? qui peut lire les courriels contenant le nom du salarié et le nom de domaine de l'employeur? comment vérifier l'état de santé des salariés? qu'en est-il de la vidéosurveillance des salariés? etc.

Des différends sont également apparus sur des questions fondamentales de la théorie du droit. Par exemple, quand est-ce qu'un employeur traite les données à caractère personnel d'un salarié conformément au consentement de ce dernier (qui peut être retiré), et quand est-ce que cela peut être fait pour garantir l'exécution du contrat de travail?

Nous avons découvert qu'il n'existait aucun fondement légal nous permettant d'apporter une réponse courte et simple à ces questions. Aucune analyse juridique fondamentale n'avait encore eu lieu en Estonie. La littérature spécialisée ne couvrait que quelques aspects de la question et la pratique des tribunaux offrait encore moins d'indications. Finalement, nous avons décidé de discuter du thème de la protection de la vie privée dans les relations de travail à l'occasion de notre conférence annuelle le 27 janvier 2010, ainsi qu'un peu plus tard, lors d'une table ronde pour les employeurs et organisations centrales de salariés, à laquelle ont participé d'autres agences et experts. Notre document relatif au traitement des données à caractère personnel dans le cadre des relations de travail était finalement prêt à la publication le 24 janvier 2011.

C. Autres informations importantes

Coopération avec les gestionnaires de bases de données

Depuis 2010, l'EDPI a renforcé sa collaboration avec les plus importants responsables du traitement des données et gestionnaires de bases de données en Estonie. Plus les informations contenues dans une base de données sont sensibles, plus les mesures de contrôle interne que doit appliquer le gestionnaire lors de l'utilisation de ces informations sont sévères. Par exemple, le contrôle interne de l'utilisation du registre de la population est relativement efficace: l'EDPI est informée de tout soupçon d'utilisation à mauvais escient.

La gestion des actifs informationnels, y compris l'octroi de droits d'accès, a fait l'objet d'une centralisation au sein de la direction de la police et des gardes-frontières, après la fusion des agences, et le système de contrôle interne de

l'agence formée a été amélioré. L'EDPI conseille aux autres agences conservant des bases de données importantes et sensibles d'envisager la mise en œuvre d'une solution semblable.

Une tolérance zéro a été instaurée envers les individus qui utilisent à mauvais escient la base de données de la police. Les auteurs de tels actes s'exposent à des sanctions disciplinaires, ainsi qu'à des poursuites judiciaires. À cette fin, la police et l'EDPI échangent régulièrement des informations. Ces mesures ont entraîné un changement notable et bénéfique au sein de l'organisation.

Par ailleurs, nous avons entamé un partenariat dans le secteur des services de santé en ligne, semblable au modèle de contrôle interne des bases de données susmentionnées.

FINLAND

A. Résumé des activités et actualités

Les services du Médiateur chargé de la protection des données se sont attaqués de façon anticipative à un changement drastique dans notre environnement opérationnel. Les missions de nos services se multiplient, tandis que, simultanément, le programme national de productivité a réduit nos ressources. Nous avons amélioré notre vaste système de conseil, de planification et de surveillance, afin d'augmenter notre efficacité. Dans l'intention d'assurer l'engagement de tous les membres du personnel, nous avons renouvelé ensemble notre vision, notre plan opérationnel, nos valeurs et notre stratégie. Notre vision décrit nos objectifs, notre plan opérationnel définit notre manière d'agir, nos valeurs guident nos prises de décision et nos stratégies gouvernent les moyens que nous employons.

Conformément à leurs objectifs, nos services se sont concentrés sur les opérations de prévention. Dans le but d'influencer le public, nous avons concentré nos efforts sur la mise à disposition d'orientations et de conseils adaptés, ainsi que sur la participation à des groupes de travail et comités jouant un rôle important dans le domaine de la protection des données. Nous participons à environ 80 groupes de travail différents.

En matière d'orientations, nos travaux ont avant tout porté sur la gestion des données. La Finlande a mis en place une procédure spéciale d'information comptable censée appuyer les dirigeants d'organisation dans leurs activités de gestion et d'information, tout en permettant au médiateur chargé de la protection des données d'être plus efficace dans ses activités de contrôle du respect de la loi.

En Finlande, outre la Journée européenne de la protection des données, un jour spécial est consacré dans tout le pays à la sécurité des données, dans le cadre de la stratégie nationale pour la sécurité des informations. L'objectif est d'améliorer la prise de conscience des citoyens à l'égard des menaces qui pèsent sur la sécurité, ainsi que d'approfondir leurs connaissances sur les moyens pouvant être mis en œuvre afin de combattre ces menaces et sur la manière dont les personnes concernées peuvent protéger leurs droits.

Nos services ont collaboré étroitement avec différents groupes d'intérêts. Plusieurs groupes de pilotage sur la protection des données ont opéré, entre autres, dans les secteurs de la santé publique, de la sécurité sociale, des télécommunications et de l'éducation. Dans le courant de l'année, un nouveau groupe de pilotage conjoint entre les services du Médiateur et les représentants du monde de l'entreprise a été créé. Celui-ci a concentré ses travaux sur des questions actuelles relatives à la protection des données dans le domaine du marketing et de la gestion des relations avec les consommateurs. Les premiers réseaux d'experts en matière de protection des données organisés par le secteur privé lui-même ont également débuté leurs activités.

Une loi adoptée par le parlement au sujet de l'identification électronique est entrée en vigueur. Simultanément, le groupe spécial de gestion de l'identité, associé au ministère de l'intérieur, a proposé un éclaircissement sur la criminalisation du vol d'identité.

Enfin, après le jugement sur les données fiscales et les moyens de communication de masse, la loi sur les données à caractère personnel, qui met en œuvre la directive 95/46/CE sur la protection des données, a été modifiée à l'initiative du ministère de la justice.

Le tableau ci-dessous synthétise les principaux chiffres liés aux services du Médiateur chargé de la protection des données.

Organisation	
Président et/ou collège	Reijo Aarnio est le médiateur chargé de la protection des données depuis le 1er novembre 1997.
Budget	Le budget annuel total est d'environ 1 541 403 EUR.
Personnel	L'effectif total comprend 20 personnes.

Activités générales	
Décisions, avis, recommandations	
Notifications	2 601
Examens préalables	284
Demandes émanant des personnes concernées	Voir notifications
Plaintes émanant des personnes concernées	881
Conseils sollicités par le Parlement ou le gouvernement	(Accès et rectifications) 174
Autres renseignements relatifs aux activités générales	110
Activités d'inspection	Collaborations avec des responsables des données dans les secteurs suivants: l'éducation, les soins de santé, les affaires sociales, les télécommunications, l'emploi et l'économie.
Contrôles, enquêtes	
Activités de sanction	
Sanctions	1 972
Amendes	
DPD	82
Chiffres relatifs aux DPD	

B. Informations sur la jurisprudence

Vie privée

La Cour suprême a condamné les auteurs du livre *Prime Minister's Bride* pour avoir diffusé des informations diffamatoires sur la vie privée du premier ministre. La Cour suprême a considéré l'auteur et l'éditeur comme responsables, car le livre publié comprenait des détails sur des éléments déterminants de la vie privée du premier ministre, ainsi que des informations sur des évènements privés. La Cour a souligné que la fonction de premier ministre occupée par un individu, ainsi que la capacité de cette personne à exercer un pouvoir politique considérable, signifient que la protection de sa vie privée est plus limitée que pour une personne privée. Toutefois, même la vie privée d'un politicien de premier rang et, en particulier, ses éléments fondamentaux, ne peuvent pas rester sans protection (arrêt 2010.39 de la Cour suprême).

La Cour administrative suprême a tranché une affaire relative aux résultats d'un test d'aptitudes. X et Y avaient tous deux déposé leur candidature pour le poste de directeur. Après l'élection d'Y au poste de directeur, X a demandé à recevoir les résultats du test d'aptitudes d'Y. X a invoqué pour cela la section 11 de la loi sur la transparence des activités des pouvoirs publics, ce test ayant pu avoir des conséquences sur la résolution d'une affaire concernant X.

Cependant, selon la Cour administrative suprême, fournir à X des informations sur le test d'aptitudes d'Y aurait été contraire à un intérêt privé majeur. La Cour s'est fondée sur le projet du gouvernement indiquant que rendre publics les résultats des tests d'aptitudes est contraire au droit humain de protection de la vie privée (arrêt 2010:60 de la Cour administrative suprême).

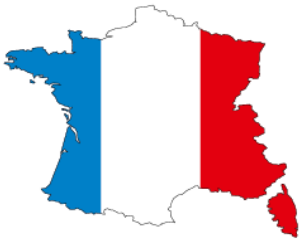
Protection des données

La Cour administrative suprême a statué concernant le droit à l'information de la police par les institutions d'assurances sociales au sujet des achats en médicaments d'un individu, dans le cadre d'une enquête de police portant sur un assassinat présumé. La Cour administrative suprême a autorisé la police à obtenir les informations requises en vertu de la section 35 de la loi sur la police (arrêt 2010:42 de la Cour administrative suprême).

Un requérant a demandé à la commission de protection des données si les informations sur l'historique de réparation des véhicules motorisés étaient considérées comme des données à caractère personnel au sens de la section 3 de la loi sur la protection des données à caractère personnel. Ce requérant a demandé l'autorisation de traiter ce type d'informations en vue de créer une nouvelle base de données pour traiter, conserver et partager ces renseignements. La commission de protection des données a rejeté la demande, dans la mesure où le traitement ne remplissait pas les conditions d'exactitude, car des données erronées, incomplètes ou obsolètes pourraient être traitées, ni les conditions d'exclusivité de l'objectif, puisque ce traitement complémentaire n'avait pas été défini avant la collecte des données. D'après la commission de protection des données, les numéros de plaques d'immatriculation doivent être considérés comme des données à caractère personnel (décision 2/932/2009 de la commission de protection des données).

La cour administrative de Turku a confirmé la décision de la commission de protection des données interdisant à une entreprise de traiter et d'envoyer via un service de messages textuels (SMS) des données relatives aux revenus mobiliers et professionnels de personnes physiques, dans l'affaire sur les données fiscales et les moyens de communication de masse (arrêt 10/0846/2 de la cour administrative de Turku).

FRANCE



A. Résumé des activités et actualités

Les jeunes, une cible prioritaire pour la CNIL....

Les jeunes sont les acteurs privilégiés du numérique d'aujourd'hui et de demain. En 2010, CNIL a souhaité faire de la sensibilisation des jeunes et des professionnels de l'éducation une de ses priorités.

C'est pourquoi elle a entrepris un effort sans précédent en leur direction en consacrant plus de 500 000 euros à une opération impliquant, notamment, la réalisation de deux éditions spéciales des journaux dédiés aux 10-14 ans et aux 14-18 ans consacrées à la question de la protection de la vie privée sur Internet.

La CNIL, une autorité pragmatique...

Persuadée que la diffusion de la culture informatique et libertés passe par un meilleur service aux usagers, la CNIL offre désormais la possibilité d'effectuer les formalités préalables en ligne ou encore de déposer plainte directement en ligne. Aujourd'hui, près de 20 % des plaintes sont ainsi adressées à la CNIL sous forme dématérialisée.

La CNIL a par ailleurs mis en œuvre une politique de contrôles très active.

Ainsi, en 2010, et alors que le cadre juridique des contrôles a été précisé[6], le nombre de contrôles effectués s'est élevé à 308 contrôles contre 270 l'année précédente. Une attention particulière a été portée aux contrôles sur les dispositifs de vidéosurveillance relevant de la loi «informatique et libertés». 55 contrôles ont ainsi porté sur ces dispositifs. De nombreux manquements ont ainsi été constatés portant notamment sur l'absence de déclaration, la disproportion du traitement, la durée de conservation des images excessive ou encore le défaut d'information ou de sécurité.

La CNIL, c'est aussi une autorité qui a su adopter des recommandations ou des délibérations aux nouvelles problématiques posées par les jeux en ligne, le vote électronique ou encore par l'application informatique permettant la gestion administrative et pédagogique des élèves.

Ce pragmatisme, et cette volonté de coller au plus près aux usages, s'appuie sur le travail réalisé par le service de l'expertise de la CNIL qui a été renforcé en termes d'effectifs et qui suit les développements les plus récents en matière de nouvelles technologies; la CNIL peut ainsi anticiper et être à même de conseiller les entreprises sur les problématiques nouvelles.

La CNIL, une autorité tournée vers l'avenir...

Afin de mieux identifier et anticiper les évolutions et de faire face au développement massif des nouvelles technologies pouvant avoir un impact sur la protection des données personnelles, une nouvelle direction a été créée au sein de la CNIL: la Direction des Etudes, de l'Innovation et de la Prospective (DEIP).

C'est ce même souci d'influer sur l'avenir de la protection des données qui pousse la CNIL à être particulièrement active dans le cadre de la révision de la directive 95/46.

---

[6] Voir les deux décisions du Conseil d'Etat N°304300 et N°304301 du 6 novembre 2009 - le Conseil d'Etat a décidé d'annuler deux sanctions prononcées par la CNIL aux motifs que les contrôles sur place sur la base desquels étaient prononcées les sanctions étaient irréguliers faute d'information suffisante des responsables de traitements. Depuis lors, la CNIL a dû modifier ses pratiques et informe dorénavant systématiquement les personnes faisant l'objet d'un contrôle sur place de leur droit à s'opposer à ce contrôle.

Organisation	Commission nationale de l'informatique et des libertés – CNIL (France)	*Commission*
Président et/ou collège	Président: Alex Türk Vice-présidents: Isabelle Falque-Pierrotin, Emmanuel de Givry Composition du collège: 4 parlementaires/2 membres du Conseil économique et social/6 juges de la Cour suprême/5 personnalités qualifiées désignées par le Conseil des ministres (3), par le président de l'Assemblée nationale (1) et par le président du Sénat (1)	Chairman: Ale Vice-Chairper Composition Economic and appointed by Chairman of
Budget	Montant total des crédits pour 2010: 14 700 000 EUR	Total credits
Personnel	Effectif: 148	Number of st
Activités générales		
Décisions, avis, recommandations	1 659 décisions/avis/recommandations	1 659 decisio
Notifications	68 863 notifications à la CNIL	68 863 notifi
Examens préalables	Demandes d'autorisation: 1 682 demandes d'autorisation et 4 273 demandes d'autorisation comprenant l'engagement des responsables des données de se conformer à une autorisation unique de la CNIL. Autorisations: 1 346 autorisations et 4 273 autorisations délivrées sur la base de l'engagement des responsables des données de se conformer à une autorisation unique de la CNIL.	Request for for authorisa decision of th Authorisation receiving the the CNIL.
Demandes émanant des personnes concernées	Demandes émanant du public: 28 490 demandes écrites et 10 000 appels téléphoniques par mois. Demandes émanant des personnes concernées: 1 877 demandes d'accès indirect dans le cas où le traitement des informations concerne la sécurité de l'État, la défense nationale ou la sécurité publique.	Requests fro Requests fro involves Stat
Plaintes émanant des personnes concernées	4 821 plaintes émises par des personnes concernées (travail: 20 %, banques: 20 %, entreprises: 20 %, internet/télécommunications: 20 %, santé/social: 5 %, autres: 15 %)	4 821 compl Internet / Tele
Conseils sollicités par le Parlement ou le gouvernement	8 avis sur des règlements 78 avis sur la mise en œuvre de traitements des données au nom de l'État	8 opinions or 78 opinions
Autres renseignements relatifs aux activités générales	500 000 EUR pour une campagne de sensibilisation du public	EUR 500 000
Activités d'inspection		
Contrôles, enquêtes	308 contrôles (biométrie: 54, marketing: 78, fichiers de police: 40, nouvelles technologies: 12, sécurité des données: 15, services à la population: 10, travail: 91, autres: 8)	308 investig technologies: 8)

Activités de sanction		
Sanctions	Sanctions imposées par la CNIL: 4 Actions en justice à l'encontre des responsables de données: 118 (mises en demeure: 111, avertissements: 4, procédures d'urgence: 3)	Sanctions imp Legal actions Emergency p
Amendes	Amendes imposées par la CNIL pour un montant total de 32 500 EUR	Total amount
DPD		
Chiffres relatifs aux DPD	7 300 organisations ont désigné un «correspondant informatique et libertés» (CIL).	7 300 organi

ALLEMAGNE

A. Résumé des activités et actualités

En dépit de la modification, en 2009, de la loi fédérale sur la protection des données (BDSG), le débat sur une modernisation nécessaire de la législation sur la protection des données se poursuit en Allemagne. En mars 2010, la Conférence des commissaires à la protection des données de la Fédération et des *Länder* a adopté un document abordant une série de questions clés, intitulé «Une législation sur la protection des données moderne pour le XXIe siècle». Ce document est une contribution au débat sur la réforme de la législation nationale en matière de protection des données et il contient d'importants principes fondamentaux censés guider cette modernisation.

Différentes modifications de la BDSG sont entrées en vigueur en 2010:

- En ce qui concerne les agences de notation et la fixation des notes, des règles améliorées en matière de protection des données sont entrées en vigueur le 1er avril 2010 (section 28b de la BDSG). Elles déterminent plus précisément quelles données à caractère personnel peuvent être transférées lors d'une demande effectuée à une agence de notation. De plus, pour la première fois, les conditions d'application et de mise en œuvre d'une procédure de notation ont été définies par la loi. Les droits à l'information des personnes concernées ont été renforcés; il existe désormais un droit à l'information gratuite sur les notes transférées à des tiers et sur la méthode de calcul du score individuel.
- Grâce à la mise en œuvre de la directive sur le crédit à la consommation, en vigueur depuis le 11 juin 2010, la BDSG garantit dorénavant l'égalité de traitement des prêteurs européens concernant l'accès aux agences de notation domestiques (section 29, paragraphe 6, de la BDSG).
- Une plus grande transparence est assurée par le nouveau règlement, selon lequel le consommateur doit être immédiatement informé si, lors d'un contrat de crédit à la consommation ou de contrats de concours financier à un paiement, sa demande de prêt est refusée après consultation (à l'issue négative) d'une agence de notation (section 29, paragraphe 7, de la BDSG).

Sur l'année qui nous concerne, presque tous les États fédérés (*Bundesländer* ou *Länder*) ont lancé leurs mesures respectives dans le but d'assurer in fine l'indépendance totale des autorités de contrôle de la protection des données dans le secteur non public, comme exigé par la Cour européenne de justice (arrêt du 9 mars 2010 dans l'affaire C-518/07). Dans l'écrasante majorité des *Länder,* il est envisagé de confier le contrôle du secteur non public aux commissaires à la protection des données des *Länder*, à moins que cela soit déjà le cas. Le pouvoir exécutif ne peut exercer la moindre influence sur les autorités chargées de la protection des données. Ces dernières doivent donc disposer d'une autonomie suffisante pour la gestion de leur personnel, de leur budget et de leur organisation. Toutefois, l'arrêt rendu par la Cour de justice de l'Union européenne sur l'avis du commissaire fédéral allemand pour la protection des données et la liberté d'information n'a pas encore fait sentir tous ses effets. Même si seul le contrôle de la protection des données dans les *Länder* est mentionné explicitement dans l'arrêt, les principes mis en avant dans cette décision sont également applicables au contrôle de la protection des données au niveau fédéral.

Comme les années précédentes, nos missions et notre charge de travail ont connu une importante croissance en 2010: par exemple, le nombre de plaintes reçues par mes services est passé de 5 066 en 2009 à 6 087 en 2010. Il est donc d'autant plus réjouissant que mes services aient pu voir leur effectif augmenter de 12,5 personnes durant l'exercice financier 2010. De 69 personnes, l'effectif est passé à 81 personnes. Ces employés supplémentaires permettent à mes services de mieux gérer leurs missions juridiques existantes en lien avec les procédures de contrôle, d'assurer une consultation pour les questions relatives à la législation sur la protection des données et, enfin, d'assumer de nouvelles tâches de façon proactive. Ainsi, nous avons pu, en particulier, développer notre compétence liée à la protection des données techniques et renforcer notre travail de surveillance et de contrôle. J'ai également étendu mon offre d'information au public, par exemple au moyen de nouveaux dépliants thématiques et

d'un court métrage diffusé sur mon site web qui traite de l'importance de la protection des données et des missions confiées à mes services.

Davantage de détails au sujet de mes activités en 2010 sont disponibles dans mon 23e rapport d'activités portant sur les années 2009 et 2010, disponible sur mon site web à l'adresse http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/TB_node.html. Mon communiqué de presse en anglais au sujet de ce rapport se trouve, quant à lui, à l'adresse http://www.bfdi.bund.de/EN/PublicRelations/PressReleases/2011/23rdActivityReport.html?nn=410156.

Il convient de préciser qu'en Allemagne, le commissaire fédéral à la protection des données et à la liberté d'information n'est pas la seule entité agissant en tant qu'autorité chargée de la protection des données. Chaque État fédéré (*Land*) possède un commissaire à la protection des données. Certains possèdent également des autorités de contrôle distinctes pour le secteur privé.

Le tableau ci-dessous ne concerne que les services du commissaire fédéral à la protection des données et à la liberté d'information.

Organisation	
Président et/ou collège	Peter Schaar, commissaire fédéral à la protection des données et à la liberté d'information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit [BfDI])
Budget	6 500 000 EUR
Personnel	81
Activités générales	
Décisions, avis, recommandations	
Notifications	s. o.
Examens préalables	s. o.
Demandes émanant des personnes concernées	s. o.
Plaintes émanant des personnes concernées	13 257
Conseils sollicités par le Parlement ou le gouvernement	6 087
Autres renseignements relatifs aux activités générales	s. o.
Activités d'inspection	Les règles d'entreprise contraignantes de la Deutsche Post AG ont été adoptées en décembre 2010.
Contrôles, enquêtes	
Activités de sanction	
Sanctions	52

Amendes	
DPD	
Chiffres relatifs aux DPD	30 plaintes (2009 et 2010) en vertu de la section 25 de la loi fédérale sur la protection des données.

B. Informations sur la jurisprudence

Décision du Tribunal constitutionnel fédéral sur la conservation des données relatives au trafic des télécommunications :

Dès 2008, le Tribunal constitutionnel fédéral avait déjà prononcé, en procédure de référé, deux jugements limitant strictement l'utilisation des données conservées à des fins d'utilisation ultérieure. Par son jugement du 2 mars 2010, le tribunal a annulé les dispositions légales relatives à la conservation des données en les déclarant anticonstitutionnelles. Cette décision a signifié la victoire du plus large recours constitutionnel collectif dans l'histoire de la République fédérale d'Allemagne, avec plus de 35 000 requérants.

Dans le cadre de ce constat d'inconstitutionnalité, le tribunal a toutefois précisé que conserver des données à caractère personnel durant six mois sans raison n'était strictement interdit que si la conservation avait lieu à des fins vagues et non encore déterminées. Dès lors, une application constitutionnelle de la directive européenne sur la conservation des données serait en principe possible, moyennant toutefois le respect d'exigences très strictes, dans la mesure où la conservation des données implique une intrusion jugée extrêmement sérieuse dans les télécommunications privées.

Dans la perspective d'une éventuelle révision de la loi, le tribunal a mentionné quatre domaines à respecter afin de s'assurer de la constitutionnalité des dispositions relatives à la conservation des données. Outre des normes strictes de sécurité des données, un niveau de transparence adéquat et un système efficace de protection juridique, le législateur doit surtout établir par la loi des règles claires sur le champ d'utilisation des données.

De plus, le tribunal a indiqué que, de manière générale, la conservation préventive des données sans raison particulière devait toujours demeurer une exception, en particulier en association avec d'autres ensembles de données déjà existants, et qu'elle ne devait pas entraîner la possibilité de pratiquement retracer toutes les activités des citoyens. La République fédérale d'Allemagne doit défendre cette idée en Europe et à l'échelle internationale.

Sources d'information:

http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (jugement en allemand)

http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html (communiqué de presse en allemand)

http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html (communiqué de presse en anglais)

Au cours de la période visée par le rapport, un débat animé s'est déroulé sur l'acquisition par les autorités fiscales allemandes de CD de données fiscales issus de «sources douteuses» étrangères, qui contenaient des informations sur de supposés fraudeurs fiscaux allemands. Entretemps, le Tribunal constitutionnel fédéral a jugé que pour toute nouvelle enquête liée au droit fiscal, le premier soupçon pouvait être appuyé par des données provenant d'un CD de données fiscales acquis par les autorités allemandes. Dans l'affaire présentée au tribunal, un informateur du Liechtenstein avait vendu un CD-ROM contenant des informations sur des personnes suspectées de fraude fiscale au service fédéral du renseignement, lequel a mis le CD à la disposition des autorités fiscales (voir le jugement 2 BvR 2101/09 du Tribunal constitutionnel fédéral du 9 novembre 2010).

C. Autres informations importantes

Gestion des géodonnées conformément aux exigences de protection des données

En réponse aux discussions en cours sur le service de géodonnées par l'internet Google Street View, les entreprises du secteur de l'internet, sous la houlette de leur organisation professionnelle BITKOM, ont présenté en décembre 2010 un «code de protection des données» visant à tenir compte des intérêts des propriétaires et des habitants en matière de publication sur l'internet de vues d'édifices. Ce code n'a pas fait l'objet d'une collaboration avec les autorités allemandes de protection des données, ni n'a été rédigé de façon appropriée du point de vue de la protection des données, puisque cet engagement volontaire du secteur n'aménage un droit d'objection qu'une fois les clichés des édifices déjà publiés sur l'internet, et parce qu'il n'est contraignant que pour les sociétés ayant signé le code. Or les autorités chargées de la protection des données estiment qu'un droit de récusation doit être aménagé avant la publication. Elles ont également demandé à ce que le code n'inclue pas uniquement les vues prises de la rue, mais aussi les photographies aériennes obliques. En conséquence, les autorités chargées de la protection des données ont appelé le législateur à prendre des mesures.

Nouvelle loi sur les cartes d'identité

Avec l'entrée en vigueur, le 1er novembre 2010, de la loi modifiée sur les cartes d'identité, un nouveau modèle de cartes d'identité a été introduit en Allemagne. La nouveauté de ces cartes est qu'elles peuvent être utilisées, outre pour l'accomplissement de leurs fonctions prévues par la loi, comme preuve électronique d'identité. Elles sont équipées d'une puce électronique comprenant des zones séparées pour les données biométriques et les données d'identification stockées aux fins prévues par la loi, pour la signature électronique et pour la fonctionnalité d'identité électronique (eID). L'utilisation de la fonctionnalité eID et de la signature électronique est volontaire. C'est aussi au titulaire de la carte d'identité de décider s'il souhaite que ses empreintes digitales soient enregistrées, en plus de la photographie, qui est obligatoire.
Du point de vue de la protection des données, l'avantage de cette nouvelle carte est surtout la possibilité de répondre aux offres sur l'internet en toute sécurité et sous un pseudonyme, à l'aide d'un identifiant spécifique aux services et aux cartes.

Identification par radiofréquence (RFID)

En vue d'analyser les menaces pesant sur la protection des données dans le cadre de l'utilisation de l'identification par radiofréquence, un outil destiné à évaluer les répercussions de ce genre de techniques sur la protection des données, appelé «évaluation de l'impact sur la vie privée» (*Privacy Impact Assessment*, PIA), a été conçu au niveau européen. Le secteur privé allemand a participé au développement de cet instrument. À l'avenir, les secteurs de l'industrie, du commerce et des affaires utilisant l'identification par radiofréquence devront rédiger des rapports et les soumettre aux autorités nationales de contrôle avant d'entamer leurs opérations. Cette «évaluation de l'impact sur la vie privée» a été officiellement adoptée par la Commission européenne en avril 2011.

L'Office fédéral pour la sécurité en matière de technologies de l'information (BSI) a, pour sa part, publié un nouveau document détaillant certains principes fondamentaux en matière de sécurité des données et de protection de ces dernières lors de l'identification par radiofréquence. Le document explique la nature complémentaire des instructions techniques du BSI pour une utilisation sûre de l'identification par radiofréquence et de l'évaluation de l'impact sur la vie privée de la Commission européenne.

GRÈCE

A. Résumé des activités et actualités

En 2010, après deux années d'effort, une augmentation progressive du personnel sur une période de trois ans a été acceptée par une décision de l'adjoint au ministre des finances. L'effectif devrait augmenter de 25 personnes (19 juristes et experts en informatique, ainsi que 6 agents administratifs). Cette augmentation risque toutefois de ne jamais se concrétiser en raison de la situation actuelle des finances publiques. L'autorité hellénique de protection des données (AHPD) demeure en conséquence incapable de répondre rapidement aux nombreuses demandes introduites par les citoyens et les responsables du traitement des données.

Pour assurer son fonctionnement dans les circonstances actuelles, l'AHPD ne possède qu'une seule option réaliste, qui consiste à se concentrer sur deux objectifs principaux: l'action préventive et le traitement sélectif des plaintes et des demandes. En ce qui concerne le second objectif, la loi sur la protection des données a été modifiée (en son article 19, paragraphe 1) afin d'autoriser l'AHPD à établir des priorités pour le traitement des affaires en fonction de critères fondés sur l'importance et l'intérêt général de la question à traiter.

Pour ce qui est du premier objectif, l'AHPD a déclaré l'année 2010 «année de l'action préventive». L'autorité grecque de protection des données a publié une directive et en a préparé deux autres (publiées au début de l'année 2011). Elle a également formulé quatre avis sur de nouvelles propositions législatives ainsi que des décisions «pilotes» en réponse à des questions auxquelles sont confrontés les responsables du traitement données dans différents secteurs. Conformément à ses prérogatives, elle a également contrôlé les systèmes informatiques de plusieurs grands hôpitaux, afin de publier, dans un avenir proche, des lignes directrices sur les bonnes pratiques dans ce secteur.

Plus spécifiquement, l'AHPD a conseillé le gouvernement au moyen des avis et décisions suivants: l'avis 1/2010 (sur la publication sur l'internet, à des fins de transparence, d'actes administratifs contenant des données à caractère personnel), l'avis 2/2010 (sur l'utilisation de la télévision en circuit fermé pour la sécurité de l'État, aux fins de prévention et d'élucidation des délits), l'avis 4/2010 (sur la carte électronique, pour le stockage électronique des preuves d'achat à des fins fiscales), la décision 43/2010 (sur le recensement des salariés de l'État et sur le stockage des informations en question sur un site web gouvernemental) et la décision 56/2010 (sur l'ajout du numéro de sécurité sociale, et donc de la date de naissance, des médecins et pharmaciens sur les prescriptions), etc.

L'AHPD a également émis les avis et les décisions «pilotes» suivants: l'avis 3/2010 (sur l'encodage de ressortissants de pays tiers dans le système d'information Schengen et le registre national des étrangers indésirables), la décision 73/2010 (sur le droit d'accès du défendeur aux données d'identification du plaignant lorsqu'une plainte est déposée auprès d'une autorité publique) et, enfin, la directive 1/2010 concernant le traitement des données à caractère personnel à des fins de communication politique.

L'AHPD a organisé diverses activités à l'occasion de la Journée européenne de la protection des données. Un kiosque d'information a été installé devant les locaux de l'AHPD afin de sensibiliser le public à la protection des données et aux activités de l'autorité, de familiariser les citoyens à la consultation de son site web, de distribuer des supports didactiques et de diffuser plusieurs clips vidéo, y compris un clip issu de la campagne norvégienne *Du bestemmer* («C'est à toi de décider»). Deux brochures d'information ont été réalisées et distribuées, la première concernant les principes généraux de la protection des données, la seconde traitant des communications non sollicitées. Une affiche a également été préparée spécialement pour l'occasion et visait à attirer l'attention des citoyens sur des situations dans lesquelles ils sont invités à communiquer des données à caractère personnel. Enfin, l'AHPD a organisé une conférence de presse pour présenter certains problèmes majeurs en matière de protection des données à l'heure actuelle, comme les évolutions juridiques, les réseaux sociaux et les services de visualisation des rues.

Enfin, le ministre de la justice a créé, à la demande du parlement grec, un comité législatif chargé d'examiner la fusion potentielle des autorités indépendantes exerçant des compétences connexes, ainsi que l'amélioration de leur statut juridique, conformément à la loi 3051/2002.

Organisation	
Président et/ou collège	Christos Yeraris (président)
Budget	2 923 500 EUR
Personnel	Département des contrôleurs: 16 juristes 11 informaticiens (dont 7 sont en congé de maternité et 2 ont, dans le courant de l'année, été détachés auprès d'organismes européens en tant qu'experts nationaux); Département des communications et des relations publiques: 6 personnes (dont une démission, un détachement, ainsi que, pendant la moitié de l'année, un autre détachement et un congé de maternité); Département des ressources humaines et des finances: 17 personnes (dont un congé de maternité) et un détachement d'un autre service public.
Activités générales	
Décisions, avis, recommandations	
Notifications	L'AHPD a émis 11 décisions, 4 avis et 1 directive de portée générale concernant la protection des données.
Examens préalables	L'AHPD a examiné 759 notifications (430 en rapport avec l'installation et l'utilisation de caméras de surveillance et 73 en rapport avec des transferts de données vers des pays tiers).
Demandes émanant des personnes concernées	L'AHPD a accordé ou renouvelé 63 autorisations de traitement de données sensibles, d'interconnexions de fichiers et de transferts de données en dehors de l'UE.
Plaintes émanant des personnes concernées	1 507 (personnes concernées et responsables du traitement des données)
Conseils sollicités par le Parlement ou le gouvernement	674 (police et ministère public: 8, défense nationale: 1, administration publique, y compris locale: 32, fiscalité, y compris le ministère des finances: 6, santé: 17, sécurité sociale: 31, éducation et recherche: 12, banques: 45, secteur privé: 208, communications électroniques: 97, relations de travail: 45, moyens de communication de masse: 9)
Autres renseignements relatifs aux activités générales	7 (avis 1/2010, avis 2/2010, avis 3/2010, avis 4/2010, décision 43/2010, décision 56/2010 et décision 19/2010)
Activités d'inspection	
Contrôles, enquêtes	
Activités de sanction	
Sanctions	11 contrôles dans le secteur de la santé, 1 dans un organisme/fonds de sécurité sociale.
Amendes	

DPD	
Chiffres relatifs aux DPD	8 sanctions (1 avertissement, 7 amendes) imposées par la DPA dans les secteurs suivants: soins de santé (1), assurances (2), banques (1), secteur privé (2), moyens de communication de masse (2).

B. Informations sur la jurisprudence

Directive 1/2010

L'AHPD a défini les règles relatives au traitement licite de données à caractère personnel à des fins de communication politique. Elle a fourni des orientations sur les sources licites de collecte de données et sur les moyens (postaux/électroniques) employés pour la communication politique.

Avis 1/2010

L'AHPD a rendu un avis sur un avant-projet de loi relatif à la publication obligatoire sur l'internet d'actes administratifs contenant des données à caractère personnel. L'autorité chargée de la protection des données a demandé la mise en place d'une limitation du temps de publication en ligne de tels actes et des mesures techniques visant à prévenir toute utilisation de ces données à des fins autres que celles prévues. Enfin, elle a estimé que les actes contenant des données sensibles ne devaient pas être mis en ligne.

Avis 2/2010

L'AHPD, dans l'esprit de son avis 1/2009, a formulé certaines propositions pour la mise en œuvre de systèmes de vidéosurveillance (télévision en circuit fermé) dans les lieux publics dans un objectif de sécurité nationale, de prévention et d'élucidation des infractions pénales, ainsi que de surveillance de la circulation. Les propositions de l'AHPD ont été principalement adoptées dans l'article 14 de la loi 3917/2011. Un décret présidentiel précisera les critères et garanties à respecter dans le cadre de l'utilisation de systèmes de vidéosurveillance aux fins mentionnées ci-dessus. L'AHPD participe à la préparation de ce décret. Entre-temps, au début de l'année 2011, l'AHPD a publié la directive 1/2011 relative à l'utilisation de systèmes de vidéosurveillance aux fins de protection des personnes et des biens.

Avis 3/2010

Chaque année, l'AHPD reçoit de nombreuses plaintes émanant d'étrangers souhaitant que leurs données inscrites dans le système d'information Schengen (SIS) et dans le registre national des étrangers indésirables (NRUA) soient supprimées, en vertu de l'article 96 de la convention d'application de l'Accord de Schengen. C'est la raison pour laquelle l'AHPD a publié l'avis 3/2010, au terme d'un échange de vues avec le ministère de la protection des citoyens.

Avis 4/2010

Un avis a été rendu sur la mise en place d'un système facultatif d'enregistrement des pièces justificatives d'achat des contribuables, afin d'épargner à ces derniers la lourde tâche de devoir conserver ces reçus pour des raisons fiscales, tout en vérifiant le respect des obligations fiscales des entreprises. Ce système repose sur une nouvelle carte magnétique utilisant les terminaux de points de vente existants employés pour les transactions par cartes de débit et de crédit. L'AHPD a demandé que ce traitement reçoive une base juridique claire confirmant le caractère facultatif de l'utilisation de ce système par les contribuables et prévoyant des règles détaillées en matière de traitement des données, de manière à garantir une sécurité juridique. De plus, elle a souligné la nécessité de

s'assurer, par des mesures de sécurité adaptées, que les banques, en tant que responsables du traitement des données, ne puissent pas utiliser ces données à leurs propres fins.

Décision 7/2010

L'AHPD a rejeté une demande de l'association grecque des entreprises de location de véhicules de créer une liste noire des clients insolvables, dans la mesure où a) le risque financier n'est pas suffisamment élevé pour menacer ce secteur particulier, b) les dommages financiers dont souffrent les petites entreprises en conséquence des vols de véhicules non assurés sont leur propre choix commercial et c) l'association n'avait pas réfléchi à une solution plus respectueuse de la vie privée.

Décision 8/2010

L'AHPD a jugé illicite la publication de données sensibles liées à une affaires pénale dans l'édition électronique d'un journal, dans la mesure où la partie requérante n'était pas une personnalité publique. Elle a donc condamné le responsable du traitement des données au paiement d'une amende et a interdit toute publication ultérieure de l'article mis en cause dans l'édition imprimée du quotidien. Elle a également ordonné que l'article déjà téléchargé soit rendu anonyme et a recommandé des mesures afin de prévenir de telles infractions à l'avenir.

Décision 31/2010

L'AHPD s'est intéressée au système biométrique de contrôle appelé à être mis en place dans certaines infrastructures critiques de l'aéroport international de Thessalonique «Macédoine» dans le cadre d'un projet de recherche visant à développer une technique biométrique respectueuse de la vie privée basée sur les empreintes digitales. L'AHPD a déclaré le système conforme à la loi 2472/1997, moyennant le respect des deux conditions suivantes: le développement par le responsable d'une politique de sécurité pour le traitement des données et la notification à l'AHPD de la suppression des données au terme d'une période d'un an, soit le temps nécessaire à l'accomplissement des opérations justifiant la collecte de ces données. La conservation des données biométriques brutes dans une base de données centrale a été interdite.

Décision 43/2010

L'AHPD a examiné, à la fois dans le cadre de l'exercice de ses prérogatives et en réponse à des plaintes, le processus de recensement des salariés de l'État, introduit en juillet 2010 par un décret ministériel. Elle a jugé que cette base juridique permettait le traitement à des seules fins salariales et que toute autre donnée non nécessaire à ces finalités ne devait pas être traitée. En matière de sécurité, l'AHPD a demandé à ce que des mesures concrètes soient adoptées concernant le processus d'authentification et la protection des données contre les accès non autorisés.

Décision 56/2010

L'AHPD a conclu que la disposition légale imposant, aux fins de maîtrise des dépenses de santé publique, la mention du numéro de sécurité sociale des médecins et des pharmaciens sur chaque prescription de manière à permettre une identification unique, était conforme au principe constitutionnel de proportionnalité. Même si la date de naissance fait partie du numéro de sécurité sociale, cela ne constitue pas une atteinte grave à la vie privée des médecins et des pharmaciens, puisque l'âge n'est révélé qu'à un nombre limité d'utilisateurs dans des circonstances précises bien décrites par la loi. L'AHPD a toutefois recommandé que l'État conçoive un numéro de sécurité sociale qui ne révèle pas directement des données à caractère personnel.

Décision 73/2010

L'AHPD a estimé que le défendeur avait le droit d'accéder non seulement au contenu même de la plainte introduite auprès d'une autorité publique, mais aussi à tous les détails relatifs à l'origine de ces données, y compris les données

d'identification du demandeur. Ce droit peut être limité si un tel accès menace l'enquête menée par l'autorité, si le document contient des informations soumises à des obligations de secret particulières ou des données relatives à la vie privée ou familiale d'un tiers, ou encore si la divulgation de ces informations risque de mettre en danger la vie du demandeur. Le demandeur doit être correctement informé lors du dépôt de sa plainte et doit être invité à justifier par écrit ses objections à l'encontre de toute divulgation.

HONGRIE

A. Résumé des activités et actualités

Au cours de la procédure de révision de la Constitution, les propositions du commissaire à la protection des données ont été transférées au comité ad hoc responsable de la préparation de la nouvelle loi fondamentale. D'après l'avis du commissaire: 1) au lieu d'un commissaire à la protection des données, il serait préférable de désigner un commissaire à l'information; un règlement durable en tant que solution efficace impliquerait de confier à l'organisme responsable du contrôle de la protection des données le contrôle de la législation relative à la liberté d'information; 2) la modification de la législation devrait se solder par une meilleure indépendance de l'institution; et 3) un commissaire à l'information responsable de deux types de droits en matière d'information devrait posséder des instruments lui permettant réellement de veiller au respect de la législation.

Les activités de sensibilisation menées par le commissaire à la protection des données ont suivi la voie des réussites des années précédentes et bon nombre d'événements à visée informative ont été organisés. La conférence sur la protection des données qui s'est déroulée à l'occasion de la Journée de la protection des données était consacrée à l'analyse des problèmes liés aux systèmes de surveillance, au développement des technologies de surveillance, à la réponse fournie par la législation à ces évolutions, à la question de l'efficacité de ces systèmes en tant qu'outils d'application de la loi et si l'on peut estimer qu'il s'agit de moyens proportionnés étant donné les finalités prévues.

La conférence internationale organisée le 28 septembre était consacrée à l'équilibre entre la protection des données et la liberté d'information.

En 2009 a débuté l'élaboration d'une publication avec les DPA polonaise et tchèque, portant sur des thèmes liés à la protection des données dans le monde du travail et de l'entreprise dans les trois pays. Cette publication, censée paraître en 2011, doit aborder les législations nationales et de l'UE pertinentes, recenser les bonnes pratiques en vigueur au niveau national et contenir des recommandations.

Organisation	
Président et/ou collège	Dr András Jóri Commissaire parlementaire à la protection des données et à la liberté d'information
Budget	374 109 000 HUF
Personnel	48
Activités générales	
Décisions, avis, recommandations	Statistiques non disponibles
Notifications	15 161
Examens préalables	s. o.
Demandes émanant des personnes concernées	Ces deux catégories ensemble: 2 013
Plaintes émanant des personnes	

concernées	
Conseils sollicités par le Parlement ou le gouvernement	639
Autres renseignements relatifs aux activités générales	Consultations: 1 035
Activités d'inspection	
Contrôles, enquêtes	Statistiques non disponibles
Activités de sanction	
Sanctions	s. o.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Le commissaire à la protection des données a lancé avec volontarisme plusieurs projets, tous conformes à la directive 95/46/CE, répondant aux questions les plus pertinentes.

Un projet de recherche exhaustif s'est soldé par une recommandation au sujet du traitement des données dans la presse et les médias. Ce projet a permis d'analyser les règles en vigueur et la pratique, ainsi que d'identifier les domaines de protection de la vie privée et des données à caractère personnel dans la presse et dans les médias, notamment: l'analyse des relations entre les droits personnels protégeant les données à caractère personnel et la vie privée; les contenus comprenant des données à caractère personnel dans les informations présentées dans les médias, la source des données, l'autorisation légale, l'obligation d'informer les personnes concernées et de limiter les finalités; les pratiques en matière de consentement accordé dans le cadre d'apparitions dans les médias, plaintes et réforme de la législation; les effets des règles relatives au journalisme d'investigation sur les règles relatives à la protection des données; et la réglementation du journalisme judiciaire.

Un autre projet a porté sur l''analyse des répercussions sociales, des avantages et des inconvénients du recours à la vidéosurveillance. Le but était de trouver des solutions et des arguments clairs et pratiques susceptibles d'apporter une contribution concrète au débat. La vidéosurveillance s'accommode mal du cadre juridique en vigueur et sa conformité à la loi est souvent faible, ce qui nuit à la protection des données. L'objectif poursuivi était de mettre à jour la précédente recommandation en la matière.

Pour accompagner l'intensification des efforts déployés par le législateur en vue d'instaurer un système de renseignements commerciaux et dans la foulée de la publication de plusieurs avis par le commissaire déplorant l'absence de garanties suffisantes quant à la nature volontaire du consentement des débiteurs, un projet a été initié afin d'étudier la manière dont ces garanties pourraient être apportées.

Des représentants de Google ont entamé des discussions avec nos services sur les exigences nécessaires en matière de protection des données pour le lancement en Hongrie du service Google Street View. Au cours de l'enquête, le commissaire a demandé à Google de suspendre les prises de vue jusqu'à ce que la base juridique soit clarifiée. Il avait déjà été préalablement établi que, conformément à la loi sur la protection des données et à la loi sur le code civil, photographier des lieux publics n'était pas illégal. Des critères précis devaient être énoncés avant que Google

puisse entamer ses activités. Les opinions européennes dans ce domaine ont été prises en considération dans les discussions et dans l'avis préliminaire du commissaire. La décision finale qui sera émise reposera sur les réponses de Google aux questions du commissaire et sur les résultats de l'enquête menée en 2011.

L'utilisation de technologies modernes répandues a donné lieu à des enquêtes du commissaire dans de nombreux secteurs. Dans le secteur de l'emploi, les tendances demeurent identiques: on utilise des systèmes de vidéosurveillance et les employeurs font souvent appel à la géolocalisation, à des détecteurs de mensonge et à d'autres outils. Ils vérifient les boîtes aux lettres et certains exigent même de passer des examens médicaux. Dans ce contexte stable, un nombre incalculable de plaintes a montré que le secteur de l'emploi avait besoin d'une régulation plus exhaustive, détaillée et conceptuelle.

Des atteintes à la vie privée ont aussi été constatées dans le secteur éducatif. Des établissements d'enseignement ont mis en place des systèmes d'inscription à l'aide de techniques d'accès facile utilisées de façon inadaptées. Le commissaire a observé que les caméras de surveillance et l'identification biométrique étaient les exemples les plus répandus de non-respect par ces établissements du principe de proportionnalité et de la limitation des finalités. Dans une affaire portant sur des examens internationaux, les candidats devaient, avant de pouvoir passer l'examen, fournir, outre leurs documents d'identité, leurs empreintes digitales et leur signature numérisée, sous peine d'être exclus de l'examen. Dans ce dernier cas, le principal nœud du problème était la nature volontaire et «libre» du consentement.

Enfin, une autre affaire a concerné le secteur des télécommunications: des photographies et des données d'identification (souvent des noms, des numéros de téléphone, etc.) avaient été téléchargées sur un réseau social, accompagnées de déclarations et de références grossières au sujet du demandeur. Puisque des données à caractère personnel étaient manifestement impliquées, le traitement de ces informations n'aurait pu être licite que moyennant le consentement de la personne concernée. Dans ce cas, le consentement a été jugé manquant et le commissaire a déposé une plainte auprès de la police (pour détournement de données à caractère personnel). La police a lancé une enquête, mais l'ensemble du contenu litigieux a été supprimé du portail hongrois et téléchargé sur d'autres sites de partage de fichiers dans des pays situés au delà de sa juridiction.

IRLANDE

A. Résumé des activités et actualités

En 2010, les services du commissaire à la protection des données ont ouvert 783 dossiers à partir de plaintes officielles. (De nombreuses plaintes sont traitées de façon informelle en transmettant aux demandeurs des informations pertinentes sur leurs droits.) Comme les années précédentes, une grande majorité de plaintes ont été réglées à l'amiable, seules 14 d'entre elles ayant donné lieu à des décisions formelles. La section B du présent rapport revient sur les poursuites effectuées en 2010. Le nombre de notifications de cas d'atteintes à la sécurité de données à caractère personnel reçues par le bureau du commissaire a fortement augmenté, principalement en raison de l'introduction, en juillet 2010, d'un nouveau code de bonnes pratiques en matière d'atteintes à la sécurité des données à caractère personnel. Le commissaire a poursuivi ses contacts avec d'importantes organisations du secteur public afin de déterminer l'ampleur du partage des données dans le secteur public. Sur la base de ces contacts et du contrôle de plusieurs entités du secteur public, le commissaire a convenu d'un ensemble de lignes directrices pour toutes les organisations du secteur public, dont les principes moteurs sont la transparence et la proportionnalité. Parmi les autres lignes directrices publiées, citons les versions révisées des lignes directrices en cas d'atteintes à la sécurité des données à caractère personnel et des lignes directrices sur la sécurité des données, ainsi que de nouvelles lignes directrices relatives aux enquêtes sur les salariés.

Organisation	Services du commissaire à la protection des données
Président et/ou collège	Billy Hawkes
Budget	1 272 000 EUR (1 449 329 EUR dépensés)
Personnel	22
Activités générales	
Décisions, avis, recommandations	3 (lignes directrices)
Notifications	Environ 5 000 inscriptions en 2010
Examens préalables	s. o.
Demandes émanant des personnes concernées	7 200
Plaintes émanant des personnes concernées	783 (droits d'accès: 39 %; marketing direct électronique: 30 %; divulgation: 10 %; traitement déloyal: 10 %; autres: 11 %)
Conseils sollicités par le Parlement ou le gouvernement	54
Autres renseignements relatifs aux activités générales	410 notifications d'atteintes à la sécurité des données à caractère personnel provenant de 123 organisations différentes
Activités d'inspection	
Contrôles, enquêtes	32 audits (contrôles)

Activités de sanction	
Sanctions	8 sociétés et particuliers ont été poursuivis en 2010.
Amendes	11 050 EUR + frais (amendes/transactions infligées par les tribunaux).
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Dans la majorité des cas, conformément à la section 10 des lois irlandaises de 1988 et de 2003 sur la protection des données, les plaintes transmises au commissaire sont réglées à l'amiable sans recours à une décision formelle ou à des mesures coercitives. Lors d'un règlement à l'amiable, il se peut, par exemple, que le responsable du traitement des données doive verser une contribution financière à la personne concernée ou à un organisme caritatif. Si nécessaire, il est recouru à l'autorité, notamment lorsque les responsables du traitement des données ne respectent pas les droits d'accès des personnes concernées. Il arrive que les responsables du traitement des données soient cités dans des études de cas incluses dans le rapport annuel du commissaire. Dans le courant de l'année 2010, le commissaire a entamé avec succès plusieurs actions en justice en rapport avec les droits conférés aux personnes concernées par les lois de 1998 et de 2003 sur la protection des données et le décret-loi 535 de 2003 (transposition de la directive 2002/58/CE en Irlande). En 2010, sept sociétés ont été poursuivies pour diverses infractions et, pour la première fois, les services du commissaire ont poursuivi deux particuliers (dont l'un a été condamné). Ces poursuites avaient été engagées pour des SMS non sollicités à des fins de marketing.

C. Autres informations importantes

Toujours en 2010, le commissaire a mené une enquête approfondie sur une base de données des demandes d'indemnisation partagée au sein du secteur des assurances, appelée *Insurance Link*. À l'époque de l'enquête, cette base de données contenait des renseignements relatifs à plus de 2,5 millions de sinistres. Le rapport de l'enquête a signalé un manque de transparence, des contrôles inadéquats de l'accès aux données et l'existence d'accès inadaptés à répétition.

ITALIE

A. Résumé des activités et actualités

En 2010, les principaux domaines d'activité de l'autorité italienne de protection des données (la «Garante») ont été les suivants:

- les soins de santé (dossiers et fichiers de santé électroniques, résultats d'examens en ligne, encodage et collecte des données d'examen dans les pharmacies, recherches scientifiques et pharmacologiques, projet de surveillance épidémiologique des soldats en Bosnie, collecte de données relatives au VIH dans les établissements de soins de santé, droits à la vie privée dans les hôpitaux et autres établissements de soins de santé et conservation des documents médicaux);
- l'administration publique (diffusion de données sur le patrimoine immobilier des entités publiques, transparence des subventions et des salaires octroyés par les administrations publiques, publication et diffusion en ligne par les organismes publics de données à caractère personnel, base de données sur la pédophilie, registre des sans-abri, mesures de sécurité pour l'anagrafe tributaria [le système d'information des services fiscaux] et interconnexion et sécurité des bases de données publiques);
- le marketing (appels téléphoniques non sollicités et registro delle opposizioni [registre des oppositions, ou opt-out] et pourriels, fax et courriels non sollicités);
- les communications électroniques (téléphones intelligents et tablettes, stockage des données téléphoniques et de l'internet à des fins judiciaires, recherches inverses, mesures de sécurité et établissement de profils clients);
- le journalisme et l'information (dossiers judiciaires mentionnés par la presse, protection des droits au respect de la vie privée des enfants et des victimes de violences, données sur la santé et sur l'activité sexuelle, adoption, photographies de personnes arrêtées par la police et archives en ligne des journaux);
- l'emploi (systèmes de détection reposant sur des données biométriques, systèmes de localisation des travailleurs, contrôle de l'usage de l'internet par les travailleurs et vidéosurveillance sur le lieu de travail);
- la police et la justice (données judiciaires liées aux activités de médiation visant à régler les litiges civils et commerciaux par la conciliation, procès civils numériques [e-justice], mesures de sécurité pour les fonctions judiciaires, nouveau système d'information pour la justice administrative, base de données informatiques «CED» du service de la sécurité publique de la police, données des dossiers des passagers aériens et mesures de sécurité pour la base de données Schengen);
- l'internet (moteurs de recherche, Google Street View, Google Buzz, Facebook et autres réseaux sociaux, conservation illégale de données relatives à l'usage de l'internet, forums et blogs, mesures de sécurité simplifiées pour les petits fournisseurs de services sur l'internet et profilage en ligne);
- nouvelles technologies (géolocalisation, techniques reposant sur l'identification par radiofréquence);
- les écoles et universités (anagrafe nazionale degli studenti [registre national des étudiants], utilisation de la vidéosurveillance dans les écoles, publication des notes et des résultats des examens, classements des élèves et données à caractère personnel utilisées pour les inscriptions à l'université);
- les organisations privées (tessera del tifoso [cartes de supporter de football], agences matrimoniales, abonnements de ski et copropriétés);
- les entreprises (transfert de données vers des pays tiers, données relatives à la sécurité sociale, agences de notation et surveillance des conflits d'intérêts, mesures simplifiées de protection des données et renseignements de nature commerciale); et
- les banques, institutions financières et compagnies d'assurance (accès aux données des clients détenues par les banques, mesures de sécurité, systèmes d'information sur les historiques de crédit, accès aux données des crédits à la consommation par les prêteurs de l'UE).

La DPA à participer à plusieurs **auditions parlementaires** sur des questions importantes relatives en particulier à la politique d'immigration, à l'*anagrafe tributaria* et à la simplification des relations entre l'administration publique et les citoyens.

L'autorité italienne de la protection des données a également adopté d'importantes **lignes directrices** concernant en particulier la divulgation d'informations relatives aux personnes morales, les règles devant être respectées par les organismes de l'administration publique lors de l'envoi par courrier de dossiers et documents administratifs contenant des données à caractère personnel («l'administration publique sur l'internet») et la détermination du degré de satisfaction des clients dans le secteur des soins de santé.

La DPA italienne a formulé des **décisions générales** dans certains domaines: la vidéosurveillance, la propagande électorale, les *tessera del tifoso* (cartes de supporter de football), le télémarketing, la transférabilité des numéros, les systèmes d'informations sur les crédits, les registres téléphoniques et les recherches inverses (c'est-à-dire la possibilité d'obtenir des informations sur un utilisateur à partir de son numéro de téléphone), l'utilisation des données dans le *pubblico registro automobilistico* (registre des données sur les véhicules) et les mesures de sécurité pour les données des clients conservées par les banques.

En matière de relations internationales et de coopération avec d'autres DPA, outre le travail effectué dans le contexte du groupe de travail «Article 29» et de ses sous-groupes thématiques (où la DPA italienne a été le rapporteur pour l'action commune de mise en application de la directive 2006/24/CE sur la conservation des données), la DPA italienne participe activement aux groupes de travail sur la protection des données à l'OCDE (groupe de travail sur la sécurité de l'information et la vie privée), ainsi qu'au Conseil de l'Europe (comité consultatif de la convention 108/1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, y compris son bureau, dont est membre la *Garante*).

La DPA italienne est également membre des autorités de contrôle communes et d'autres organismes de supervision multipartites reposant sur des instruments juridiques de l'Union européenne et qui ont mis en place des systèmes d'information communs (JSB Europol, Schengen, douanes, Eurodac).

La DPA assiste aux réunions du Groupe de travail international sur la protection des données dans les télécommunications (IWGDPT) et aux réunions de l'atelier de traitement des dossiers qui a lieu lors de la conférence printanière des autorités européennes chargées de la protection des données.

En matière de coopération judiciaire et policière, la DPA italienne a œuvré à la promotion et au respect de la protection des données dans le cadre du groupe de travail «Police et justice», dirigé par le président de la DPA, le professeur Pizzetti.

Comme à son habitude, la DPA a directement participé aux deux conférences (une européenne et une internationale) organisées cette année.

Dans la lignée de ses initiatives préalables, la DPA italienne s'est également concentrée sur des activités de sensibilisation, surtout adressées aux jeunes, notamment en diffusant des brochures sur les réseaux sociaux, dans les écoles et dans le secteur de la santé. Fidèle à ses objectifs, elle a aussi lancé un concours pour les étudiants de l'enseignement secondaire, intitulé «Vie privée 2.0. Les jeunes et les nouvelles technologies».

La DPA italienne est légalement tenue de soumettre un rapport annuel au Parlement sur le travail qu'elle a effectué. Le rapport annuel portant sur l'année 2010 était accompagné de deux documents de référence, l'un sur l'informatique en nuage et l'autre sur les téléphones intelligents et les tablettes, comprenant des lignes directrices et principes communs en matière de protection des données adaptés aux nouvelles évolutions techniques et partiellement inspirés de l'expérience et du savoir-faire de la DPA (voir point C ci-dessous).

Organisation	Autorité italienne de protection des données (*Garante per la protezione dei dati personali)*
Président et/ou collège	Président: P[f]. Francesco Pizzetti Collège: Giuseppe Chiaravalloti Mauro Paissan Giuseppe Fortunato
Budget	Environ 16 500 000 EUR
Personnel	118
Activités générales	
Décisions, avis, recommandations	Nombre de décisions prises par le collège: environ 600
Notifications	1 197
Examens préalables	Environ 10
Demandes émanant des personnes concernées	Nombre total de demandes: environ 4 000 Demandes d'informations (*quesiti*): 353 Dénonciations et plaintes (*segnalazioni* et *reclami*) reçues en 2010 des personnes concernées: 3 359
Plaintes émanant des personnes concernées	(Plaintes officielles réglementées spécifiquement par le code de protection des données à caractère personnel, concernant l'accès à ses propres données personnelles) environ 350
Conseils sollicités par le Parlement ou le gouvernement	Avis rendus en réponse à des demandes du Parlement: 4 Avis rendus aux ministères et au cabinet du premier ministre: 16 Sujets: police et sécurité publique: 4; activité judiciaire: 1; administration en ligne et bases de données: 5; éducation et formation: 2; emploi dans les organismes publics: 1; soins de santé: 1; entreprises: 1; bien-être: 1; et marketing (par téléphone): 1
Autres renseignements relatifs aux activités générales	En 2010, les services de première ligne de la DPA ont reçu plus de 26 000 appels téléphoniques et courriels, concernant essentiellement le démarchage par téléphone, les courriels et fax non sollicités, la vidéosurveillance, l'internet et les réseaux sociaux, ainsi que la protection de la vie privée sur le lieu de travail (à la fois dans le secteur public et dans le secteur privé). Autorisations nationales pour des règles d'entreprise contraignantes (BCR): 2
Activités d'inspection	

Contrôles, enquêtes	Nombre de contrôles et/ou d'enquêtes (sur place): environ 500 (dont 55 pour des infractions pénales, rapportées à l'autorité judiciaire compétente). Principaux sujets traités: défaut d'avis d'information, insuffisance des mesures de sécurité, défaut de produire les informations et/ou documents demandés par la DPA, notifications manquantes ou incomplètes à la DPA, violation d'une décision de la DPA, violation des dispositions sur la conservation des données, violations multiples par les responsables du traitement des données de bases de données à grande échelle ou comprenant des données sensibles.
Activités de sanction	
Sanctions	Environ 500
Amendes	Montant: environ 4 800 000 EUR imposés par la police financière chargée des contrôles au nom de la DPA.
DPD	
Chiffres relatifs aux DPD	s. o. (L'ordre juridique italien n'autorise pas le recours à des DPD.)

B. Informations sur la jurisprudence

Le **tribunal de Milan** a déclaré les directeurs de Google coupables d'avoir violé la section 167 (traitement illégal de données, y compris diffusion de données sensibles) du code de la vie privée (décret législatif nº 196 du 30 juin 2003). La violation consistait en la diffusion, sur un site web, d'une vidéo montrant le harcèlement d'un mineur handicapé par ses camarades de classe (décision du 24 février 2010).

Le **tribunal de Palerme** a établi la responsabilité d'une banque à l'égard de deux de ses clients pour l'exécution d'un transfert bancaire non autorisé vers un pays tiers par l'intermédiaire de ses services bancaires en ligne, dont les mesures de sécurité n'assuraient pas une protection adéquate. La décision repose principalement sur la section 15 du code de la vie privée disposant que toute personne causant un dommage à autrui en conséquence d'un traitement de données à caractère personnel est tenue de verser des dommages et intérêts, conformément à la section 2050 du code civil (responsabilité découlant de l'exercice d'activités de nature dangereuse) (décision du 20 décembre 2009).

Le **Conseil d'État** (**juridiction administrative suprême**) a jugé que le droit des personnes concernées à faire rectifier leurs données en vertu de la section 7 du code de la vie privée devait toujours être assuré, afin de conserver l'exactitude des données à caractère personnel enregistrées dans le *casellario giudiziale* (casier judiciaire) (décision nº 473/2010).

Le **Conseil d'État** a approuvé la demande d'accès d'un époux à des dossiers administratifs contenant des données sensibles sur la santé de l'autre époux en vue de l'annulation du mariage. En l'espèce, le droit à la vie privée des personnes concernées n'a pas été jugé supérieur à la demande du requérant, formulée dans le cadre d'une voie de recours juridique (l'annulation) légitime. La plus haute instance administrative du pays a donc confirmé la demande de divulgation de données sensibles relatives à la santé, conformément à la section 60 du code de la vie privée (décision nº 7166/2010).

La **Cour de cassation** a déclaré illégal le licenciement d'un salarié au motif que celui-ci avait été surpris à plusieurs reprises en train de surfer sur l'internet à des fins personnelles. En l'espèce, c'est un logiciel installé par l'employeur qui avait permis ces observations et qui permettait d'accéder aux données conservées sur les ordinateurs personnels utilisés par ses salariés. Conformément à la loi nº 300/1970 (loi sur les travailleurs ou *statuto dei lavoratori*), la cour

a formellement déclaré que: bien que nécessaire, «le contrôle des activités des salariés doit se limiter à une 'dimension humaine' et ne doit pas être exacerbé par le recours à des technologies entraînant la violation de toutes les formes de vie privée et d'autonomie dans l'accomplissement des obligations professionnelles». Les dispositifs informatiques qui «permettent de surveiller la 'navigation' sur l'internet sont des 'équipements visant à surveiller à distance' les travailleurs». Dès lors, le déploiement de tels systèmes «doit faire l'objet d'un accord avec les représentants syndicaux au sein de l'entreprise ou, dans le cas où un tel accord n'existerait pas, d'une autorisation de l'inspection du travail (section 4.2 de la loi sur les travailleurs)». Les données obtenues en violation de cette disposition ne peuvent dès lors pas être invoquées devant la justice (décision nº 4375/2010).

Dans une autre affaire relative à la légitimité d'un licenciement, la **Cour de cassation** a jugé que le respect du droit à la vie privée ne pouvait en soi empêcher l'exercice d'autres droits fondamentaux, tels que le droit à la défense ou le droit de travailler. Dans de tels cas, il devient vital d'établir le bon équilibre entre les différents droits en jeu (décision nº 18279/2010).

C. Autres informations importantes

La DPA a ouvert une enquête sur les principaux fabricants de systèmes d'exploitation pour **téléphones intelligents**, afin de vérifier l'adéquation des mesures de sécurité concernant les applications mobiles développées pour ces systèmes. Les réponses reçues jusqu'à présent ont montré que les politiques de sécurité adoptées divergeaient à de nombreux égards. Les principaux aspects soulignés par cette enquête ont été décrits dans un document intitulé «Téléphones intelligents et tablettes: le scénario actuel et les perspectives d'exploitation», qui se trouve en annexe du rapport annuel d'activités de 2010 de la DPA italienne.

Avec sa brochure *L'informatique en nuage: lignes directrices pour un usage réfléchi de ces services*, la DPA italienne a proposé des orientations élémentaires pour les utilisateurs de services d'informatique en nuage (par exemple, le besoin d'une évaluation préalable fondée sur les risques, tenant compte notamment de la fiabilité du fournisseur envisagé, et une vérification des clauses contractuelles spécifiques, notamment la localisation du serveur, le type de services offerts et la formation du personnel réalisant le traitement des données) afin d'encourager une utilisation réfléchie de ces services et de fournir à l'avenir des règles précises concernant les mesures de sécurité.

Vidéosurveillance: ce sujet a récemment été abordé dans le cadre d'une **décision générale** en date du 27 avril 2010, qui s'applique aux entités publiques comme privées dans le cadre de l'installation de systèmes de vidéosurveillance, notamment de télévision en circuit fermé. Les règles stipulées dans cette décision générale procurent des garanties particulières en faveur de la vie privée des individus dont les données sont collectées et traitées par l'intermédiaire de tels systèmes. Cette décision en remplace une autre formulée par la DPA en 2004, afin de prendre en compte non seulement la législation ultérieure, mais aussi les nouvelles technologies et l'augmentation substantielle de l'emploi de la vidéosurveillance à des fins diverses. Une attention particulière a été consacrée aux mesures visant à informer les personnes concernées que des caméras de surveillance fonctionnent dans les locaux/zones auxquels elles sont sur le point d'accéder (obligation de fournir des avis d'information spécifiques, sauf dans le cas de caméras de surveillance utilisées pour des raisons de sécurité publique), de même qu'aux limites en matière de conservation des données collectées par ces caméras et par les systèmes de vidéosurveillance. (Les images, lorsqu'elles sont enregistrées, ne peuvent être conservées que durant une période limitée qui ne doit pas excéder 24 heures. Une conservation plus longue peut être envisagée dans des cas particuliers, tels que pour la police et les enquêtes judiciaires, la sécurité des banques, etc).

LETTONIE

A. Résumé des activités et actualités

Les modifications de 2010 à la loi sur la protection des données à caractère personnel ont été adoptées par le Parlement de la République de Lettonie le 6 mai 2011 (en vigueur depuis le 2 juin 2010). Plus précisément, l'article 10, chapitre 4, de la loi sur la protection des données à caractère personnel a été modifié et détermine désormais les cas dans lesquels le traitement des données à caractère personnel est, à titre d'exception, autorisé à des fins autres que celles initialement prévues dans les affaires pénales. Une autre modification majeure est celle liée aux décisions de l'Inspection nationale des données (article 31, chapitre 2): défier ou faire appel contre les actes administratifs émis par l'Inspection nationale des données en matière de blocage du traitement des données à caractère personnel ou d'interdiction permanente ou temporaire de traiter des données, ne suspend pas l'application de la décision de l'Inspection nationale des données (à moins d'une suspension décidée par l'examinateur de l'appel).

Au niveau national, l'Inspection nationale des données de Lettonie a exprimé son avis sur divers actes législatifs et initiatives politiques, dont les principaux sont décrits ci-dessous.

- Le projet de loi sur le registre des crédits: cet avis a été émis à l'intention de la Banque nationale de Lettonie au sujet du droit des personnes concernées d'accéder à ce registre. Au départ, il y avait en effet une restriction à ces droits contraire à la loi sur la protection des données à caractère personnel. L'avis de l'Inspection nationale des données a été pris en considération.
- Le projet de loi sur le recouvrement des créances: après un avis rendu par l'Inspection nationale des données, il a été décidé qu'aucun renseignement à caractère personnel ne pouvait être inclus dans une base de données de solvabilité dans le cas où la personne concernée n'avait pas reconnu la dette.
- Le projet de loi modificative de la loi sur la protection des droits du consommateur: l'avis de l'Inspection nationale des données a été pris en considération. Celle-ci avait critiqué le fait que les modifications proposées ne tenaient pas compte des restrictions imposées par la directive 2008/48/CE en matière de demandes de crédit en ce qui concerne le montant du crédit et les conditions dans lesquelles il n'est pas nécessaire de vérifier la solvabilité d'un client.
- L'Inspection nationale des données de Lettonie n'a pas pris part aux projets nationaux visant la mise en place d'une politique de services de santé en ligne. Cependant, en 2010, elle a mené un contrôle au sein du secteur de la santé sur le traitement des données à caractère personnel sensibles. Ces contrôles devaient se poursuivre en 2011.

Principales questions au sujet desquelles les pouvoirs publics ont consulté la DPA

L'Inspection nationale des données ne possède pas de statistiques sur les demandes de conseils formulées par les pouvoirs publics. Toutefois, elle reçoit quotidiennement des appels de différentes autorités publiques au sujet de problématiques variées liées au traitement des données à caractère personnel, notamment sur la nécessité d'informer d'un tel traitement, ainsi que d'autres questions plus complexes requérant une analyse exhaustive pour identifier la meilleure solution de protection des données à caractère personnel.

Informations sur les activités de sensibilisation

L'Inspection nationale des données a organisé plusieurs séminaires sur des sujets touchant à la protection des données, destinés à des publics cibles différents, par exemple des directeurs d'établissements d'enseignement, des instituteurs, etc. L'inspection propose des séminaires ouverts à toutes les personnes intéressées. (Trois séminaires de ce type se sont déroulés en 2010..

Organisation	Inspection nationale des données de Lettonie (*Datu valsts inspekcija*)

Président et/ou collège	Directeur: Signe Plūmiņa
Budget	266 907 LVL (environ 370 457 EUR)
Personnel	19 personnes (y compris le personnel administratif et de maintenance)
Activités générales	
Décisions, avis, recommandations	En ce qui concerne les statistiques sur les décisions et avis: s. o. En ce qui concerne la recommandation: la recommandation a été diffusée sur les réseaux sociaux. (Elle visait leurs utilisateurs.)
Notifications	352 (y compris les notifications de modifications apportées à des opérations de traitement déjà notifiées)
Examens préalables	267
Demandes émanant des personnes concernées	s. o.
Plaintes émanant des personnes concernées	234 plaintes reçues de personnes concernées au sujet d'une atteinte possible à la protection des données à caractère personnel 2 plaintes de personnes concernées originaires de pays tiers relatives au traitement de leurs données à caractère personnel au sein du SIS 22 plaintes liées aux pourriels (15 enquêtes exécutées)
Conseils sollicités par le Parlement ou le gouvernement	9 (concernant la modification de la loi sur la protection des données à caractère personnel et le projet de loi sur la sécurité informatique)
Autres renseignements relatifs aux activités générales	Lors des consultations téléphoniques, les principales questions posées étaient les suivantes: certaines informations sont-elles considérées comme des données à caractère personnel? qui peut exercer une vidéosurveillance, quand et où? comment peut-on lutter contre le traitement illégal des données à caractère personnel sur l'internet? *quid* du traitement des données à caractère personnel dans le cadre du recouvrement des créances? quand est-on autorisé à traiter des numéros personnels et qui y est autorisé?
Activités d'inspection	
Contrôles, enquêtes	234 plaintes. La plupart des personnes qui ont contacté l'Inspection nationale des données de Lettonie ont signalé une possible violation de la loi sur la protection des données à caractère personnel dans les domaines suivants: le traitement sur l'internet de données à caractère personnel (également dans des situations où le responsable n'avait pas prévu les moyens

	techniques appropriés pour la protection des données); le traitement de données à caractère personnel pour recouvrer des créances et dresser l'historique des crédits; le vol d'identité, lorsque sont transmises des données à caractère personnel appartenant à autrui et qu'il en résulte donc un traitement illégal des données (de nombreux cas concernant des données à caractère personnel erronées envoyées à la police nationale ou locale concernant plusieurs infractions administratives); les opérations de traitement des données menées par des sociétés d'entretien domestique; et la vidéosurveillance.
Activités de sanction	
Sanctions	L'Inspection nationale des données puise son pouvoir de sanction dans le code letton des infractions administratives. Dans 42 affaires, des violations de la loi sur la protection des données à caractère personnel ont été constatées et des amendes administratives ont été imposées. Toutes les enquêtes initiées en 2010 n'ont pas été clôturées.
Amendes	Montants (indiquer si ce sont les tribunaux ou les DPA qui ont imposé ces amendes). Amendes imposées par l'Inspection nationale des données: 28 avertissements, 14 amendes pour un montant total de 14 250 LVL (environ 19 249 EUR).
DPD	
Chiffres relatifs aux DPD	9 délégués à la protection des données enregistrées. 4 examens organisés pour les délégués à la protection des données.

B. Informations sur la jurisprudence

En 2010, le nombre de cas de violation de la loi sur la protection des données à caractère personnel a augmenté. Les sanctions pour de telles violations sont prévues par le droit pénal. Ces affaires ont donc été transférées aux services du procureur général.

L'Inspection nationale des données plaide pour une meilleure coopération à l'échelle de l'UE, de manière à lutter plus efficacement contre les atteintes à la protection des données sur l'internet et à veiller ainsi au respect des droits des citoyens de l'UE en matière de protection des données.

LITHUANIE

A. Résumé des activités et actualités

La loi du 12 mai 2011 modifiant et complétant la loi sur la protection juridique des données à caractère personnel (journal officiel, 1996, nº 63-1479, et 2008, nº 22-804) entrera en vigueur le 1er septembre 2011. En matière d'acception du risque et de solvabilité, la nouvelle version de la loi sur la protection juridique des données à caractère personnel (ci-après LPJDP) dispose que les institutions financières qui proposent des services financiers peuvent partager entre elles, aux fins de l'analyse du risque financier et de la gestion des créances, des données à caractère personnel relatives à l'état civil, à l'emploi et à l'éducation des personnes concernées auxquelles ces institutions fournissent ou prévoient de fournir des services financiers, à la condition que les personnes concernées aient donné leur consentement. Par ailleurs, la loi dispose dorénavant que des données à caractère personnel peuvent être traitées dans le cadre d'enquêtes publiques et sociales moyennant le consentement de la personne concernée.

La loi sur la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, mettant en œuvre la décision-cadre 2008/977/JAI du Conseil, a été adoptée le 21 avril 2011 et devait entrer en vigueur le 1er juillet 2011.

Le 27 novembre 2010, une nouvelle version de la loi du gouvernement de la République de Lituanie est entrée en vigueur. Sa nouvelle formulation précise des changements relatifs au statut juridique du directeur de l'Inspection publique de protection des données de la République de Lituanie (ci-après IPPD). Il y est indiqué que le directeur de l'IPPD deviendra un fonctionnaire de l'État. D'après cette même nouvelle version de la loi, l'IPPD devra opérer conformément au plan stratégique approuvé par le ministère de la justice. Elle précise également que le ministre de la justice donnera au gouvernement la possibilité de désigner ou de révoquer le directeur de l'IPPD, de le promouvoir et de lui imposer des sanctions. De plus, le ministre de la justice est compétent pour décider des vacances du directeur, et pour l'envoyer en mission. En vertu de cette loi, le directeur de l'IPPD est responsable devant le gouvernement et le ministère de la justice et doit leur rendre des comptes.

Le 23 décembre 2009, le gouvernement de la République de Lituanie a adopté une résolution sur la décision 2009/371/JAI portant création de l'Office européen de police (Europol). Aux termes de l'article 3 de cette résolution, l'IPPD a été désignée comme autorité de contrôle pour mener les tâches de mise en œuvre de l'article 33 de la décision 2009/371/JAI du Conseil (entrée en vigueur le 1er janvier 2010).

La Journée européenne de la protection des données a été fêtée le 28 janvier 2010. Une réunion s'est déroulée au Bureau d'information européen du Seimas. Cet événement a été consacré aux diverses institutions, agences et organismes nationaux menant des activités en rapport avec la protection des données à caractère personnel. Des représentants du secteur public ont été informés des problèmes actuels en matière de protection des données à caractère personnel en Lituanie et dans d'autres pays. Une grande attention a été accordée à la vidéosurveillance. Trois rapports ont été présentés à ce sujet: «Réglementation juridique de la vidéosurveillance», «Questions techniques sur la vidéosurveillance» et «Les problèmes relatifs à la vidéosurveillance dans la capitale Vilnius: le présent et le passé».

Le 26 mai 2010, l'IPPD, en collaboration avec la société Expozona, a tenu une conférence intitulée «La protection des données dans les technologies les plus récentes et dans l'espace électronique». L'événement était axé sur la gestion de l'identité, la protection des données et de la vie privée dans les technologies de l'information et de la communication, ainsi que sur la mobilité. Ces sujets couvraient les principaux thèmes analysés durant les quatre conférences du projet PrivacyOS (*Privacy Open Space*). Le projet PrivacyOS réunit l'industrie, les PME, les pouvoirs publics, le monde académique et la société civile, dans le but de stimuler le développement et le déploiement d'infrastructures pour le respect de la vie privée en Europe. Plus de soixante représentants des secteurs privé et public ont assisté à la conférence.

Le 24 novembre 2010, l'IPPD et la société Expozona ont organisé une autre conférence intitulée «Les données à caractère personnel sont-elles traitées en toute légalité en Lituanie? Les problèmes, leurs causes et des façons de les résoudre». Cette conférence s'adressait aux directeurs des entreprises, institutions et organisations, aux juristes et aux professionnels responsables du traitement des données à caractère personnel des salariés et des clients. Les

intervenants de l'IPPD et du cabinet d'avocats LAWIN Lideika, Petrauskas, Valiūnas et associés ont livré six exposés sur divers sujets: «Que faut-il savoir pour traiter licitement des données à caractère personnel?», «Le traitement des données à caractère personnel des salariés, problèmes et solutions», «Pratiques d'examen des plaintes. Décisions de justice importantes en matière de protection des données», «Transfert licite de données à caractère personnel à des destinataires de données dans des pays tiers», «Pratiques en matière de traitement des données à caractère personnel appartenant à des catégories particulières en Lituanie et dans l'Union européenne» et «Questions d'actualité sur la protection des données à caractère personnel en Lituanie et en Europe».

Organisation	
Président et/ou collège	Dr Algirdas Kunčinas
Budget	Budget alloué et exécuté de 1 886 000 000 LTL
Personnel	30
Activités générales	
Décisions, avis, recommandations	Recommandation sur «l'application du droit d'un individu au respect de la vie privée et des principes de protection des données pour les moyens concernés d'identification par radiofréquence»
Notifications	760 (sur le traitement des données)
Examens préalables	204
Demandes émanant des personnes concernées	8
Plaintes émanant des personnes concernées	270
Conseils sollicités par le Parlement ou le gouvernement	1
Autres renseignements relatifs aux activités générales	3 294 consultations, 102 communiqués d'information au public, 7 résumés des résultats des enquêtes ouvertes à la suite de plaintes et sur la jurisprudence, 6 demandes liées au traitement des données dans le système central d'information Schengen, 86 conclusions sur des documents de l'UE et du Conseil de l'Europe, 92 réponses à des demandes de parties à la Convention (STE nº 108), 238 actes juridiques coordonnés et documents des responsables des données, 5 actes juridiques préparés
Activités d'inspection	
Contrôles, enquêtes	80 (légitimité du traitement des données et degré de latitude des utilisateurs des sites de réseaux sociaux, légitimité du traitement des données lors de la prestation de services rapides de crédit, légitimité du stockage des données relatives au trafic sur l'internet lors de prestations de services internet, portée et la légitimité de la publication de données à caractère personnel sur le site web des municipalités et légitimité du traitement des données à caractère personnel d'un client dans les clubs de sport privés)

Activités de sanction	
Sanctions	L'IPPD a rédigé 41 constats d'infractions administratives. (En 2010, seules 29 décisions formelles ont été émises par les tribunaux.)
Amendes	23
DPD	
Chiffres relatifs aux DPD	S.O.

B. Informations sur la jurisprudence

Vidéosurveillance dans un salon de beauté

L'IPPD a reçu une plainte relative à l'installation de caméras de vidéosurveillance par un salon de beauté, dont une était dissimulée et orientée de telle sorte à permettre de surveiller l'ensemble du corps du client et une autre était installée dans les vestiaires du personnel. L'IPPD a établi que ce type de vidéosurveillance était utilisé sans qu'un responsable des données n'ait rédigé de document écrit pour la réglementer et, par ailleurs, dans des locaux où la personne concernée pouvait raisonnablement s'attendre à une protection absolue de sa vie privée. L'IPPD a également indiqué que le responsable du traitement des données n'avait communiqué aucune information de contact à la personne concernée, n'avait pas informé par écrit le personnel de la vidéosurveillance et n'avait pas notifié le traitement des données automatique à l'IPPD. Pour les points enfreignant la LPJDP, l'IPPD a rédigé un dossier constatant les infractions administratives commises par le propriétaire du salon de beauté. Le tribunal de grande instance de la ville de Vilnius a confirmé le constat d'infractions administratives et a condamné le propriétaire du salon de beauté à verser une amende.

Droit d'un avocat de collecter des données à caractère personnel sensibles

L'IPPD a reçu une plainte concernant la divulgation par un directeur d'hôpital, en conséquence d'une demande d'un avocat agissant pour le compte de son client, de l'ensemble de l'historique médical personnel du plaignant à l'avocat, rendant ainsi ces données publiques, peut-être illégalement.

Au terme d'une enquête, il a été établi que l'avocat, en vertu de son contrat de représentation juridique et de l'article 44 de la loi du barreau de la République de Lituanie, avait demandé à l'hôpital de lui transmettre une copie de l'historique médical du plaignant. Cette copie était destinée à servir de preuve devant le tribunal, afin d'établir si la crainte de se faire attaquer par un chien, sans qu'aucun contact physique n'ait lieu entre le chien et le plaignant, était susceptible d'influer sur la santé du plaignant et, le cas échéant, dans quelle mesure. La demande a été acceptée et l'avocat a présenté l'historique médical au tribunal.

L'article 180 du code de procédure civile de la République de Lituanie indique qu'un tribunal ne peut accepter des informations qui lui sont présentées que si ces dernières permettent de confirmer ou de réfuter des éléments de l'affaire.

Conformément à la LPJDP et au code de procédure civile, l'IPPD a conclu qu'une présentation complète de la copie de l'historique médical du plaignant à l'avocat, au lieu d'un extrait des données de l'historique médical directement liées à l'attaque du chien n'était, en l'espèce, pas excessive et qu'aucune violation de la LPJDP n'avait eu lieu.

Le demandeur a fait appel de la décision de l'IPPD auprès du tribunal administratif régional de Vilnius. Ce dernier a toutefois rejeté l'appel pour les mêmes raisons que celles avancées par l'IPPD. Le demandeur a également fait appel de cette décision, mais la Cour administrative suprême de la République de Lituanie (ci-après, la Cour administrative suprême) a rejeté sa demande.

According to the LLPPD and Code of Civil Procedure, the SDPI concluded that full presentation of the applicant's health history transcript to the lawyer instead of presentation of a health history extract related to the dog attack was not excessive in this case and that there was no violation of the LLPPD.

The applicant appealed the decision of the SDPI before the Vilnius Regional Administrative County Court; however the Court rejected these arguments on the same basis as the SDPI. The applicant also appealed this decision, but the Supreme Administrative Court of the Republic of Lithuania (hereinafter – Supreme Administrative Court) rejected the applicant's appeal.

Collecte par la police de données à caractère personnel aux fins de contrôles internes

L'IPPD a reçu une plainte concernant la collecte illicite par la police de données à caractère personnel relatives au demandeur. L'IPPD a établi que la police avait reçu une information anonyme selon laquelle un officier de police (le frère du demandeur) avait, en remplissant sa demande de remboursement de frais de déplacement, indiqué de fausses données sur sa résidence et son véhicule. Sur la base de ces informations anonymes, la police a lancé un contrôle interne et a vérifié les données à caractère personnel de l'officier. Il a été établi que le véhicule pour lequel l'officier de police avait demandé le remboursement était enregistré au nom du plaignant. La police a donc vérifié les données du plaignant dans le registre des véhicules motorisés de la République de Lituanie, afin d'identifier les véhicules motorisés lui appartenant.

L'IPPD a décidé que la collecte, dans ces circonstances, de données à caractère personnel relatives au plaignant constituait une violation de l'article 3, paragraphe 1, de la LPJDP et a émis une directive à cet effet. Le tribunal administratif régional de Vilnius a toutefois rejeté les arguments de l'IPPD, en précisant que les données à caractère personnel du plaignant avaient été traitées à des fins légitimes en vue de mener un contrôle interne minutieux. L'IPPD a fait appel de cette décision et la Cour administrative suprême a confirmé l'appel, déclarant que l'étendue des données à caractère personnel collectées ne répondait pas à l'objectif de contrôle interne.

C. Autres informations importantes

L'IND met en œuvre le projet «Système de services électroniques pour l'IPPD». Ce projet vise à dématérialiser quatre services publics de l'IPPD (deux pour les particuliers et deux pour les entreprises) de manière à améliorer la qualité des services, de développer la protection des données dans l'environnement électronique et de contribuer à l'évolution de la société de l'information.

LUXEMBOURG

A. Résumé des activités et actualités

Modifications de la législation

La loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques a été modifiée par une loi en date du 24 juillet 2010. Celle-ci met en œuvre les dispositions de la directive 2006/24/CE sur la conservation des données en droit luxembourgeois. Elle stipule que les données doivent être conservées pendant six mois par les différents fournisseurs nationaux de services de télécommunications et opérateurs de réseaux. Les services de police sont les seuls à pouvoir accéder à ces données, moyennant une autorisation judiciaire et dans le cadre de l'élucidation, de la mise au jour et de la poursuite d'«infractions pénales graves», c'est-à-dire des infractions passibles d'un emprisonnement d'une durée égale ou supérieure à un an. Le règlement grand-ducal du 24 juillet 2010 reprend une liste détaillée des différentes catégories de données censées être conservées dans le cadre de la fourniture de services de communications par téléphone fixe ou portable et par l'internet.

Questions de fond

En 2010, la Commission nationale de protection des données a dispensé au gouvernement luxembourgeois des conseils portant sur un large éventail de questions législatives, notamment:

- le projet de loi évoqué plus haut qui transpose les dispositions de la directive 2006/24/CE;
- le projet de règlement grand-ducal qui met en œuvre une base de données nationale des élèves détenue par le ministère de l'éducation;
- le projet de loi sur les dossiers médicaux électroniques;
- le projet de loi transposant les dispositions de la directive 2009/136/CE.

Actualités

Le traitement de données sensibles à des fins de recherche médicale et scientifique a constitué une grande partie du travail de la commission dans le domaine des directives et des autorisations préalables pour les responsables du traitement des données.

La CNPD a publié des lignes directrices générales pour le traitement des données des citoyens par les autorités locales. Elle a également été consultée dans le contexte de la préparation du «recensement» général de la population prévu au début de l'année 2011.

La CNPD a décidé d'entreprendre une enquête sur la question de la collecte «fortuite» de données Wi-Fi par les voitures de Google dans le cadre des voyages de reconnaissance visant la mise en place du service Street View. Au cours de cette enquête, une voiture de Google a été inspectée avec l'aide d'un spécialiste extérieur, qui a conclu que tous les dispositifs contestés avaient été retirés de la voiture. De plus, la DPA nationale a reçu des réponses satisfaisantes à toutes les questions qu'elle avait soulevées.

Au cours de l'année 2010, la CNPD a dû intervenir dans divers cas d'atteintes aux données et de failles de sécurité, parmi lesquels des transmissions accidentelles de données à caractère personnel à des destinataires non visés, des pertes de données, des atteintes aux données liées à des dossiers de clients et de nombreux cas de piratage de sites web (dont les mesures de sécurité étaient déficientes).

Principaux événements et activités de sensibilisation

En 2010, la CNPD a poursuivi ses activités d'information et sa campagne de sensibilisation. Outre une vaste campagne de communication lancée à l'occasion de la Journée européenne de la protection des données, elle a

participé activement à une campagne de sensibilisation sur la sécurité des mots de passe, en collaboration avec le ministère de l'économie et du commerce. La CNPD a également contribué à la création d'une brochure intitulée «Comment protéger vos données sur l'internet», adressée aux jeunes enfants et aux adolescents. Au total, 21 conférences et formations ont été organisées en 2010, outre de nombreuses réunions avec des responsables des secteurs privé et public.

Afin d'élever le niveau de transparence à l'égard du grand public, la commission a demandé à tous les responsables du traitement des données ayant obtenu une autorisation préalable à des fins de vidéosurveillance d'utiliser des étiquettes spéciales conçues par la CNPD. Ces étiquettes informatives doivent être placées à côté des panneaux de vidéosurveillance et avertissent le public de la présence d'un système de surveillance. Elles mentionnent, entre autres, le numéro de l'autorisation et permettent aux personnes concernées de vérifier dans le registre public l'étendue et les restrictions appliquées au traitement autorisé des données.

Organisation	Commission nationale pour la protection des données (CNPD)
Président et/ou collège	M. Gérard Lommel, president M. Thierry Lallemang, commissaire M. Pierre Weimerskirch, commissaire
Budget	1 440 000 EUR
Personnel	Collège: 3 Service juridique: 4 Notifications et vérifications préalables: 2 Administration générale: 3 Communication et documentation: 1 Total: 13
Activités générales	
Décisions, avis, recommandations	436
Notifications	310
Examens préalables	483
Demandes émanant des personnes concernées	242
Plaintes émanant des personnes concernées	145
Conseils sollicités par le Parlement ou le gouvernement	6
Réunions et consultations (secteur public/privé)	110

Conférences et réunions d'information	21
Cas de règles d'entreprise contraignantes où la DPA est l'autorité «chef de file»	2
Activités d'inspection	
Contrôles, enquêtes	16
Activités de sanction	
Sanctions	3
Amendes	s.0.
DPD	
Chiffres relatifs aux DPD	DPD désignés en 2010: 10 Nombre total de DPD désignés (à la date du rapport): 55

B. Informations sur la jurisprudence

La justice de paix en matière civile, dans une affaire en compensation pour des dommages causés par un article publié dans un quotidien national

Les initiales, la profession, l'employeur et la description du poste d'un employé communal ont été mentionnés dans un article publié dans un journal, qui reliait en outre directement le demandeur à une infraction relative à une conduite en état d'ivresse. La justice de paix a jugé que ces mentions constituaient une violation des droits du demandeur en matière de respect de la vie privée. Bien que cette affaire ne relève pas directement des dispositions légales relatives à la protection des données, elle peut être considérée comme un précédent dans le domaine de la vie privée. En effet, les juges ont établi un test permettant d'établir la limite entre liberté de la presse et violation des droits relatifs à la protection de la vie privée.

MALTE

A. Résumé des activités et actualités

Aucune modification de la loi sur la protection des données et des règlements qui en découlent n'a été introduite pendant la période de référence du présent rapport. Toutefois, nos services ont travaillé en étroite collaboration avec l'Autorité maltaise des communications, dans l'objectif d'entamer la procédure de transposition de la directive 2009/136/CE qui modifie, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Le projet d'acte juridique portant transposition des nouvelles dispositions et dispositions modifiées visées par cette directive a été approuvé par les services de l'avocat général. Sa publication était prévue pour le deuxième trimestre 2011. Cet effort de transposition conjoint avec l'Autorité maltaise des communications était nécessaire dans la mesure où, en 2003, la directive 2002/58/CE avait été transposée en partie par la loi sur la protection des données et, en partie, pour les dispositions techniques, par la loi sur les communications électroniques.

Des décisions du commissaire ont été contestées à deux reprises devant les tribunaux en vertu de l'article 49, qui autorise les parties s'estimant lésées par une décision du commissaire à saisir la juridiction d'appel en matière de protection des données. Dans la première affaire, le tribunal s'est prononcé en faveur du commissaire. Dans la mesure où le demandeur n'a pas fait appel de la décision du tribunal dans les délais prévus, l'affaire a été clôturée. Dans la seconde affaire, le demandeur a décidé, au terme de la deuxième audience du tribunal, de retirer son recours et de se plier aux directives du commissaire. Le demandeur a respecté la décision du commissaire et l'affaire a été clôturée.

Des responsables du traitement des données ont également introduit des demandes d'examen préalable concernant l'introduction de systèmes biométriques sur le lieu de travail et l'installation de systèmes de vidéosurveillance, ainsi que pour d'autres types d'opérations de traitement des données entraînant des risques particuliers d'interférences avec les droits et libertés des personnes concernées.

Les missions de nos services comprennent la sensibilisation à la protection des données à l'égard des citoyens, mais également des divers secteurs et responsables du traitement concernés. Un travail continu est entrepris à cette fin, avec la tenue régulière d'exposés, des entretiens avec des journaux locaux et la rédaction d'articles de presse. Cette année, nos services ont tenu des exposés devant divers organismes au sujet de l'applicabilité des règles sur la protection des données dans des secteurs spécifiques. On dénombre parmi ces présentations celles effectuées pour l'association des employeurs maltais, la police maltaise, l'ETC (*Employment and Training Corporation*), les jeunes entreprises et l'université de Malte. Au cours de l'année de référence, nos services ont eu l'occasion de rédiger un article mensuel pour le supplément informatique du *Times* de Malte, abordant les problèmes relatifs à la protection des données dans divers secteurs du domaine numérique, tels que les appareils biométriques, l'informatique en nuage, la publicité comportementale en ligne et les caméras de vidéosurveillance. Cette initiative de sensibilisation a reçu des échos positifs.

Le 28 janvier, l'autorité maltaise de la protection des données s'est associée à d'autres DPA pour célébrer la Journée de la protection des données. Pour célébrer l'évènement à l'échelle locale, les services du commissaire à la protection des données ont distribué des documents informatifs aux élèves des écoles publiques, privées et confessionnelles, dans le but de transmettre le message et de sensibiliser les citoyens, surtout les plus jeunes, aux risques liés à la divulgation d'informations à caractère personnel sur l'internet. Nos services sont en effet intimement convaincus qu'un réel changement de culture n'aura pas lieu sans un investissement permanent auprès des jeunes générations. Apporter un tel changement exige du temps, mais consolider tous les éléments inhérents à la vie privée finira par produire les résultats escomptés. Face au nombre croissant d'applications de réseaux sociaux disponibles, les frontières de la vie privée s'estompent et nos services entendent renforcer les objectifs en la matière, guidés par le concept fondamental d'attentes raisonnables en matière de respect de la vie privée.

Plusieurs dispositions de la loi sur la liberté de l'information sont entrées en vigueur en 2010. En vertu de cette même loi, des règlements ont par ailleurs été publiés sur les frais applicables lors de l'accès aux documents, sur le délai d'introduction d'une plainte ou d'une demande d'enquête, ainsi que sur des exemplaires de formulaires de demande à utiliser par les citoyens pour effectuer une demande d'informations. Les principales autres dispositions devraient être introduites dans un avenir proche.

Organisation	
Président et/ou collège	Commissaire à la protection des données et de l'information
Budget	290 000 EUR
Personnel	Spécialisé: 4.
Activités générales	Appui technique: 2.
Décisions, avis, recommandations	Appui administratif: 2.
Notifications	
Examens préalables	Décisions: 16 décisions et directives émises à la suite de plaintes formelles reçues par nos services.
Demandes émanant des personnes concernées	
Plaintes émanant des personnes concernées	22 avis et recommandations, sous la forme d'articles de presse ciblant à la fois le grand public et les responsables du traitement des données, ou sous la forme d'avis et de recommandations à l'intention des responsables du traitement sur des problèmes spécifiques.
Conseils sollicités par le Parlement ou le gouvernement	184 nouvelles notifications.
Autres renseignements relatifs aux activités générales	4 requêtes d'examen préalable.
Activités d'inspection	Demandes reçues par téléphone: en moyenne 35 appels par semaine.
Contrôles, enquêtes	Demandes reçues par courrier électronique: 191.
Activités de sanction	44 plaintes.
Sanctions	s. o.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	En tout, 8 contrôles ont été effectués en 2010:

B. Informations sur la jurisprudence

There was no new case-law during the period under review.

PAYS-BAS

A. Résumé des activités et actualités

Afin d'assurer une protection aussi efficace et utile que possible des données à caractère personnel, la DPA néerlandaise établit des priorités en se fondant sur une évaluation des risques réalisée annuellement par nos services et constamment mise à jour en fonction des signaux que nous recevons de sources diverses, notamment des journaux, et de la fonctionnalité de signalement proposée aux citoyens sur notre site web. Cette évaluation des risques repose sur des critères tels que la gravité de l'infraction présumée, le nombre de personnes touchées, l'évidence des indices de l'infraction, la faisabilité juridique et les répercussions d'une utilisation à grande échelle des nouvelles technologies. De manière générale, la DPA néerlandaise se concentre sur une application stratégique de la loi de manière à accroître le niveau global de conformité.

En 2010, nos services ont terminé leur enquête relative aux mesures prises par les hôpitaux pour garantir la sécurité des données de leurs patients. Sous l'effet de mesures coercitives sous la forme d'astreintes progressives, le dernier hôpital inspecté a préparé une nouvelle analyse des risques satisfaisante, répondant ainsi aux normes de sécurité applicables au secteur de la santé. L'hôpital a informé la DPA des mesures de réparations adoptées et celle-ci a pu clore l'enquête. L'autorité néerlandaise responsable de la protection des données a aussi enquêté sur la collecte et puis la vente de données et profils sensibles de personnes ayant visité un site web lié à la santé.

Les opérations de traitement des données suivantes, entre autres, ont également fait l'objet d'une enquête de la DPA néerlandaise en 2010:

- la collecte de données Wi-Fi par les voitures Street View de Google;
- le traitement de données à caractère personnel d'étudiants possédant un titre de transport sous forme de carte à puce;
- le croisement de fichiers de données par le service d'enquête de la sécurité sociale;
- l'entrée d'informations policières dans le système d'information Europol;
- l'utilisation de la reconnaissance automatique des plaques d'immatriculation par deux forces de police; et
- l'échange de données relatives à un patient au moyen de dossiers de patients électroniques.

Dans certains cas, l'autorité chargée de la protection des données a dû réagir dans l'urgence. Elle a par exemple dû entamer des discussions avec les maires des villes d'Ede et d'Enschede sur l'enregistrement ethnique des Roms dans leur ville.

Outre la conduite d'enquêtes, la DPA néerlandaise a également pour mission de conseiller le gouvernement sur les projets de loi avant leur soumission au Parlement. Les propositions sont (souvent) modifiées conformément aux suggestions de la DPA afin d'éviter toute atteinte à la vie privée. Ainsi, la proposition de loi relative à l'instauration de compteurs intelligents a été modifiée au profit du consommateur à la suite de nos propositions. La proposition législative pour l'installation dans les voitures d'un éthylotest antidémarrage a elle aussi été modifiée, en vue de garantir que les données ne soient pas conservées plus longtemps que nécessaire.

Enfin, le gouvernement néerlandais, entré en fonction l'année passée, pense présenter une loi néerlandaise sur la protection des données à caractère personnel renouvelée et conforme aux intentions du gouvernement précédent. La DPA contribue activement au processus de consultation préalable à la rédaction du projet de loi, en vue de garantir la rédaction d'un bon projet en faveur des personnes concernées, des responsables du traitement des données, mais aussi de la DPA elle-même.

Organisation	Autorité néerlandaise de protection des données
Président et/ou collège	Jacob Kohnstamm, président. Jannette Beuving, membre du collège et vice-présidente. Madeleine McLaggan, membre du collège.
Budget	Alloué: 7 679 000 EUR. Exécuté: 7 699 000 EUR.
Personnel	77 équivalents temps plein (88 personnes).
Activités générales	
Décisions, avis, recommandations	775 (enquêtes, lignes directrices, code de conduite, examens préalables, sanctions et conseils dans le cadre du processus législatif).
Notifications	3 720
Examens préalables	642
Demandes émanant des personnes concernées	Questions posées à la DPA via son site web: 974. Courriers électroniques reçus: 2 814. Appels téléphoniques reçus: 2 417. Sur l'ensemble de ces demandes, 172 plaintes, 226 demandes d'informations et 154 cas de médiation ont été traités.
Plaintes émanant des personnes concernées	Nombre de plaintes recevables traitées: 172.
Conseils sollicités par le Parlement ou le gouvernement	35
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	60
Activités de sanction	
Sanctions	35
Amendes	s.o.
DPD	
Chiffres relatifs aux DPD	310 DPD signalés à la DPA.

B. Informations sur la jurisprudence

1. Utilisation de caméras de sécurité et rôle de ces dernières lors de poursuites judiciaires

Dans un bar, un individu s'est retrouvé gravement blessé après avoir été frappé au visage avec un verre de bière. Cet incident a été enregistré par une caméra de sécurité du bar et lorsque la police est arrivée sur les lieux ce soir-là, les agents ont regardé l'enregistrement. Le propriétaire du bar a décidé de conserver l'enregistrement et de le stocker sur un disque, pour s'assurer, selon lui, que la police puisse à nouveau visionner la scène si nécessaire.

Dans cette affaire, le tribunal a dit pour droit que le propriétaire du bar pouvait librement livrer l'enregistrement à la police en vertu de l'article 8, point f), associé aux articles 9 et 43, de la loi néerlandaise sur la protection des données, dans l'intérêt de la prévention, de la détection et de la poursuite des crimes. Le tribunal a également retenu qu'une violation éventuelle de la loi néerlandaise sur la protection des données, constituée par la mise à disposition de la séquence aux services de police contrairement aux dispositions de la loi, ne rendait pas l'utilisation de ladite vidéo illégale dans le cadre d'une enquête judiciaire, dans la mesure où la police pourrait y demander l'accès au titre de l'article 126 nd du code pénal.

De plus, le tribunal a estimé que, dans cette affaire, les données ne devaient pas être considérées comme sensibles aux termes de l'article 126 nf du code pénal, puisque la séquence vidéo ne contenait pas plus de détails que ceux observés par les autres clients du bar et ne comprenait pas d'informations supplémentaires au sujet des personnes enregistrées.

Cette décision du tribunal est conforme à l'arrêt rendu par la Cour européenne des droits de l'homme dans l'affaire Perry c. Royaume-Uni, où la Cour a estimé qu'une utilisation normale des caméras de sécurité dans un lieu public n'entraînait aucune violation de la vie privée d'un individu.

2. Droit de rectification

Une personne a réclamé que lui soient communiqués les documents utilisés lors de la rédaction d'un rapport individuel, lequel avait été employé pour évaluer sa demande de permis de séjour. Par la suite, cette personne a demandé à rectifier les documents et le rapport individuel. Sa demande a été refusée. Le Conseil d'État (la plus haute juridiction administrative) a estimé que le but du droit de rectification n'était pas de corriger ou de supprimer des impressions, des avis, des résultats de recherche ou des conclusions présentés à titre d'avis et avec lesquels la personne concernée n'est pas d'accord. Par ailleurs, le Conseil d'État a jugé que le ministère de la justice était en droit d'invoquer l'article 43, point e), de la loi néerlandaise sur la protection des données pour justifier le fait que certains paragraphes du rapport individuel étaient masqués.

3. Droit de rectification et d'accès aux données à caractère personnel

Le ministère de la justice a reçu une demande d'une personne physique souhaitant accéder à des données la concernant elle-même ainsi qu'une fondation, et à les rectifier. Ces données étaient détenues par le bureau BIBOB (l'acronyme BIBOB désignant la loi sur la promotion des jugements d'intégrité par l'administration publique). La requête se rapportant aux données liées à la fondation a été rejetée, car celle-ci n'est pas une personne physique et les articles 35 et 36 ne pouvaient donc pas être invoqués. Les demandes de rectification et d'accès aux données à caractère personnel de la personne concernée ont également été refusées. En effet, selon le ministère de la justice, la loi BIBOB prévoit un régime de transfert en circuit fermé, lequel échapperait donc au champ d'application de la loi néerlandaise sur la protection des données.

En se fondant sur l'histoire juridique, le tribunal a toutefois jugé que la loi BIBOB ne s'opposait pas aux demandes effectuées en vertu des articles 35 et 36 de la loi néerlandaise sur la protection des données et que celle-ci était donc applicable. En outre, le régime de transfert en circuit fermé de la loi BIBOB ne s'applique qu'aux données appartenant à des tiers et non à celles détenues par le bureau au sujet de la personne souhaitant accéder à ses propres données et les rectifier. Dès lors, le tribunal a ordonné au bureau BIBOB de reconsidérer les demandes présentées par le requérant.

POLOGNE

A. Résumé des activités et actualités

En 2010, la loi du 29 août 1997 sur la protection des données à caractère personnel a fêté son douzième anniversaire.

L'année 2010 a vu la désignation d'un nouvel inspecteur général pour la protection des données à caractère personnel (GIODO). Le 25 juin 2010, le Sejm de la République de Pologne a nommé à ce poste le Dr Wojciech Rafał Wiewiórowski. Après l'approbation de sa nomination par le Sénat de la République de Pologne et sa prestation de serment le 4 août 2010, le Dr Wojciech Rafał Wiewiórowski a pris ses fonctions d'inspecteur général pour un mandat de quatre ans.

L'année 2010 a aussi été celle des travaux législatifs sur la révision de la loi polonaise sur la protection des données à caractère personnel, qui ont abouti à l'adoption par le Sejm de la loi du 29 octobre 2010 modifiant la loi sur les données à caractère personnel.

Au nombre des changements les plus significatifs introduits par ces modifications, on distingue les nouvelles compétences du GIODO, y compris le pouvoir d'imposer des sanctions financières comme mesures coercitives à l'intention des entités qui ne respectent pas ses décisions.

En outre, la nouvelle version de la loi accorde expressément au GIODO le droit d'inviter les autorités compétentes à prendre des initiatives législatives et à adopter ou modifier des actes législatifs dans des domaines relatifs à la protection des données à caractère personnel. Les entités ayant reçu un avis formel ou une demande formelle du GIODO ont désormais l'obligation de lui répondre dans les trente jours.

Les dispositions modifiées de la loi sur la protection des données à caractère personnel ont introduit un nouveau type d'infraction, à savoir empêcher ou entraver la réalisation des activités d'inspection du GIODO. Ce délit est désormais passible d'une amende, d'une limitation de liberté, voire d'un emprisonnement d'une durée maximale de deux ans. Cette peine peut être imposée non seulement à un responsable du traitement des données, mais aussi à toute personne impliquée qui aurait empêché ou entravé la conduite de l'inspection. La loi de 2010 modifiant la loi sur la protection des données à caractère personnel entrera en vigueur le 7 mars 2011.

Organisation	Bureau de l'inspecteur général pour la protection des données à caractère personnel
Président et/ou collège	D' Wojciech Rafał Wiewiórowski, inspecteur général pour la protection des données à caractère personnel
Budget	13 842 000 PLN
Personnel	127
Activités générales	
Décisions, avis, recommandations	1 412 décisions administratives émises, dont 879 sur l'enregistrement des fichiers de données à caractère personnel, 137 sur les contrôles, 359 sur les plaintes et 37 sur le transfert des données à caractère personnel vers des pays tiers
Notifications	9 921 fichiers de données à caractère personnel enregistrés
Examens préalables	En conséquence des procédures d'enregistrement (examen préalable), 1 650 fichiers de données à caractère personnel ont été inscrits dans le registre correspondant. Par ailleurs, le traitement de fichiers de données à caractère personnel contenant des informations sensibles ne peut

	commencer qu'une fois la procédure d'enregistrement terminée.
Demandes émanant des personnes concernées	3 448 questions juridiques
Plaintes émanant des personnes concernées	1 114 plaintes au sujet d'atteintes à la protection des données à caractère personnel ont été reçues concernant: • l'administration publique (149 plaintes); • les tribunaux, les services du procureur général, la police et les huissiers (55 plaintes); • les banques et autres institutions financières (119 plaintes); • l'internet (157 plaintes); • le marketing (59 plaintes); • les questions de logement (52 plaintes); • les assurances sociales, individuelles et de biens (28 plaintes); • le système d'information Schengen (38 plaintes); • les télécommunications (57 plaintes); • l'emploi (77 plaintes); et • d'autres sujets (323 plaintes).
Conseils sollicités par le Parlement ou le gouvernement	617 projets de loi ont été soumis au GIODO pour examen.
Autres renseignements relatifs aux activités générales	55 formations ont été assurées par le GIODO sur les dispositions relatives à la protection des données à caractère personnel. Ces formations ciblaient principalement les institutions publiques.
Activités d'inspection	
Contrôles, enquêtes	196 contrôles ont été effectués, y compris dans: • des universités et des établissements de l'enseignement supérieur (26 contrôles); • des sociétés d'investissements menant des activités de courtage (16 contrôles); • des bureaux de contrôle fiscal (10 contrôles); • des fournisseurs de services de télécommunications (14 contrôles); • des entités municipales (16 contrôles); et • des compagnies d'assurance (12 contrôles).
Activités de sanction	
Sanctions	En 2010, le GIODO a signalé 23 soupçons d'infraction. Les tribunaux n'ont imposé de sanctions pénales à aucune entité.
Amendes	
DPD	

Chiffres relatifs aux DPD	s.o.

B. Informations sur la jurisprudence

Le jugement du tribunal administratif régional de Varsovie du 12 mai 2010 (II SA/Wa 652/10) a fait date. Par ce jugement, le tribunal a confirmé la décision du GIODO de refuser de diffuser des informations publiques sous la forme d'un protocole de contrôle des entreprises publiques, en déclarant irrecevable et en rejetant le recours déposé contre cette décision. Le GIODO avait refusé de divulguer lesdites informations, car celles-ci portaient sur des secrets d'entreprise.

La Cour administrative suprême s'est rangée à l'avis du GIODO, selon lequel les entités vendant des produits et services d'un tiers n'ont pas le droit de procéder au traitement à des fins commerciales de données à caractère personnel recueillies dans le cadre d'une demande relative auxdits produits ou services, et ce en vertu de l'article 23, paragraphe 1, point 5, et de l'article 23, paragraphe 4, point 1, de la loi sur la protection des données à caractère personnel (arrêt de la Cour administrative suprême du 5 janvier dans l'affaire I OSK 399/09). La cour a estimé qu'un concessionnaire automobile avait l'obligation d'obtenir le consentement des clients potentiels pour traiter, à des fins commerciales, les données à caractère personnel de personnes s'étant montrées intéressées par l'achat d'une voiture sans toutefois avoir procédé à un essai de conduite. Les données recueillies sur la base d'un contrat de concession ne l'ont pas été dans le cadre de la commercialisation des propres produits et services du concessionnaire et ne peuvent donc pas faire l'objet d'un traitement à cette fin sur la base de l'article 23, paragraphe 1, point 5, de la loi (sur la protection des données à caractère personnel), à savoir sur la base d'un intérêt légitime dans le chef du responsable du traitement des données.

Dans une autre affaire, le tribunal administratif régional de Varsovie a confirmé la position du GIODO estimant qu'à partir du moment où une personne physique est connectée à un compte sur un site web, suite à son identification, le responsable du traitement des données doit tenir compte des objections soulevées par la personne concernée quant au traitement de ses données à caractère personnel à des fins de marketing et, le cas échéant, arrêter de diffuser des publicités (jugement du tribunal administratif de Varsovie du 15 juin 2010 dans l'affaire affaire II SA/WA 556/10).

C. Autres informations importantes

En 2010, l'inspecteur général a reçu 617 projets de loi pour avis. L'autorité de la protection des données s'est montrée préoccupée de la tendance de diverses entités à former des «mégabases» de données à caractère personnel contenant des informations sur des millions d'individus. En 2010, le GIODO a rendu des avis sur plusieurs projets de lois en la matière: le premier visait la mise en place d'un système d'information dans le secteur de la santé, ou «système d'information médicale» (SIM); le deuxième consistait à mettre en place un système d'information sur l'éducation (SIO) qui, sous le couvert de la collecte de données à des fins statistiques, était appelé à devenir un fichier de données à caractère personnel incluant des données sensibles sur les enfants en âge préscolaire, les élèves du primaire et du secondaire, ainsi que sur les enseignants; et le troisième visait l'instauration d'un registre central des entités, à savoir un registre national des contribuables, reprenant partiellement et diffusant à plus large échelle les informations de la base de données de la sécurité sociale en vue de les utiliser comme référence, notamment dans le cadre de dossiers fiscaux.

En 2010, le GIODO a participé activement à l'élaboration de la législation appelée à mettre en œuvre la loi modifiée sur l'informatisation des entités chargées de missions publiques, ainsi qu'à la définition des objectifs de la loi sur la fourniture de services par voie électronique. Il a, à cette occasion, attiré particulièrement l'attention sur la compatibilité de ces projets législatifs avec les principes généraux de la protection des données et sur le besoin de transposer en droit polonais les dispositions de la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de 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 et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

En 2010, le GIODO a examiné l'état de la situation en matière de protection des données à caractère personnel traitées dans les systèmes de vidéosurveillance, dans le but d'initier l'élaboration d'un cadre législatif exhaustif en la matière. Dans ce cadre, le GIODO collaborera avec le médiateur (RPO).

En 2010, davantage de fichiers de données à caractère personnel ont été enregistrés par rapport aux années précédentes (3 760 en 2008, 6 465 en 2009 et 9 921 en 2010), peut-être en raison de la diminution du nombre d'erreurs dans les déclarations par rapport aux années antérieures. Ce résultat a été sans aucun doute influencé par les initiatives du GIODO qui ont entraîné la modification d'un programme informatique permettant de faciliter le remplissage du formulaire de demande instauré en vertu du règlement du ministère des affaires intérieures et de l'administration du 11 décembre 2008 relatif au modèle de notification des fichiers de données pour l'enregistrement auprès de l'inspecteur général pour la protection des données à caractère personnel.

En 2010, le GIODO a poursuivi ses activités didactiques:

- Un protocole d'accord a été signé avec l'association des employeurs de l'industrie de l'internet, IAB Pologne. Celui-ci vise à faire en sorte que les fournisseurs d'accès à l'internet adhèrent, dans le cadre de leurs activités, aux principes de respect de la vie privée, notamment par l'élaboration conjointe d'un code de bonnes pratiques. Les sites web de médias grand public et d'autres sociétés du secteur souhaitent, en signant ce protocole, mettre l'accent sur l'attention qu'ils accordent à une protection adéquate des données à caractère personnel, afin que les personnes qui utilisent divers contenus et services sur l'internet se sentent en sécurité.
- Un «Guide pour les utilisateurs de services de télécommunications accessibles au public» a été élaboré en collaboration avec l'Office des communications électroniques (UKE). Ce guide entend répondre aux besoins tant des consommateurs qui s'apprêtent à choisir un service de télécommunications que de ceux qui utilisent déjà diverses formes de communication électronique.
- Plusieurs conférences ont été organisées, dont une conférence relative à la «réforme de la vie privée», qui a officiellement lancé le débat public sur les moyens de protéger la vie privée à l'ère de la technologie moderne. Ce débat public a pour dessein la formation d'une opinion sur les modifications à apporter aux législations polonaise et de l'Union européenne en matière de protection des données et de la vie privée.

PORTUGAL

A. Résumé des activités et actualités

Cette année a été marquée par la préparation de procédures de notification en ligne devant être lancées en janvier 2011. Dans ce cadre, il a fallu mettre au point un fichier électronique complet, afin de réduire sensiblement la charge pesant sur les responsables du traitement des données dans le cadre du respect de leurs obligations, ainsi que pour diminuer le délai de réponse sans compromettre la qualité de l'évaluation. Le système informatique interne de la DPA a également été amélioré, dans le but de faire progresser le processus de dématérialisation entamé il y a quelques années. Un système de gestion a été instauré, qui facilite la gestion des demandes d'informations des personnes concernées et des responsables du traitement des données, ainsi que le dépôt des plaintes. Toutes ces évolutions techniques ont été réalisées par des experts internes, sans recourir à des sous-traitants.

La DPA a décidé d'augmenter les frais de notification à partir de 2011, qui s'élèveront désormais à 75 EUR pour un enregistrement et à 150 EUR pour un examen préalable du traitement des données.

En dépit d'une charge de travail croissante (presque 10 000 nouvelles procédures), le personnel de la DPA (28 personnes) n'a pas augmenté en 2010. Des règles administratives très strictes rendent extrêmement difficile l'augmentation des ressources humaines.

Par ailleurs, une modification substantielle a été apportée à la loi organique de la DPA. Dorénavant, le budget de la DPA, dont l'ensemble provenait jusqu'à présent du Parlement, aura plusieurs origines et sera en partie issu d'un département du gouvernement, à concurrence du montant équivalent aux propres recettes de la DPA. La DPA déplore les effets très négatifs de ce changement législatif sur son indépendance, puisque l'utilisation de ces fonds sera soumise à une autorisation provenant d'un service relevant directement du gouvernement. En outre, le montant encore reçu du Parlement ne couvrira pas les dépenses de la DPA. En conséquence, son fonctionnement dépendra de façon inacceptable des décisions gouvernementales. Enfin, la DPA est pleinement compétente dans le secteur public et devrait dès lors n'être limitée en aucune façon dans l'exécution de ses tâches.

Un autre point important est la poursuite du projet Dadus. Il s'agit d'un projet de sensibilisation entrepris en 2008 dans les écoles et qui cible les enfants âgés de 10 à 15 ans. Il repose sur une plateforme web proposant des contenus variés sur la protection des données à l'usage des jeunes, des enseignants et des parents. La DPA a développé un programme destiné à être employé dans les classes et qui fait appel à des documents multimédias complémentaires produits par la DPA sur un éventail de sujets.

En 2010, la DPA a également lancé un second concours pour les étudiants appelé «Un slogan pour la vie privée» et a participé à des dizaines de séances dans les écoles. Plus de 2 000 enseignants sont déjà inscrits dans le cadre de ce projet.

Organisation	CNPD – Comissão Nacional de Protecção de Dados
Président et/ou collège	Luís Lingnau da Silveira (président), Ana Roque, Carlos Campos Lobo, Helena Delgado António, Luís Durão Barroso, Luís Paiva de Andrade et Vasco Almeida.
Budget	Budget alloué: environ 3 480 000 EUR (environ 2 140 000 EUR de recettes propres provenant des amendes et des frais de notification). Budget exécuté: environ 2 000 000 EUR.
Personnel	28
Activités générales	

Décisions, avis, recommandations	7 120 décisions. 75 avis émis sur des projets de loi du gouvernement ou du Parlement.
Notifications	8 269
Examens préalables	7 320
Demandes émanant des personnes concernées	Environ 5 600 demandes reçues par courrier électronique (y compris les demandes de responsables du traitement des données reçus par nos services de première ligne). Appels téléphoniques: environ 11 000 (via la ligne téléphonique «vie privée» prévue à cet effet).
Plaintes émanant des personnes concernées	Environ 200. (Les chiffres exacts ne sont pas disponibles, puisque les plaintes sont incluses dans le nombre d'enquêtes initiées par la DPA.) La majorité des plaintes concernaient des communications électroniques non sollicitées (courriers électroniques et appels téléphoniques), ainsi que des techniques variées de surveillance des travailleurs sur leur lieu de travail (vidéosurveillance, examens médicaux abusifs, contrôle des courriers électroniques et de l'utilisation de l'internet, installation dans les voitures de dispositifs de géolocalisation tels que des GPS et téléphones portables octroyés à des salariés qui peuvent en faire un usage privé).
Conseils sollicités par le Parlement ou le gouvernement	83 demandes d'avis. Les principaux thèmes abordés ont été les suivants: les accords bilatéraux entre le Portugal et d'autres États sur la sécurité sociale et la coopération dans les matières policières et fiscales, la vidéosurveillance dans les lieux publics, la surveillance électronique dans le cadre de poursuites judiciaires, les bases de données de la police de la sécurité publique, la mise en place d'une base de données centrale des comptes bancaires dans le cadre de la lutte contre la corruption, la transposition des directives 2006/123/CE, 2006/22/CE, 2008/48/CE et 2007/59/CE, les questions pertinentes relatives à la protection des données dans le budget de l'État, l'enregistrement des appels téléphoniques dans les centres d'appels et la réglementation générale des services pénitentiaires.
Autres renseignements relatifs aux activités générales	Demandes de suppression et d'accès aux données du système d'information Schengen (SIS), droit exercé indirectement par l'intermédiaire de la DPA: 149 Mise à disposition d'orientations à l'intention des responsables du traitement des données concernant certaines questions relatives à la protection des données: • enregistrement des appels téléphoniques dans trois situations (lors de relations contractuelles avec des clients, lors d'appels téléphoniques d'urgence et dans le cadre de l'évaluation de la qualité des performances des travailleurs des centres d'appels); • mise à jour des lignes directrices au sujet des services de santé et de sécurité sur le lieu de travail, conformément aux modifications du code du travail; et • alcootests et dépistage de drogues sur le lieu de travail.

Activités d'inspection	
Contrôles, enquêtes	863 enquêtes 189 contrôles sur place (à la fois dans le secteur privé et dans le secteur public).
Activités de sanction	
Sanctions	248 amendes.
Amendes	507 291,69 EUR imposés par la DPA
DPD	
Chiffres relatifs aux DPD	s.0.

B. Informations sur la jurisprudence

Aucune nouvelle jurisprudence majeure pour la période de référence.

C. Autres informations importantes

The DPA has been involved in many cooperation procedures as part of its own way of carrying out its mission.

Therefore, participation in national working groups should be underlined, such as the Secure Identity National Plan, the platform for health and security in the working environment, or the meetings held with several Government departments to discuss EU legal instruments being developed as well as regular contacts with other independent bodies working in similar areas to ours.

At international level, the DPA is a member of the Ibero-American Data Protection Network and co-organises with the Spanish DPA a yearly meeting to discuss issues of common interest.

The DPA also plays an active role in cooperation with other Member States in Schengen matters.

ROMANIE

A. Résumé des activités et actualités

En 2010, l'autorité de contrôle a été confrontée, d'une part, à des restrictions budgétaires et, d'autre part, à l'impossibilité de pourvoir les cinquante postes prévus par la législation. Un autre problème important (au moment de la rédaction) est que l'autorité nationale de contrôle du traitement des données à caractère personnel est toujours confrontée à un manque de locaux adéquats, ce qui l'empêche de fonctionner conformément à la loi.

En 2010, de nombreuses personnes morales de droit public et privé ont sollicité l'opinion de l'autorité de contrôle quant à la définition des termes «responsable du traitement» et «sous-traitant de données», compte tenu du type d'opérations de traitement effectuées et concernant le besoin de notifier les opérations de traitement de données exécutées par des sous-traitants installés sur le territoire roumain pour le compte de responsables du traitement des données établis ailleurs dans l'Union européenne.

Des informations et des opinions ont également été sollicitées au sujet du traitement des données biométriques (empreintes digitales) susceptibles d'avoir lieu dans le cadre d'un système de contrôle d'accès. Compte tenu des dispositions légales et de la nécessité d'assurer une protection efficace du droit au respect de la vie privée, familiale et intime dans le cadre du traitement des données à caractère personnel, la collecte et le traitement de données biométriques ont été considérés comme excessifs par rapport aux objectifs déclarés de ce traitement. La DPA a recommandé le recours à d'autres solutions pour contrôler l'accès des salariés et enregistrer leurs heures de travail (par exemple, en utilisant un code PIN associé à d'autres informations d'identification relatives au salarié).

En ce qui concerne le transfert/la transmission de données à d'autres États, la majorité des affaires résolues en 2010 ont porté sur la transmission de données à d'autres États membres de l'UE ou à des pays garantissant un niveau adéquat de protection des données à caractère personnel approuvé par la Commission européenne.

Les enquêtes conduites en 2010 par l'autorité de contrôle ont porté sur des cas d'atteintes aux droits des personnes concernées, notamment de leur droit d'accès aux données et de leur droit d'opposition, ainsi que dans divers cas de traitement de données à caractère personnel au sein de fichiers du type de ceux employés par les sociétés de renseignements commerciaux, parmi lesquels un cas de transmission de données négatives à une société de renseignements commerciaux sans information préalable.

En vertu des dispositions de l'article 21, paragraphe 3, point h, de la loi nº 677/2001 sur le traitement des données à caractère personnel et la libre circulation de telles données, l'autorité de contrôle a émis une série d'avis sur des projets d'actes législatifs rédigés par diverses autorités et institutions publiques et renvoyant, entre autres, aux problèmes de la collecte et du traitement des données à caractère personnel. En 2010, l'autorité de contrôle a rendu des avis sur 48 projets de loi, accords, décisions gouvernementales, arrêtés ministériels, etc.

Organisation	Autorité nationale de contrôle du traitement des données à caractère personnel
Président et/ou collège	Mme Georgeta Basarabescu – Présidente
Budget	Budget alloué: 3 679 000 RON, soit environ 876 000 EUR.
Personnel	46 temps plein, plus la présidente et le vice-président.
Activités générales	
Décisions, avis, recommandations	En 2010, comme lors des années antérieures, les personnes concernées et les responsables du traitement des données ont demandé l'avis de l'autorité de contrôle sur les conditions légales du traitement de données à caractère personnel. Au total, 250 avis ont été demandés, ce qui témoigne d'un intérêt croissant envers les dispositions légales relatives à la protection des

	données à caractère personnel.
Notifications	8 956 notifications ont été reçues de responsables du traitement des données à caractère personnel.
Examens préalables	1 contrôle préliminaire.
Demandes émanant des personnes concernées	En 2010, l'autorité de supervision a reçu: 50 demandes d'informations (spécifiques); et 47 pétitions. Ces chiffres ne tiennent pas compte des demandes par téléphone.
Plaintes émanant des personnes concernées	569 plaintes
Conseils sollicités par le Parlement ou le gouvernement	L'autorité de contrôle a rendu des avis sur 48 projets de loi, accords, décisions gouvernementales, arrêtés ministériels, etc.
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	240 enquêtes
Activités de sanction	
Sanctions	70 sanctions. 7 décisions de mettre fin au traitement de données à caractère personnel ou de supprimer les données à caractère personnel traitées.
Amendes	59 600 RON, soit environ 14 200 EUR. 43 avertissements.
DPD	
Chiffres relatifs aux DPD	Cette possibilité n'est pas prévue par le droit roumain.

SLOVAQUIE

A. Résumé des activités et actualités

En 2010, le Bureau de protection des données à caractère personnel de la République slovaque (ci-après «le Bureau») a poursuivi ses travaux en vue de la refonte de la loi actuellement en vigueur sur la protection des données. L'avant-projet de loi modificative tiendra compte des recommandations issues du dialogue structuré avec les représentants de la Commission européenne, des enseignements tirés de l'application de la loi sur la protection des données en pratique, ainsi que des derniers développements intervenus après le lancement d'une approche globale en lien avec le cadre de l'UE pour la protection des données. L'avant-projet de loi modificative a été dévoilé au public et soumis à une procédure de consultation interservices en décembre 2010. La procédure législative était toujours en cours à la fin de l'année.

Le Bureau a également été confronté à une réduction drastique de son budget, d'environ 23 % par rapport à l'année précédente. Dans l'impossibilité d'assumer la totalité des salaires du personnel lors du dernier trimestre de l'année, le Bureau a même dû demander au ministère des finances la réallocation aux fins de paiement des salaires d'actifs économisés par le Bureau les années précédentes dans ses dépenses en capital, ce qui a finalement eu lieu moyennant certaines réserves convenues.

Une baisse supplémentaire a été prévue pour 2011-2013 sous prétexte d'une réduction globale des dépenses de l'administration publique. La situation actuelle a des conséquences négatives sur le contrôle national de la protection des données à caractère personnel et sur l'exécution des tâches du Bureau. En outre, la réputation internationale du Bureau pâtit de l'absence continue de ses représentants dans les conférences et groupes de travail appropriés.

Organisation	Bureau de protection des données à caractère personnel de la République slovaque
Président et/ou collège	Mr Gyula Veszelei
Budget	728 696 EUR
Personnel	34
Activités générales	
Décisions, avis, recommandations	467+16 au titre de la loi sur l'accès du public à l'information
Notifications	40 notifications, ainsi que 1020 notifications de délégués à la protection des données personnelles
Examens préalables	0
Demandes émanant des personnes concernées	483
Plaintes émanant des personnes concernées	121 35
Conseils sollicités par le Parlement ou le gouvernement	85
Autres renseignements relatifs aux	Procédures de contrôle: 277

activités générales	Examens de notifications: 324 Ordres contraignants du Bureau de portée individuelle: 144 Décisions à la suite d'objections formulées à l'encontre des décisions du Bureau: 12 Flux de données transfrontaliers: 11 décisions après approbation de transferts internationaux vers des pays tiers Affaires pénales: 3
Activités d'inspection	
Contrôles, enquêtes	125; 73 demandes d'explication. Autres: Contrôles à l'initiative du Bureau: 121 Principaux thèmes et questions abordés: • fuite de données à caractère personnel de prestataires de soins de santé, notamment de la part des maternités en vue d'assurer les nouveau-nés; • violations dans le chef des distributeurs de télévision par satellite et par câble, ainsi que par les prestataires de services cartographiques et géodésiques; • information insuffisante des personnes concernées dans le secteur du commerce en ligne; • mauvaise communication de données des émetteurs de cartes de fidélité; • copies et numérisations illicites de documents personnels; • marquage inadéquat de zones sous vidéosurveillance; et • collecte de données à caractère personnel excessive par rapport à l'objectif original du traitement et à des fins incompatibles.
Activités de sanction	
Sanctions	21
Amendes	60 578 EUR
DPD	
Chiffres relatifs aux DPD	s.o.

B. Informations sur la jurisprudence

En 2010, trois décisions du Bureau ont été attaquées devant les tribunaux. Un responsable d'un système informatique de traitement de données à des fins de commerce en ligne a intenté une action contre le Bureau, car ce dernier l'avait sanctionné pour ne pas s'être montré suffisamment coopératif. La sanction imposée était de nature disciplinaire. La décision du Bureau est en cours de réexamen par le tribunal de première instance.

Les deux autres affaires portaient sur des «mesures de remédiation» imposées à un responsable du traitement des données et sur leur légalité. Dans le premier cas, le Bureau avait contraint le responsable (comté de Bratislava, vieille

ville) à détruire les données à caractère personnel des personnes concernées publiées sur sa page web sans fondement légal. Le tribunal de première instance n'a pas encore tranché la question. Dans la seconde affaire, le Bureau avait exigé que le responsable (un magasin d'édition multimédia) détruise les données à caractère personnel de nature sensible (données médicales) d'une personne concernée qui avaient été publiées dans un magazine hebdomadaire de société. Dans cette affaire, le tribunal n'a pas non plus encore arrêté son verdict.

SLOVENIE

A. Résumé des activités et actualités

Le Commissaire à l'information est l'autorité compétente pour les infractions et les contrôles dans le domaine de la protection des données, comme prévu par la loi sur la protection des données à caractère personnel de Slovénie (LPDP). En 2010, le Commissaire a ouvert 599 affaires relatives à des violations présumées des dispositions de la LPDP, dont 202 dans le secteur public et 397 dans le secteur privé. Au sein du secteur public, les violations présumées les plus courantes ont porté sur le transfert non autorisé de données à des tiers, la publication illicite de données, la collecte illégale de données, le refus d'accès d'une personne concernée à ses données et la mauvaise sécurité des données. Dans le secteur privé, la plupart des violations présumées ont été liées au détournement des données à des fins de marketing direct, de collecte ou de publication illégales de données, de vidéosurveillance illégale et de transfert de données à des tiers non autorisés. Le Commissaire a imposé des sanctions dans 179 affaires. Le nombre de procédures de contrôle et d'infraction est semblable à celui de l'année précédente.

Outre ses compétences en matière d'infractions et de contrôles, le Commissaire remplit d'autres fonctions fixées par la LPDP. Il rend des avis non contraignants et des éclaircissements sur des questions précises en matière de protection des données soulevées par des particuliers, des responsables du traitement des données, des organismes publics et des organisations internationales. En 2010, le Commissaire a émis 1 859 avis et éclaircissements, ce qui constitue une augmentation significative par rapport à l'année précédente (1 334). Cette hausse peut être attribuée au travail intensif et transparent de sensibilisation du public réalisé par le Commissaire. En vertu de la LPDP, le Commissaire est également compétent pour mener des vérifications préalables sur les mesures biométriques, le transfert de données vers des pays tiers et le raccordement de fichiers. Avant d'effectuer de telles opérations, les responsables du traitement des données doivent recevoir l'autorisation du Commissaire. Le nombre de vérifications préalables n'a pas augmenté par rapport à l'année précédente.

Dans le cadre de ses activités de sensibilisation, le Commissaire a poursuivi son travail de prévention (exposés, conférences et ateliers pour divers types de public). En collaboration avec le Centre slovène pour un internet plus sûr, nos services ont mené des activités de sensibilisation à l'intention des enfants et adolescents (exposés dans les écoles et publications). Quatre ensembles de lignes directrices ont été publiées en rapport avec différents sujets relatifs à la protection des données: les forums en ligne, les évaluations d'impact sur la vie privée, des lignes directrices pour les prestataires de services de santé et des lignes directrices pour les développeurs de solutions informatiques. Deux brochures sur les données des patients et sur la protection des données des consommateurs ont également été publiées. Dans le contexte de la Journée européenne de la protection des données, le Commissaire a organisé un débat sous la forme d'une table ronde, centré sur la propagation du marketing direct et ciblé par les détaillants au mépris des droits des consommateurs. À cette occasion, le Commissaire a récompensé trois responsables du traitement des données pour leurs bonnes pratiques en matière de protection des données à caractère personnel. L'un des prix remis était dédié aux efforts réalisés pour appliquer le principe du respect de la vie privée dès la conception. Grâce à ces initiatives, le Commissaire jouit d'une très bonne réputation et de la confiance du public, ce dont témoignent les résultats du sondage d'opinion représentatif *Politbarometer*. D'après les résultats de l'enquête, le Commissaire occupe la deuxième place dans le classement des institutions slovènes qui jouissent du plus haut niveau de confiance du public.

Le Commissaire s'est impliqué dans divers groupes de travail interservices concernant des projets d'administration en ligne tels que la santé et les services sociaux électroniques, e-VEM (le portail pour les entrepreneurs) et l'archivage en ligne, ainsi qu'à un groupe de travail interservices en charge de la stratégie de développement de la société de l'information pour la période 2011-2015. En outre, les conseils du Commissaire ont été sollicités par le législateur et les autorités compétentes pour 51 lois et autres textes législatifs. Le Commissaire a aussi apporté sa contribution à divers organismes internationaux: le groupe de travail «Article 29», l'autorité de contrôle commune d'Europol, l'autorité de contrôle commune de Schengen, l'autorité de contrôle commune des douanes, EURODAC, le groupe de travail «Police et justice», le groupe de travail international sur la protection des données dans les télécommunications et le comité consultatif du Conseil de l'Europe pour le contrôle de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD). Enfin, M^{me} Pirc Musar a poursuivi son travail en tant que vice-présidente de l'autorité de contrôle commune d'Europol.

Organisation	Commissaire à l'information de la République de Slovénie

Président et/ou collège	Mme Nataša Pirc Musar
Budget	1 500 000 EUR
Personnel	33 personnes: direction (4), administratifs (3), conseillers juridiques sur l'accès aux informations publiques (11), conseillers et chercheurs sur la protection des données (5), contrôleurs de la protection des données (10)
Activités générales	Protection des données et accès aux informations publiques.
Décisions, avis, recommandations	575 avis et recommandations en réponse à des requêtes formulées par des personnes concernées ou des responsables du traitement des données
Notifications	250 notifications relatives à des fichiers de données à caractère personnel
Examens préalables	25 examens préalables: 8 relatifs aux données biométriques, 10 au transfert de données vers des pays tiers et 7 au regroupement de fichiers
Demandes émanant des personnes concernées	1 859 demandes d'avis ou d'éclaircissements de la part de personnes concernées
Plaintes émanant des personnes concernées	Total de 628 plaintes émanant de personnes concernées. 477 plaintes valides: 102 pour des collectes de données illicites, 101 pour des transferts illégaux de données, 90 pour des publications illégales de données, 86 cas de marketing direct, 85 cas de refus à des personnes concernées d'accéder à des données, 59 cas de vidéosurveillance, 47 plaintes sur la sécurité des données et 58 liées à d'autres sujets.
Conseils sollicités par le Parlement ou le gouvernement	Le législateur et les autorités compétentes chargées de rédiger les projets législatifs ont consulté le Commissaire au sujet de 51 lois et autres textes législatifs, y compris la loi sur la protection de la vie privée, la loi sur la procédure criminelle, la loi sur les étrangers, la loi sur les procureurs, la loi sur les conducteurs, la loi sur les assurances, la loi bancaire, la loi sur les jeux de hasard, la loi sur la protection en matière de circulation routière, etc.
Autres renseignements relatifs aux activités générales	En 2010, le Commissaire: • a poursuivi son travail de prévention (exposés, conférences) en collaboration avec le Centre slovène pour un internet plus sûr; • a participé à plusieurs groupes de travail interservices sur des projets d'administration en ligne, de services sociaux, santé et archivage en ligne, etc.; et • a publié quatre ensembles de lignes directrices sur divers sujets liés à la protection des données: les forums en ligne, les évaluations de l'impact sur la vie privée, des lignes directrices pour les prestataires de services de santé et des lignes directrices à l'intention des développeurs de solutions informatiques. Deux brochures sur les données des patients et sur la protection des données des consommateurs ont également été publiées.
Activités d'inspection	

Contrôles, enquêtes	599 contrôles: 202 dans le secteur public et 397 dans le secteur privé.
Activités de sanction	
Sanctions	179 procédures ouvertes pour infraction (45 dans le secteur public et 82 dans le privé), qui ont donné lieu à 36 avertissements, 81 réprimandes, 35 amendes et 10 injonctions de paiement.
Amendes	La DPA a imposé des amendes pour un montant total de 157 417 EUR.
DPD	
Chiffres relatifs aux DPD	s.o.

B. Informations sur la jurisprudence

La société publique de transports en commun de Ljubljana a mis en place un ***système de télébillettique reposant sur l'utilisation d'une carte de voyage électronique anonyme ou nominative.*** Dans ce cadre, elle a commencé à procéder, entre autres, au traitement de données de localisation des passagers (données relatives à l'heure et à l'endroit où la personne est montée dans l'autobus, ainsi que la ligne empruntée). Le Commissaire a établi que, dans le cas d'une carte de voyage nominative, il n'était pas indispensable que la société traite les données relatives à la localisation des passagers puisque ces derniers payaient une somme fixe tous les mois. En l'absence d'un consentement des passagers, le Commissaire a conclu que la société ne disposait pas de la base juridique nécessaire pour procéder au traitement de ces données. Il a été ordonné à la société de supprimer les données de localisation collectées et d'adapter son système en vue de ne plus procéder à l'avenir à un tel traitement.

Le Commissaire a reçu une plainte introduite par un individu qui s'était inscrit à un club par SMS. Il avait rapidement annulé son inscription, mais il continuait à recevoir des SMS à teneur commerciale. La société qui gérait le club par SMS a déclaré qu'un simple ***numéro de téléphone portable ne pouvait pas être considéré comme une donnée à caractère personnel*** dans la mesure où il se rapportait à un appareil et non forcément à une personne. Le Commissaire a estimé qu'un numéro de téléphone portable devait être considéré comme une donnée à caractère personnel, compte tenu de la possibilité pour le responsable du traitement de données d'identifier son détenteur, eu égard à tous les moyens dont il peut raisonnablement disposer pour ce faire. Le marketing direct par SMS n'est autorisé que moyennant le consentement de la personne concernée. Par ailleurs, le responsable du traitement doit supprimer les données ou les rendre anonymes si la personne concernée a annulé son inscription. La cour administrative a ultérieurement confirmé cette décision.

Une société de distribution de journaux a instauré un ***contrôle GPS des personnes distribuant les journaux***. La société a obtenu le consentement de ses salariés, mais les a menacés de licenciement dans le cas où ils ne porteraient pas le dispositif. Le Commissaire a établi que la surveillance par GPS constituait, en l'espèce, une opération de traitement des données et que la société ne disposait pas de la base juridique nécessaire pour procéder à un tel traitement. Le traitement de données à caractère personnel fondé sur le consentement de la personne ne suffit pas dans le cadre de relations de travail, où l'employeur est la partie la plus forte et où le salarié ne peut octroyer un consentement valide s'il est menacé par la rupture du contrat de travail. Le Commissaire a ordonné à la société de mettre un terme à l'utilisation des dispositifs GPS à cette fin.

Une municipalité a entamé des opérations de ***visionnage d'enregistrements de caméras de vidéosurveillance afin de déceler des infractions en matière de stationnement.*** Plutôt que de procéder aux constats «sur place», les agents de la circulation visionnaient les enregistrements des caméras de vidéosurveillance afin de vérifier si des véhicules n'étaient pas stationnés ou à l'arrêt de façon illégale. Ils déterminaient ensuite l'identité des conducteurs et leur faisaient parvenir une contravention. Le Commissaire a estimé qu'une telle conduite était disproportionnée et, par ailleurs, dépourvue de fondement légal. Le Commissaire à l'information a interdit à la municipalité de visionner les enregistrements du système de vidéosurveillance à des fins de poursuites.

Le Commissaire a reçu un grand nombre de plaintes au sujet de la ***publication de données à caractère personnel dans les médias, sur l'internet et, en particulier, sur les sites de réseaux sociaux.*** Le Commissaire n'a compétence que pour agir dans les affaires liées à des données faisant partie de fichiers. Dès lors, dans la plupart des affaires (par exemple dans le cas de la publication de contenus diffamatoires sur des forums en ligne ou de faux profils sur les réseaux sociaux), le Commissaire se contente de conseiller aux individus d'introduire une plainte auprès de la police ou des services du procureur, seuls compétents. Tout détournement de données à caractère personnel est une infraction pénale, comme précisé par le code pénal de Slovénie. La partie lésée peut aussi intenter une action au civil devant un tribunal. Dans les affaires où une publication est liée à des données issues de fichiers (par exemple la publication de poursuites pénales, de dossiers médicaux, etc.), le Commissaire entame une enquête.

C. Autres informations importantes

Le Commissaire s'est également montré actif dans le domaine de la coopération bilatérale internationale. En 2010, le Commissaire a accueilli une visite d'étude de représentants polonais, hongrois et kosovars, ainsi que d'un fonctionnaire du Fonds européen pour les Balkans.

Dans le cadre d'un consortium avec l'Institut autrichien des droits de l'homme Ludwig Boltzmann, le Commissaire à l'information a participé à un projet de jumelage portant sur la mise en œuvre d'une stratégie relative à la protection des données à caractère personnel au Monténégro. Ce projet avait pour ambition de créer un organisme de contrôle national pour la protection des données, ainsi que d'établir et d'appliquer un cadre juridique pour la protection des données au Monténégro.

Parmi les questions de politique largement traitées par le Commissaire, il convient de mentionner l'usage croissant de la vidéosurveillance. En réponse à ce phénomène, le Commissaire a proposé des modifications à la législation existante qui permettraient de mieux protéger les droits des individus dans ce domaine. Le Commissaire a également attiré l'attention sur le développement rapide de la vidéosurveillance intelligente à reconnaissance faciale. Il a par ailleurs relevé que les systèmes informatiques des sociétés privées n'étaient pas suffisamment sécurisés et ne répondaient par conséquent pas aux normes de la LPDP. Une question importante qui suscite de nombreuses préoccupations est le droit des travailleurs à la protection des données et de la vie privée sur le lieu de travail. Le Commissaire a répondu à ces préoccupations par un projet de loi sur la confidentialité des communications sur le lieu de travail. Une attention particulière a été accordée à la formation des responsables du traitement des données afin de promouvoir l'adoption du principe du respect de la vie privée dès la conception, dans le cadre des projets de passage au commerce électronique, des outils de sécurité de l'information et de gestion des événements, ainsi que de l'installation de radars de contrôle de la vitesse moyenne au bord des routes. Le Commissaire s'est en outre intéressé tout spécialement à l'expansion de l'informatique en nuage, qui soulève de nombreuses inquiétudes en termes de sécurité des données et de responsabilité des responsables du traitement, ainsi qu'à l'internet dit «des choses».

ESPAGNE

A. Résumé des activités et actualités

En vue de faciliter le respect par les responsables du traitement des données et les sous-traitants de la loi organique sur la protection des données à caractère personnel et de son règlement d'application, le site web de l'agence espagnole de la protection des données (AEPD) donne dorénavant accès à un outil d'auto-évaluation appelé EVALÚA. Cet outil permet à son utilisateur de vérifier la conformité de ses opérations de traitement avec la législation et d'obtenir un rapport détaillant toute erreur détectée, afin de lui permettre, le cas échéant, d'adopter les mesures correctives nécessaire. À la fin de l'année 2010, l'outil EVALÚA comptabilisait 20 294 accès.

Dans la poursuite de sa politique d'information des experts et des individus soumis à la loi sur la protection des données à caractère personnel, l'agence a organisé sa 3e session annuelle ouverte, à laquelle ont assisté plus de 800 personnes. Elle a également élargi son éventail de guides informatifs disponibles au sujet de la loi sur la protection des données, avec la publication d'un guide intitulé «Guide du respect de la vie privée et de la sécurité de la technologie d'identification par radiofréquence», en collaboration avec l'INTECO (Institut national des technologies de la communication) et à la réédition du «Guide sur la sécurité». Cet ouvrage inclut un modèle de «document de sécurité» qui fait office de guide et facilite la mise en œuvre et le respect des règles sur la protection des données.

De plus, le Conseil général du pouvoir judiciaire et l'AEPD ont signé un accord de collaboration établissant un protocole relatif à l'exécution de contrôles en matière de protection des données dans les organes du système judiciaire et à la mise en œuvre de mesures favorisant la bonne application par l'ensemble des organes judiciaires des règles relatives à la protection des données.

Dans le même esprit et vu l'importance des données médicales, l'AEPD a décidé de rédiger un «rapport sur le respect de la loi sur la protection des données à caractère personnel dans les hôpitaux», après avoir constaté une augmentation des cas de violation de cette loi et principalement de ses dispositions imposant des obligations en matière de sécurité et de confidentialité. Ce rapport a été élaboré sur la base des réponses reçues à un questionnaire envoyé à plus de 600 centres repris dans le registre national des hôpitaux, dont 92 % ont répondu.

Par ailleurs, l'AEPD a entretenu des contacts avec d'importants réseaux sociaux en ligne, tels que Tuenti et Facebook, afin d'améliorer leur politique de respect de la vie privée et d'éviter que les mineurs de moins de 14 ans puissent y accéder.

En juin 2009, l'AEPD a été choisie comme chef de file d'un projet de jumelage devant être réalisé en Croatie. Ce projet vise à collaborer avec l'Agence croate de protection des données à caractère personnel afin de préparer son entrée dans l'UE. Il est financé par l'Union européenne à hauteur de 1 350 000 EUR et doit durer 22 mois. En 2010, le projet de jumelage avec l'État d'Israël avait été un succès. L'AEPD avait été choisie pour coordonner ce projet qui avait duré 20 mois.

Comme il ressort du tableau ci-dessous, les activités d'enregistrement et de contrôle s'intensifient.

Organisation	Agence espagnole de protection des données
Président et/ou collège	M. Artemi Rallo/M. José Luis Rodriguez (depuis juin 2011)
Budget	15 425 160 EUR
Personnel	147 fonctionnaires, 7 agents contractuels et 1 commissaire.
Activités générales	
Décisions, avis, recommandations	Nombre de décisions relatives à des réclamations: 6 189; rapports: 120.
Notifications	623 148 opérations enregistrées (fichiers publics et privés). Nombre total de fichiers notifiés: 2 144 872 (+ 31 %).
Examens préalables	s.o.
Demandes émanant des personnes concernées	104 826 demandes reçues par la ligne d'assistance (par écrit, par téléphone, via l'internet ou au guichet) (+ 8,2 %). 597 demandes de rapport envoyées au service juridique (298 provenant des administrations publiques et 229 de citoyens ou de sociétés).
Plaintes émanant des personnes concernées	4 300 plaintes de personnes concernées, concernant, entre autres, les secteurs des télécommunications et de la vidéosurveillance (respectivement 29 et 14 %), de l'internet et de la publicité.
Conseils sollicités par le Parlement ou le gouvernement	L'AEPD a émis des avis juridiques sur un total de 97 dispositions générales, y compris sur la loi pour une économie durable, la loi sur le registre civil, la loi sur le crédit à la consommation et la loi de réglementation des jeux de hasard, ainsi que plusieurs projets d'arrêtés royaux.
Autres renseignements relatifs aux activités générales	2 499 179 accès par l'internet (en moyenne 7 619 par jour). 2 508 850 consultations du registre public. $ 560 autorisations du directeur des transferts internationaux.
Activités d'inspection	
Contrôles, enquêtes	4 302 enquêtes préalables et 1 643 réclamations émanant de personnes concernées. 6 189 résolutions de procédures de contrôle (+ 5,76 %) dont: – 1 830 réclamations relatives à la protection de droits (d'accès, de rectification, de suppression et d'opposition et – 4 359 procédures liées au pouvoir de sanction. Le service de contrôle n'a pas seulement agi en réaction à des problèmes précis, mais aussi spontanément, dans le cadre de ses fonctions, dans divers secteurs: • la protection des données dans les hôpitaux; • le transfert de données commerciales;

	• le contrôle de la vente de dettes par les opérateurs de télécommunications et les institutions financières; • le contrôle du système Schengen en Espagne; • l'analyse des clauses contractuelles des opérateurs de télécommunications; et • une enquête sur les critères d'accès basés sur l'intérêt légitime pour le registre foncier, le registre des véhicules et le registre du cadastre.
Activités de sanction	
Sanctions	591 sanctions, dont 92,49 % liées à la loi sur la protection des données, 7,23 % à la loi sur les services de la société de l'information (courriers électroniques publicitaires non sollicités) et 0,28 % à la loi sur les télécommunications (publicités, fax).
Amendes	17 497 410,02 EUR (- 29,65 % par rapport à 2009).
DPD	
Chiffres relatifs aux DPD	s.o.

B. Informations sur la jurisprudence

Le «droit à l'oubli» sur l'internet est devenu un sujet de débat des plus brûlant en lien avec les nouveaux services liés à l'internet. L'Agence espagnole de la protection des données a réagi aux plaintes du public à propos de services rendus par des multinationales en considérant que la loi espagnole de protection des données est applicable dans les situations où se présente un mélange d'éléments tels que l'utilisation de moyens en Espagne, l'existence d'un établissement et le ciblage des utilisateurs. Certaines décisions ont fait l'objet d'un appel devant l'*Audiencia Nacional* (tribunal national) même si celui-ci n'a encore rendu aucun jugement.

La DPA espagnole a cosigné avec diverses autorités de plusieurs régions une lettre commune adressée à Google Inc. relative à *Google Buzz*. Comme l'illustre cet exemple parmi d'autres, l'agence entend donc, en collaboration avec d'autres organismes, faire progresser la protection des utilisateurs de l'internet. C'est dans cet objectif que s'inscrivent également diverses enquêtes menées au sujet d'atteintes présumées à la législation relative à la protection des données. En octobre 2010, l'AEPD a entamé une procédure à l'encontre de Google Inc. et de Google Espagne pour avoir collecté et stocké des informations sur les réseaux Wi-Fi grâce aux véhicules employés pour le service *Street View*. Des contrôles de Facebook ont également débuté au mois d'octobre. Facebook a fait l'objet de demandes de renseignements afin de déterminer si des utilisateurs espagnols avaient été touchés par la divulgation de données à des annonceurs ou autres sociétés par l'une ou l'autre des applications les plus populaires de Facebook. En novembre, des actions similaires ont été entreprises à l'égard de MySpace.

Résolutions de l'AEPD

→ L'AEPD a confirmé le droit à la suppression des données personnelles dans un blog de la plateforme *Blogger* de Google. Dans cette affaire, l'agence a considéré que les renseignements à caractère personnel devaient être supprimés, la liberté d'expression s'arrêtant aux frontières d'autres droits. Sur ce point, le tribunal national a estimé que, même si l'information divulguée n'avait pas d'intérêt pour le public, les droits de protection des données primaient. Si le moteur de recherche n'est pas responsable du contenu des blogs repris sur sa plateforme, il doit néanmoins ordonner leur retrait ou y empêcher l'accès lorsque l'AEPD le décide en tant qu'autorité compétente et qu'il en a connaissance (TD/00242/2010 et TD/00021/2010).

→ Le fait d'envoyer des courriers commerciaux non sollicités sans utiliser le champ CCI et en divulguant les adresses des destinataires constitue une double infraction. D'une part, ce type d'envois est considéré comme un courrier commercial non sollicité (spam) et constitue dès lors une violation de l'article 21 de la loi sur les services de la société de l'information. D'autre part, l'adresse de courrier électronique est considérée comme une donnée à caractère personnel et envoyer un courrier électronique qui divulgue plusieurs adresses à des destinataires différents sans leur consentement est une violation de l'article 10 de la loi sur la protection des données à caractère personnel relatif à la violation du secret et de la confidentialité des données (PS/00228/2010).

Jurisprudence: Tribunal national

- Par décision du 10 février 2010, le tribunal a estimé qu'un journal officiel s'était rendu coupable d'infraction à l'obligation de secret en publiant une décision disciplinaire prise à l'encontre d'un fonctionnaire, comprenant des détails relatifs aux faits reprochés, les motifs précis de la sanction imposée, en lien avec des poursuites pénales engagées à l'encontre de ce fonctionnaire, ainsi qu'une transcription, mot pour mot, de la condamnation pénale du plaignant, révélant ainsi le crime et sa sanction. Le tribunal national a considéré que la divulgation de ces données était excessive par rapport à la finalité prévue de la publication.
- Dans un autre jugement rendu le 23 février 2010, le tribunal a affirmé la primauté du droit à la liberté d'information dans le cas de la publication dans un journal en ligne de données relatives aux salaires et aux contrats des gestionnaires de sociétés publiques et de leur époux ou épouse.

Jurisprudence: Cour suprême

- Dans son arrêt du 2 juin 2010, la Cour suprême a confirmé la doctrine en vigueur relative à la violation du devoir de secret lors de la divulgation de documents. Elle a estimé que l'infraction était imputable à la société demanderesse si les documents en question avaient été abandonnés par un tiers qui a montré ultérieurement qu'il travaillait pour cette société.
- Dans ses arrêts du 22 juillet et du 5 octobre 2010, la cour a insisté sur la nécessité de conclure un contrat écrit dans le cadre du recours à un sous-traitant pour des opérations de traitement de données ou, à défaut, de pouvoir prouver par tout autre moyen l'objet de la sous-traitance, conformément à l'article 12.2 de la loi sur la protection des données, ce qui n'était pas le cas dans l'affaire considérée.

Trois arrêts du 15 juillet 2010 se sont avérés particulièrement pertinents pour le règlement des recours introduits contre le règlement d'application de la loi sur la protection des données et deux décisions préjudicielles concernant l'article 10.2, point b), dudit règlement (relatif à la notion d'intérêt légitime). La Cour suprême, qui approuve pleinement le règlement, n'a annulé que 5 des 158 éléments qui le composaient, sans se prononcer sur l'article 10.2, point b), et en renforçant la sécurité juridique autour du régime espagnol de protection des données[7].

[7] Pour davantage d'informations, consulter l'adresse suivante (en espagnol): https://www.agpd.es/portalwebAGPD/jornadas/3_sesion_abierta_2010/common/SESION_ABIERTA_2010_SEGUNDA_PARTE.pdf.

SUÈDE

A. Résumé des activités et actualités

Évolutions législatives

Amendements à la constitution suédoise

En 2010, de nombreux lois et projets de lois entraînant des répercussions sur le respect de la vie privée ont vu le jour. Le *Riksdag* (Parlement suédois) a notamment adopté, le 24 novembre, divers amendements à la Constitution, dont un renforçant la protection de la vie privée. Cette dernière modification vise à garantir que l'État et les municipalités ne mettent pas au point de nouvelles bases de données détaillées sans motifs juridiques clairs et sans évaluer si la mesure législative en question est proportionnelle compte tenu de l'atteinte à la vie privée qu'elle constitue. Cet amendement constitutionnel est le résultat de critiques exprimées par un comité du gouvernement, le comité de la protection de la vie privée, après une enquête poussée et une analyse présentée dans deux rapports de 2007 et 2008. Au fil des ans, le Conseil de l'inspection des données a rencontré de nombreux exemples d'avant-projets de textes juridiques dont l'analyse relative à la vie privée était très mauvaise, certains en étant même dépourvus.

Loi sur les informations en matière de crédits

Dans les précédents rapports, nous avons fourni des informations sur la loi sur les informations en matière de crédits et sur le fait qu'un amendement à la loi fondamentale sur l'expression (une loi constitutionnelle) de 2003 avait entraîné la possibilité de divulguer à toute personne des informations de solvabilité sur un site web, sans devoir se conformer aux règles strictes de la loi sur les informations en matière de crédits. Cette situation a conduit à des violations de la vie privée et à de nombreuses plaintes. En juin 2010, le *Riksdag* a adopté la proposition du gouvernement visant la modification de la loi sur les informations en matière de crédits dans le but d'assurer une meilleure protection des particuliers sur l'internet.

Directive sur la conservation des données

La directive européenne sur la conservation des données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public n'a toujours pas été transposée en droit national suédois. Le gouvernement suédois a présenté un projet de loi sur la conservation des données relatives au trafic à des fins d'application de la loi, afin de mettre en œuvre la directive en Suède. Toutefois, une minorité regroupant trois groupes parlementaires est parvenue à imposer un gel du projet de loi en vertu du chapitre 2, article 22, de l'Instrument de gouvernement (l'une des lois fondamentales). En conséquence, le projet de loi ne pourra pas être adopté par le *Riksdag* avant le mois de mars 2012.

Activités de contrôle et autres questions d'intérêt

Loi de surveillance des signaux

Le 12 février 2009, le gouvernement a chargé le Conseil d'inspection des données d'examiner le système de gestion des données à caractère personnel de l'Établissement radio de la défense nationale (FRA) dans le cadre de ses activités de surveillance des signaux électromagnétiques à des fins de renseignement. La nouvelle loi de surveillance des signaux est entrée en vigueur le 1er janvier et, bien qu'elle comprenne un grand nombre de règles destinées à protéger la vie privée, le *Riksdag* a demandé davantage de mécanismes de contrôle. En décembre 2010, le Conseil de l'inspection des données a communiqué ses conclusions au gouvernement. Nos services ont analysé, entre autres, les problèmes liés à la vie privée susceptibles de survenir dans le cadre de l'exercice des activités de renseignement d'origine électromagnétique du FRA. Le Conseil de l'inspection des données a également étudié les procédures et directives encadrant ces activités, afin de déterminer si celles-ci offraient des garanties suffisantes pour la gestion de ces problèmes. À la suite de remarques de la part du Conseil de l'inspection des données, le FRA a amélioré ses procédures de gestion des données à caractère personnel. Il a, notamment, instauré des audits systématiques et réguliers des journaux permettant un suivi des accès incorrects ou non autorisés aux données à caractère personnel.

Contrôle du système d'identification électronique nationale en vigueur (e-id)

L'Office national d'audit suédois a déclaré que le contrôle du système d'identification électronique nationale (*e-id*) était insuffisant. Ni toutes les opérations ni toutes les parties impliquées dans l'émission et la vérification des identités électroniques n'ont été soumises à des audits de sécurité de l'information. Le Conseil de l'inspection des données a ouvert un projet qui vise à comprendre les différentes étapes de l'émission d'une identité électronique et à cartographier les intervenants, notamment les responsables du traitement et les éventuels sous-traitants. Ce projet comprend une série de contrôles effectués chez les émetteurs (les banques, par exemple) et chez les utilisateurs (les autorités publiques, entre autres) afin d'établir si le système *e-id* est conforme aux règles de protection des données.

Un site contre les atteintes à la vie privée sur l'internet

Début 2010, le Conseil de l'inspection des données a lancé un site web à l'intention des jeunes, *kränkt.se* ou *krankt.se*. Ce site met à leur disposition des conseils s'ils s'estiment victimes d'un abus sur l'internet.

Rapport annuel sur le respect de la vie privée

Une nouvelle fois, le Conseil de l'inspection des données a rédigé un rapport sur la vie privée, intitulé ***Respect de la vie privée en 2010***. Comme les deux années précédentes, ce rapport revient dans les détails sur les nouvelles lois, les propositions, les décisions et les évolutions techniques qui ont eu une influence sur la vie privée au cours de l'année.

Organisation	Conseil de l'inspection des données
Président et/ou collège	Le Conseil de l'inspection des données est dirigé par le directeur général. Il comprend également un comité consultatif où siègent cinq membres
Budget	3 300 000 EUR
Personnel	44 (27 juristes, 4 informaticiens TI et 1 collaborateur chargé des ressources humaines, 2 personnes chargées de la communication et 10 agents administratifs)
Activités générales	
Décisions, avis, recommandations	Lignes directrices sur les alertes professionnelles (*whistleblowing*), liste de contrôle sur l'utilisation des techniques de localisation, rapport sur la façon de gérer et de protéger les données à caractère personnel sensibles dans les compagnies d'assurance privées et recommandations au gouvernement sur l'IMI.
Notifications	289 notifications. Il convient d'ajouter que le législateur suédois a utilisé presque toutes les possibilités de dérogation à l'obligation de notification.
Examens préalables	344
Demandes émanant des personnes concernées	2 100 courriers électroniques et 5 300 questions par téléphone au sujet de la loi sur la protection des données, 527 questions par téléphone au sujet de la loi sur les informations en matière de crédits et 884 questions par téléphone relatives à la loi sur le recouvrement des dettes.

Plaintes émanant des personnes concernées	332 relatives à la loi sur la protection des données à caractère personnel, 18 relatives à la loi sur les informations en matière de crédits et154 relatives à la loi sur le recouvrement des dettes.
Conseils sollicités par le Parlement ou le gouvernement	74 consultations et 50 consultations informelles au sujet de projets de loi susceptibles d'affecter la vie privée.
Autres renseignements relatifs aux activités générales	Le Conseil de l'inspection des données a émis une nouvelle règle administrative concernant les alertes professionnelles. Elle a également traité plus de 70 consultations avec des délégués à la protection des données et environ 10 règles d'entreprise contraignantes dans le cadre de la procédure de collaboration (et non en tant que «chef de file»).
Activités d'inspection	
Contrôles, enquêtes	210 contrôles, centrés principalement sur le blanchiment d'argent, les médias sociaux, les technologies de localisation dans la vie professionnelle, les caméras de vidéosurveillance, le système *eCall*, les bases de données de la police et le marché de la pharmacie.
Activités de sanction	
Sanctions	Aucune en 2010
Amendes	s.o.
DPD	
Chiffres relatifs aux DPD	Nombre total de notifications de DPD: 6 442, dont 206 nouvelles en 2010. Le nombre total de DPD s'élève à 3 828. (Un même DPD peut exercer plusieurs mandats.).

B. Informations sur la jurisprudence

Décision de la Cour administrative suprême de Suède relative à la publication sur l'internet d'informations sur les créanciers dans le cadre d'une faillite

Cette affaire portait sur l'application de l'article 10, point f), de la loi sur les données à caractère personnel relatif à la détermination de l'importance relative des intérêts du responsable du traitement des données et de ceux de la personne concernée. Un cabinet de conseil avait, sur son site web, publié les noms, adresses et montants des dépôts d'un grand nombre de créanciers, ainsi que des informations sur les débiteurs d'une institution financière en faillite. Les personnes concernées n'avaient pas donné leur consentement pour cette publication et la Cour administrative suprême a déclaré que publier ces données sur l'internet rendait l'information très facile d'accès et la diffusait largement. Elle a jugé que l'intérêt du responsable du traitement des données à caractère personnel n'était pas plus important que celui qu'avaient les personnes concernées à protéger leur vie privée.

Décision de la cour administrative d'appel relative aux clés électroniques

Une société de logement avait mis en place un système de clés électroniques que devaient utiliser les résidents pour déverrouiller les portes extérieures, mais également intérieures, des bâtiments. Chaque clé électronique était reliée à un appartement précis et chaque utilisation laissait une trace dans un journal de passage, qui indiquait

quand et où le résident utilisait la clé. L'un des objectifs poursuivis grâce à ces journaux était le contrôle des personnes ayant accédé à la buanderie, afin de régler certains problèmes qui avaient été soulevés dans ce local. Aucun consentement n'avait été accordé pour le traitement de ces journaux de passage. La cour a déclaré, à l'instar du Conseil de l'inspection des données, que l'intérêt des personnes concernées à la protection de leur vie privée était plus important que l'intérêt du responsable, la société de logement, à résoudre les problèmes liés à la buanderie.

Décision de la cour administrative d'appel relative à l'utilisation de SMS par l'Office d'assurance sociale

Le Conseil de l'inspection des données a ordonné que l'Office d'assurance sociale (l'Office) mène une analyse de risques et de vulnérabilité sur, entre autres, la transmission par messages textuels d'informations relatives aux allocations parentales temporaires. L'Office a affirmé qu'il n'était pas dans l'obligation de réaliser cette analyse, puisqu'il n'était pas le responsable du traitement des données tant que l'information envoyée par SMS n'avait pas atteint sa destination sur son site web. Le Conseil de l'inspection des données et les tribunaux ont estimé que l'Office était le responsable du traitement dès l'instant où les individus envoyaient l'information. La cour administrative d'appel a estimé que le Conseil de l'inspection des données, en tant qu'autorité de contrôle, devait, au cas par cas, fixer les mesures de sécurité devant être mises en place par le responsable du traitement des données. La cour a jugé que l'analyse en question était une mesure de ce type et qu'elle n'était ni coûteuse ni en aucune autre manière inappropriée.

Décision de la cour administrative sur les alertes professionnelles

Une société avait demandé au Conseil de l'inspection des données la permission de traiter des données à caractère personnel dans le cadre d'un système de dénonciation. L'autorisation a été accordée, mais seulement dans une certaine mesure et moyennant le respect de conditions particulières. L'une d'entre elles était que le traitement de données à caractère personnel relatives à des délits ne pouvait être effectué que pour les personnes occupant des fonctions clés ou élevées dans la hiérarchie de la société. Cette dernière a introduit un appel à l'encontre de cette restriction et a déclaré que tous les salariés devaient être inclus dans le système de notification. Au départ, la cour a indiqué que le traitement concernait des données à caractère personnel extrêmement sensibles, relatives à des rapports sur des infractions présumée à la loi. Elle a ensuite décidé, après avoir pesé les différents intérêts, que ceux de la société n'étaient pas plus importants que ceux des personnes concernées en matière de protection de la vie privée.

Décision de la cour administrative relative à la vidéosurveillance des travailleurs

Une société de transports publics avait, durant un mois, mis en place un système de vidéosurveillance dans l'un de ses dépôts d'autobus, afin de résoudre de graves problèmes liés, entre autres, au sabotage de véhicules et d'oblitératrices. Le lieu de travail en question regroupait environ 600 travailleurs et un pour cent d'entre eux, au plus, était impliqué dans ces méfaits. La cour a estimé que cette vidéosurveillance constituait une atteinte particulière au droit à la vie privée, puisqu'elle n'avait fait l'objet d'aucune information. D'après la cour, cette surveillance s'était soldée par un empiètement sur la vie privée des personnes concernées qui était sans commune mesure avec les objectifs de la surveillance.

C. Autres informations importantes

En 2010, le nombre de contrôles a considérablement augmenté.

En 2010, le Riksdag a décidé d'augmenter de presque 10 % le budget du Conseil de l'inspection des données.

ROYAUME-UNI

A. Résumé des activités et actualités

January: le projet de loi sur les coroners et la justice a reçu la sanction royale, fournissant au Commissaire à l'information (ICO) le pouvoir de contrôler certains services publics centraux sans autorisation particulière.

À l'occasion de la Journée européenne de la protection des données, nous avons lancé une campagne intitulée «Pensez à la vie privée» et assuré la promotion du projet i in online («moi, en ligne»).

February: dans le cadre de la préparation de notre rapport au Parlement sur la situation en matière de surveillance, nous avons chargé le «réseau des études sur la surveillance» (Surveillance Studies Network) de rédiger un rapport sur l'évolution de la surveillance au Royaume-Uni depuis 2006.

Nous avons mis en demeure le parti travailliste de cesser de procéder à des appels automatisés non sollicités à des fins de marketing en infraction avec la législation relative à la vie privée et aux communications électroniques.

March: nous avons accueilli à Manchester la conférence des délégués à la protection des données.

Nous avons publié un rapport sur les dividendes de la vie privée (Privacy Dividend Report) présentant aux organisations des arguments financiers susceptibles de les pousser à adopter de bonnes pratiques en matière de protection des données.

April: nos nouvelles compétences sont entrées en vigueur, permettant à l'ICO d'imposer des sanctions pécuniaires pour des violations graves de la loi sur la protection des données.

Nous avons émis des lignes directrices sur la protection des données à l'intention des partis politiques et des candidats aux élections législatives.

July: nous avons publié notre nouveau code de bonnes pratiques relatif aux informations à caractère personnel en ligne à l'intention des organisations réalisant des opérations commerciales en ligne.

Nous avons lancé une campagne en vue de rappeler aux médecins non conventionnés d'informer l'ICO au sujet de l'endroit où ils traitent les informations personnelles. Plus de 3 300 nouvelles notifications ont été reçues en conséquence directe de notre campagne.

August: nous avons rappelé aux agents louant et vendant des biens immobiliers qu'ils encourent des poursuites judiciaires en cas d'absence de notification à l'ICO. Près de 1 000 nouvelles notifications ont été reçues des suites directes de notre campagne.

Nous avons commandé un examen sur la disponibilité des conseils en matière de sécurité pour les organisations de petite taille et de taille moyenne, afin de mieux comprendre comment elles accèdent à des conseils sur la protection des données à caractère personnel.

September: nous avons accueilli une délégation de Macédoine, dont les membres recherchaient des conseils concernant l'adoption et l'application de dispositifs législatifs relatifs à la protection des données.

Par ailleurs, nous avons reçu à Manchester l'atelier européen de traitement des dossiers, avec 50 représentants de 29 pays et territoires européens.

October: George Osborne, député local et ministre des finances, a officiellement inauguré l'extension de notre siège de Wilmslow, qui accueille désormais sous le même toit l'ensemble du personnel de l'ICO.

Nous avons imposé nos deux premières amendes à l'encontre de la société privée A4e et du Conseil du comté du Hertfordshire, pour violations graves de la loi sur la protection des données.

Google Inc. s'est engagé par écrit à améliorer la gestion des données afin de garantir que des violations telles que la collecte de données sur les réseaux Wi-Fi par les véhicules de Google *Street View* ne se reproduisent pas.

November: nous avons livré au Parlement une mise à jour de la situation en matière de surveillance et lui avons rappelé que toute nouvelle loi appelée à avoir des conséquences sur la vie privée devrait être soumise à un examen post-législatif.

Nous avons intenté avec succès des actions en justice contre deux anciens salariés de T-Mobile, en vertu de l'article 55 de la loi sur la protection des données, qui dispose que la divulgation ou la vente de données à caractère personnel sans le consentement du responsable de leur traitement constitue une infraction.

December: nous avons rappelé aux écoles de ne pas se cacher derrière des mythes sur la protection des données pour empêcher les parents de photographier les spectacles scolaires de Noël, une information relayée par plus de 100 articles et reportages de presse.

Nous avons réagi à l'annonce du gouvernement sur le projet de loi relative à la protection des libertés.

Plus d'informations sur nos activités de 2010 se trouvent dans nos rapports annuels de 2009/2010 et 2010/2011, publiés sur notre site web à l'adresse www.ico.gov.uk.

Sauf mention contraire, les chiffres ci-dessous se rapportent à l'exercice financier s'étendant d'avril 2010 à avril 2011

Organisation	Bureau du Commissaire à l'information
Président et/ou collège	Christopher Graham, commissaire à l'information
Budget	Environ 20 172 000 GBP
Personnel	351 (327 équivalents temps plein, y compris le personnel pour la loi sur la liberté de l'information et autre collaborateurs n'exerçant pas de tâches directement en rapport avec la protection des données, dans la gestion des bâtiments, les finances et les ressources humaines, p. ex.)
Activités générales	
Décisions, avis, recommandations	36 déclarations publiques autres que des lignes directrices et des actions coercitives. Sont comprises dans ce nombre les déclarations effectuées à propos de Google, de la sensibilisation en matière de vie privée, des droits relatifs à la protection des données et en matière d'obligations, ainsi qu'à propos des modifications aux lois sur la liberté de l'information et sur la protection des données (notamment en ce qui concerne les *cookies*). 3 codes de bonnes pratiques (informations personnelles en ligne, partage de données, avis d'évaluation). 55 procédures de sanction (voir ci-dessous) et déclarations correspondantes aux médias.
Notifications	339 298
Examens préalables	s.o.
Demandes émanant des personnes concernées	206 585 appels via la ligne d'assistance (comprend l'ensemble des appels, à savoir ceux liés aux lois sur la liberté d'information, sur la protection des données personnelles, sur la vie privée et les communications électroniques, sur l'information sur l'environnement; voir ci-dessous pour les statistiques combinées du nombre de demandes écrites et de plaintes).
Plaintes émanant des personnes concernées	26 227 affaires relatives à la protection des données ont été reçues (y compris les demandes par écrit et les affaires en matière de vie privée et de communications électroniques). 29 685 affaires relatives à la protection des données ont été clôturées.

Conseils sollicités par le Parlement ou le gouvernement	L'année 2010 a été relativement calme en raison des élections législatives et de la mise en place d'un nouveau gouvernement de coalition. Nous avons conseillé le gouvernement/Parlement dans les matières suivantes: • le projet de loi sur les documents d'identité; • le piratage des téléphones (à la commission des affaires intérieures); • la gouvernance informatique (à la commission de l'administration publique); • la mise à jour de notre rapport sur la société de surveillance (à la commission des affaires intérieures); • notre surveillance d'une base de données de l'Agence de lutte contre la grande criminalité organisée (à la commission de la Chambre des Lords); et • les risques en matière de vie privée associés à la cartographie de la criminalité (au ministère de l'intérieur et à la police).
Autres renseignements relatifs aux activités générales	3 règles d'entreprise contraignantes approuvées
Activités d'inspection	
Contrôles, enquêtes	Rédaction de 26 rapports d'audit à la suite de contrôles réalisés dans des organismes publics et privés. Huit d'entre eux ont été effectués dans des organisations ayant donné leur accord pour être inspectées dans le cadre d'enquêtes sur des violations de la loi. Cette année, 97 % des recommandations formulées dans les rapports ont été approuvées par les organisations. Lors d'audits ultérieurs de vérification, 92 % de nos recommandations avaient été totalement ou partiellement appliquées. Les domaines qui nécessitent régulièrement des améliorations sont, notamment: l'information du personnel quant à la politique de protection des données, la formation du personnel aux aspects pertinents en matière de protection des données et, enfin, la sécurité générale, entre autres l'insuffisance du codage sur les dispositifs portables, le partage des mots de passe et le manque de mesures physiques de sécurité de base, par exemple la mise à disposition d'armoires à verrou.
Activités de sanction	
Sanctions	Entreprises: 46 Poursuites: 5 Amendes au civil: 4
Amendes	Amendes au civil: 4 amendes d'un montant compris entre 60 000 et 100 000 GBP (total de 310 000 GBP), 3 dans le secteur public, 1 dans le privé. Ces amendes sont imposées par le Bureau du Commissaire à l'information.
DPD	
Chiffres relatifs aux DPD	s.o.

B. Informations sur la jurisprudence

Conservation des casiers judiciaires:

En 2008, le commissaire a mis en demeure cinq forces de police de supprimer d'anciennes condamnations du fichier informatique national de la police (PNC). Cette mesure a été prise au terme d'une enquête, effectuée sur la base de plaintes envoyées par cinq individus qui avaient été condamnés ou qui avaient reçu un avertissement de la part de la police à une seule reprise et qui, ultérieurement, n'avaient plus été condamnés pour la moindre infraction.

Dans chaque affaire, le commissaire a écrit à la force de police concernée et a demandé à ce que les données soient soit retirées du PNC, soit «circonscrites», c'est-à-dire conservées dans le PNC mais rendues uniquement accessibles aux utilisateurs de la police. Chaque force de police a accepté de réduire l'accessibilité des informations, mais pas de les supprimer.

En conséquence, le commissaire a mis en demeure les cinq chefs des forces de police correspondantes, exigeant dans chacun des cas la suppression des informations relatives à la condamnation de l'individu concerné du PNC.

Les chefs de police ont fait appel de la décision du commissaire devant le tribunal de l'information, dans le but d'être autorisés à conserver les informations pertinentes relatives aux condamnations sur le PNC.

Le tribunal a confirmé les mises en demeure adressées par le commissaire et a exigé des chefs de police qu'ils suppriment les données concernées sur les cinq individus.

Les cinq responsables de la police ont reçu l'autorisation d'introduire un recours devant la cour d'appel, qui a jugé qu'il n'était pas nécessaire pour les forces de police de supprimer les informations qu'elles détenaient et que la conservation de ces données n'enfreignait pas la loi sur la protection des données. L'arrêt peut être consulté à l'adresse www.bailii.org/ew/cases/EWCA/Civ/2009/1079.html. Nous nous sommes ensuite tournés vers la Cour suprême, afin d'obtenir une autorisation d'interjeter appel de ce dernier jugement, mais notre demande a été rejetée en 2010.

À nos yeux, ce jugement soulève d'importantes questions, non seulement pour ces personnes et pour les nombreuses autres dont des informations anciennes et de peu d'importance relatives à des condamnations sont détenues, mais aussi au regard de l'interprétation pratique de la loi sur la protection des données. Cette décision pose également de sérieuses questions sur l'applicabilité de l'article 8 de la Convention européenne des droits de l'homme en matière de données relatives à des condamnations détenues par la police.

Chapitre Trois

Union Européenne et Activités Communautaires

3. Union Européenne et Activités Communautaires

3.1. COMMISSION EUROPÉENNE

Édition 2010 de la Journée européenne de la protection des données[8], le 28 janvier 2010

Au sein de l'UE, la protection des données à caractère personnel est un droit fondamental. Selon la Charte des droits fondamentaux de l'Union européenne, **«toute personne a droit à la protection des données à caractère personnel la concernant»**.

Le 28 janvier 2010, la Commission et les États membres du Conseil de l'Europe ont célébré pour la quatrième fois la Journée de la protection des données.

Cette date marque l'anniversaire de la convention n° 108 du Conseil de l'Europe, le premier instrument international juridiquement contraignant de protection des données.

Cette journée offre l'occasion aux citoyens européens de s'informer davantage sur la protection des données à caractère personnel et sur leurs droits et devoirs dans ce domaine.

À cette occasion, la Commission européenne a organisé un atelier à huis clos sur le thème «Comment les personnes concernées sont-elles informées au sujet du traitement de leurs données et de l'exercice de leurs droits?». Les interventions y ont porté plus précisément sur l'information et les droits des personnes concernées dans le secteur médical, sur la manière de faire des personnes concernées les principaux acteurs de la défense de leur propre vie privée, sur le respect de la vie privée et la protection des données sur le lieu de travail, ainsi que sur la pratique de la Commission européenne concernant l'information et les droits des personnes concernées et, enfin, la protection des données et les droits à la vie privée dans le secteur des communications électroniques.

Consultation des parties prenantes: réunion sur le réexamen du cadre législatif de l'UE relatif à la protection des données, le 1er juillet 2010[9]

Dans le prolongement de la consultation publique organisée en 2009 sur le réexamen du cadre législatif de l'UE relatif à la protection des données, la Commission a préparé une série de réunions de consultation ciblées avec certaines des principales parties prenantes.

L'objectif de ces séances était de **consulter les parties prenantes du secteur non public sur un éventail de questions liées aux règles existantes en matière de protection des données, d'identifier les problèmes et de débattre des solutions éventuelles.**

La Commission a rédigé une base de discussions comprenant une série de questions. Ce document est divisé en différentes thématiques et a pour objectif de guider et de structurer les discussions lors des rencontres.

Consultation publique sur le futur accord international entre l'UE et les États-Unis[10]

Dans le cadre de l'élaboration de ses politiques et de ses propositions législatives, la Commission européenne sonde largement les citoyens de l'UE et les parties prenantes grâce à des consultations publiques. Dans cette optique, les

8 http://ec.europa.eu/justice/newsroom/data-protection/events/100128_en.htm

9 http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm

10 http://ec.europa.eu/justice/newsroom/data-protection/opinion/100128_en.htm

citoyens ont été invités à se prononcer, du 28 janvier 2010 au 12 mars 2010, sur le futur accord international entre l'Union européenne (UE) et les États-Unis concernant la protection des données à caractère personnel et le partage d'informations à des fins d'application de la loi. L'objectif de cette consultation était de réunir des avis dans la perspective dudit accord international.

Soixante-quatre réponses ont été reçues dans le cadre de cette consultation publique, de la part de citoyens, d'organisations (enregistrées ou non) et de pouvoirs publics.

3.2. COUR DE JUSTICE DE L'UNION EUROPÉENNE

Arrêt de la Cour (grande chambre) du 9 mars 2010 – Commission européenne/République fédérale d'Allemagne (affaire C-518/07)[11]

La Commission a ouvert une procédure en manquement à l'encontre de l'Allemagne, qui s'est conclue par l'arrêt de la Cour de justice de l'UE du 9 mars 2010 (C-518/07). La Cour a estimé que l'Allemagne avait manqué à ses obligations en vertu de l'article 28 de la directive 95/46/CE et qu'en plaçant sous la tutelle de l'État les autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel par les organismes non publics et les entreprises de droit public prenant part à la concurrence sur le marché, l'Allemagne n'avait pas transposé correctement l'exigence selon laquelle ces autorités exercent leur mission «en toute indépendance».

La Cour a souligné que les autorités de contrôle devaient agir de manière objective et impartiale, et, dès lors, demeurer à l'abri de toute influence extérieure, directe ou indirecte, exercée par toute autorité publique et non seulement par les organismes contrôlés. Elle a également précisé que le seul risque que les autorités de tutelle puissent exercer une influence politique sur les décisions des autorités de contrôle suffisait pour entraver l'exercice indépendant des fonctions de celles-ci.

3.3. CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

A) *Résumé des activités et actualités*

Au niveau de l'Union européenne (UE), l'année 2010 a, tant dans le cadre de l'élaboration des politiques que dans la poursuite de grandes tendances, marqué une nouvelle étape vers une meilleure protection des données à caractère personnel. Tout d'abord, les conséquences du traité de Lisbonne se font de plus en plus ressentir. En fournissant une base juridique solide pour une protection exhaustive des données à caractère personnel dans tous les domaines d'action de l'UE, celui-ci a résolument placé la protection des données au cœur de l'agenda politique européen. Ensuite, le réexamen en cours du cadre juridique de l'UE pour la protection des données suscite des attentes élevées, notamment au regard de l'importance croissante de la protection des données sur la scène internationale. Enfin, le programme de Stockholm et la stratégie numérique de l'UE revêtent l'un comme l'autre une importance considérable pour la protection de la vie privée et des données.

Le besoin d'intensifier les efforts afin d'assurer une protection effective des données peut être observé dans les activités du CEPD en 2010. En ce qui concerne son rôle de supervision, les principaux faits marquants ont été les suivants:

- un changement de direction fondamental relatif à la mise en application du règlement sur la protection des données dans l'administration européenne, en vue de garantir une approche plus ferme en la matière. La nouvelle politique énonce plusieurs critères visant à garantir une application proactive, cohérente et transparente des pouvoirs d'exécution du CEPD;

[11] JO C 113 du 01.05.2010, p.3, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:113:0003:0004:FR:PDF.

- une extension du champ d'application de la supervision du CEPD qui, depuis l'entrée en vigueur du traité de Lisbonne, s'applique à toutes les institutions et à tous les organes de l'UE, y compris dans des domaines situés en dehors de l'ancien droit communautaire;

- l'adoption de 55 avis sur la notification de contrôles préalables concernant des opérations de traitement de données à caractère personnel dans l'administration de l'UE, certains concernant des activités fondamentales, telles que le système d'alerte précoce et de réaction pour la prévention et le contrôle des maladies transmissibles, et d'autres concernant des procédures administratives de routine, comme l'évaluation du personnel, le recrutement et les promotions; et

- une augmentation de la complexité des plaintes. En 2010, 94 plaintes ont été reçues, dont environ deux tiers étaient irrecevables, car relevant du niveau national. Les plaintes recevables concernaient principalement l'accès aux données, ainsi que la rectification, l'utilisation abusive, ainsi que des opérations de collecte excessive et de suppression des données. Dans 11 affaires, le CEPD a conclu que les règles relatives à la protection des données avaient été enfreintes.

Dans le cadre de son **rôle consultatif**, le CEPD a accordé une importance particulière:

- à la modernisation du cadre juridique de l'UE pour la protection des données: le CEPD a systématiquement recommandé une approche ambitieuse en vue de l'élaboration d'un cadre moderne complet pour la protection des données, qui couvrirait tous les domaines d'action de l'UE et assurerait une protection efficace dans la pratique;

- au programme de Stockholm et à la stratégie numérique de l'UE: ces deux programmes clés ont une grande importance pour la protection des données et sont donc surveillés de près par le CEPD dans le cadre de son rôle consultatif. Par ailleurs, ces politiques montrent que la protection des données est un élément essentiel contribuant à la légitimité et à l'efficacité des mesures dans les domaines concernés; et

- à un nombre record de 19 avis législatifs: en 2010, des avis ont été adoptés sur divers sujets, y compris sur des questions essentielles relatives au programme de sécurité intérieure de l'UE, à la stratégie de l'UE visant à lutter contre le terrorisme, à une approche globale pour les transferts des données PNR vers les pays tiers, à la gestion de l'information dans l'espace de liberté, de sécurité et de justice, au principe de «respect de la vie privée dès la conception» ancré dans la stratégie numérique et, enfin, à l'accord commercial anticontrefaçon (ACAC).

Dans le **domaine de la coopération**, le CEPD a poursuivi son étroite collaboration avec les autorités créées dans le but d'exercer un contrôle conjoint des systèmes informatiques à grande échelle de l'UE. Un important travail a notamment été effectué en matière de «contrôle coordonné» du système Eurodac et du système d'information des douanes, pour lesquels les responsabilités de surveillance sont partagées avec les autorités nationales compétentes. Conjointement avec l'institut universitaire européen de Florence, le CEPD a aussi organisé un atelier relatif à la protection des données dans les organisations internationales, qui a permis d'aborder les multiples défis rencontrés par ces organisations lorsqu'elles tentent d'assurer un bon niveau de protection des données sans base juridique claire.

Organisation	Contrôleur européen de la protection des données
Président et/ou collège	Peter Hustinx, contrôleur Giovanni Buttarelli, contrôleur adjoint
Budget	7 104 351 EUR

Personnel	38 fonctionnaires
Activités générales	
Décisions, avis, recommandations	19 avis législatifs adoptés sur divers sujets, y compris sur des questions essentielles telles que le programme de sécurité intérieure de l'UE, la stratégie de l'UE visant à lutter contre le terrorisme, une approche globale pour les transferts des données PNR vers les pays tiers, la gestion de l'information dans l'espace de liberté, de sécurité et de justice, au principe de «respect de la vie privée dès la conception» ancré dans la stratégie numérique et, enfin, à l'accord commercial anticontrefaçon (ACAC). 7 séries d'observations formelles concernant, entre autres, la révision du règlement FRONTEX, l'internet ouvert et la neutralité du web, le système d'information du marché intérieur, les scanneurs de sécurité et les accords internationaux d'échange de données.
Notifications	89 notifications d'opérations de traitement présentant des risques particuliers envoyées pour examen préalable par des délégués à la protection des données auprès des institutions et organes de l'UE.
Examens préalables	55 avis sur la notification de contrôles préalables concernant, notamment, des données relatives à la santé, l'évaluation du personnel, le recrutement, la gestion du temps, les enquêtes de sécurité, les enregistrements téléphoniques et les outils de performance.
Demandes émanant des personnes concernées	141 demandes écrites d'informations ou de conseils reçues du public.
Plaintes émanant des personnes concernées	94 plaintes reçues, dont 25 recevables. Les plaintes avaient principalement pour objet des atteintes à la confidentialité des données, ainsi que des opérations de collecte excessive des données et d'exploitation illégale des données par le responsable. Dans 10 cas, le CEPD n'a constaté aucune violation des règles de protection des données. Dans 11 cas, le CEPD a déclaré l'opération non conforme aux règles de protection des données.
Conseils sollicités par le Parlement ou le gouvernement	Parmi les 19 avis législatifs évoqués ci-dessus, 11 ont été exprimés à la demande de la Commission européenne.
Autres renseignements relatifs aux activités générales	35 consultations sur des mesures administratives liées au traitement de données à caractère personnel dans l'administration de l'UE. Des conseils ont été prodigués dans un éventail de matières juridiques relatives au traitement des données à caractère personnel par les institutions et les organes de l'UE.

Activités d'inspection	
Contrôles, enquêtes	Contrôles sur place menés dans une institution de l'UE. Suivi systématique des inspections précédentes, surveillance ciblée et exercices de rapport, comprenant notamment des visites sur place.
Activités de sanction	
Sanctions	s.o.
Amendes	Adoption d'une nouvelle politique de conformité et de mise en application afin de garantir une approche ferme en matière de respect des règles. La nouvelle politique énonce plusieurs critères visant à assurer une application proactive, cohérente et transparente des pouvoirs d'exécution du CEPD.
DPD	
Chiffres relatifs aux DPD	47 DPD dans les institutions et organes de l'UE.

B. Informations sur la jurisprudence

Accès du public aux documents contenant des données à caractère personnel

Depuis qu'il est actif, le CEPD traite des questions relatives aux relations, parfois complexes, entre les règles de l'UE sur l'accès du public aux documents et celles liées à la protection des données. Le CEPD a traité ces questions en apportant, pour commencer, des conseils aux institutions de l'UE, notamment par la publication en 2005 d'un document d'information.

Le CEPD a également défendu sa position en intervenant dans l'importante affaire *Bavarian Lager c. Commission*, qui portait sur une demande d'accès du public au procès-verbal d'une réunion de la Commission, y compris au nom des participants. L'accès à ces noms a été refusé en raison des règles de protection des données. Le tribunal a approuvé l'avis défendu par le CEPD, mais la Cour, saisie de l'appel, a annulé cette décision dans son arrêt du 29 juin 2010 et a fourni une interprétation différente des règles de l'UE concernées.

Une partie de l'analyse présentée dans le document d'information de 2005 n'était plus valable à la lumière de la décision de la Cour. Le CEPD a donc préparé un document complémentaire dans lequel il insiste sur la nécessité d'adopter une **approche anticipative** de la question. En d'autres termes, les institutions sont invitées à préciser clairement aux personnes concernées, avant ou au plus tard au moment de la collecte de leurs données à caractère personnel, la mesure dans laquelle le traitement de ces données inclut ou pourrait inclure une divulgation des informations au public. Le CEPD a considéré que les institutions étaient tenues de se plier à cette approche pour une question de bonnes pratiques.

Plusieurs autres affaires en cours, suspendues en attendant que soit tranchée l'affaire *Bavarian Lager*, ont été relancées après l'arrêt de la Cour de juin 2010. Le CEPD est intervenu dans plusieurs d'entre elles. Si cela se révélait pertinent, il en a profité pour exprimer son point de vue sur l'application de l'arrêt rendu par la Cour dans l'affaire *Bavarian Lager* à ces autres cas. Le CEPD a également donné son avis dans le cadre d'une nouvelle affaire intentée dans le même domaine.

Par ailleurs, l'arrêt rendu dans le cadre de l'affaire *Bavarian Lager* a entraîné un non-lieu de la première affaire introduite auprès du tribunal à l'encontre du CEPD.

Autres affaires en justice

Le CEPD est aussi intervenu dans un autre jugement rendu par le tribunal de la fonction publique le 15 juin 2010, dans l'affaire Pachtitis c. Commission. Cette affaire portait entre autre sur le refus de la Commission de fournir au candidat l'accès aux questions d'un test de niveau auquel il avait participé. Puisque les règles relatives à la protection des données ont été invoquées à cet égard et qu'une question intéressante a été soulevée sur la portée du droit d'accès à ses propres données à caractère personnel, le CEPD est intervenu. Il s'est fait entendre aux côtés du requérant, qui a remporté l'affaire, sans toutefois que ne soit réglé le problème relatif à la protection des données. En conséquence, le CEPD s'est retiré de l'appel ultérieur introduit par la Commission auprès du tribunal.

En juillet 2010, le tribunal de la fonction publique a proposé au CEPD d'intervenir dans une affaire concernant le transfert de données médicales entre deux institutions de l'UE. C'était la première fois que le CEPD était invité par ce Ttribunal à contribuer à une affaire. Le CEPD a accepté l'invitation et a préparé à cette occasion une déclaration précisant les dispositions applicables du règlement sur la protection des données.

Chapitre quatre

Principaux Développements dans les pays de l'EEE

4. Principaux Développements dans les pays de l'EEE

ISLANDE

A. Résumé des activités et actualités

L'une des principales questions traitées en 2010 a été un avant-projet de loi visant à modifier la législation en matière de recherche scientifique. La proposition n'a pas encore été présentée au Parlement, mais la DPA islandaise a donné son avis sur certains de ses points clés. Conformément à la législation actuelle, l'accès à des dossiers médicaux à des fins scientifiques doit être approuvé par la DPA. Toutefois, d'après les termes de l'avant-projet de loi, l'approbation de la DPA ne sera plus nécessaire. Au lieu de cette approbation, des commissions bioéthiques (la commission nationale de bioéthique dans la majorité des cas, mais, parfois, des commissions faisant partie des plus grands établissements de soins de santé) évalueront les questions relatives à la protection des données lorsqu'elles émettront des autorisations pour des projets de recherche scientifique. La DPA s'y est opposée en soulignant, entre autres, qu'une évaluation indépendante des exigences légales d'accès aux dossiers médicaux était nécessaire.

Une autre question importante a été posée par la mise en œuvre d'une nouvelle législation sur les informations relatives aux patients, à savoir la loi nº 55/2009 sur les dossiers médicaux. En vertu de cette loi, plusieurs établissements de soins de santé peuvent utiliser le même système de dossiers médicaux électroniques, moyennant le feu vert du ministre des affaires sociales et la confirmation de la DPA que la sécurité des données à caractère personnel est assurée de manière satisfaisante. La DPA a formulé une telle confirmation en 2010, pour un système de dossiers médicaux électroniques commun à des établissements de soins de santé dans le nord de l'Islande. Dans sa décision, la DPA a précisé que la mise en place de ce système doit s'accompagner, entre autres, d'un journal de tous les accès et d'un contrôle interne approprié. De plus, la DPA a souligné que les dispositions de la loi sur les dossiers médicaux relatives au droit des patients à empêcher l'accès à leurs données devaient faire l'objet d'une mise en œuvre suffisante.

En Islande, chaque habitant reçoit un numéro personnel d'identité qui est unique. Comme le précise la loi sur la protection des données, ce numéro ne peut être utilisé que lorsqu'il est nécessaire de garantir l'identification exacte d'un individu. En 2010, la DPA a eu à connaître de plusieurs affaires portant sur ce numéro d'identification et, notamment, sur son utilisation par des institutions financières. D'après la législation sur la prévention du blanchiment de capitaux et du financement du terrorisme, l'identification correcte des clients est l'une des méthodes permettant d'éviter ce type d'activités. Cependant, conformément à la directive 2005/60/CE, l'application de certaines mesures sévères dans ce domaine n'est obligatoire que si les transactions dépassent un certain montant. Or la DPA a reçu deux plaintes selon lesquelles il aurait été demandé à des clients de fournir leur numéro personnel d'identité lors de transactions portant sur des montants peu importants, notamment lors du règlement de factures et de l'échange de devises étrangères en devise islandaise. La DPA a conclu que, dans ce cas, demander le numéro personnel d'identité constituait une violation de la règle susmentionnée de la loi sur la protection des données. Les institutions financières concernées ont reçu l'ordre de modifier leurs procédures. Par la suite, il s'est avéré que l'une d'entre elles ne s'était pas conformée à cette décision; la DPA a donc décidé d'imposer des amendes journalières si les procédures n'étaient pas transformées. À la suite de cette décision, la DPA a reçu des éclaircissements sur les améliorations apportées par l'institution financière, rendant des amendes journalières inutiles.

Une autre question intéressante concerne la diffusion d'images recueillies par des caméras de surveillance afin de montrer au personnel de magasins et de supermarchés des vols présumés dans les établissements où ils travaillent. La DPA a reçu deux plaintes au sujet de la diffusion de ce type d'images dans d'importantes chaînes de magasins. Dans les deux cas, les plaignants soupçonnaient que leurs photographies étaient conservées dans les magasins afin d'avertir le personnel. La DPA n'a pas trouvé de preuve confirmant que des photographies des individus en question étaient utilisées de la sorte, mais il s'est avéré que la chaîne de magasins en question possédait une vaste collection de photographies d'individus utilisée pour mettre en garde son personnel. Par ailleurs, aucune information n'avait été communiquée à ces individus sur l'utilisation de leur image. La DPA a indiqué que ce procédé pouvait mener à la désignation injuste de certains individus comme délinquants et que le traitement était dépourvu de base juridique. En conséquence, elle a conclu que le traitement était illégal et a ordonné qu'il y soit mis un terme.

En 2010, un certain nombre d'actes juridiques incluant des dispositions sur le traitement des données à caractère personnel ont été adoptés, y compris: la loi nº 12/2010 sur un mandat d'arrêt nordique concernant, entre autres, son lien avec le mandat d'arrêt européen et la coopération au titre de Schengen; la loi nº 42/2010 relative aux cartes d'identité sur le lieu de travail et au contrôle au travail, qui permet aux organisations professionnelles et patronales de conclure des accords sur des cartes identifiant les travailleurs dans des secteurs sélectionnés et de faciliter ainsi la surveillance des règles relatives au marché du travail; la loi nº 78/2010 modifiant les actes juridiques relatifs aux opérations de change et complétant notamment la loi nº 87/1992 sur les opérations de change de manière à permettre à la Banque nationale de collecter des informations détaillées sur les opérations en devises étrangères; ainsi que les lois nº 100 et 101/2010 sur le médiateur de dettes et la réduction des dettes comprenant des dispositions relatives, entre autres, a) aux pouvoirs du médiateur de collecter des données relatives aux individus demandant son assistance dans le cadre d'un accord avec les créanciers sur la réduction des dettes, b) au consentement des individus pour la collecte de données, et c) au transfert de données à des créanciers.

Organisation	
Président et/ou collège	Sigrún Jóhannesdóttir, commissaire; Páll Hreinsson, président du conseil d'administration
Budget	66 400 000 ISK, soit environ 415 000 EUR
Personnel	4 conseillers juridiques, 1 secrétaire
Activités générales	
Décisions, avis, recommandations	
Notifications	Environ 70
Examens préalables	407
Demandes émanant des personnes concernées	149 autorisations de traitement accordées
Plaintes émanant des personnes concernées	Environ 300
Conseils sollicités par le Parlement ou le gouvernement	135
Autres renseignements relatifs aux activités générales	Environ 50
Activités d'inspection	Au total, 1 221 nouveaux dossiers enregistrés en 2010
Contrôles, enquêtes	
Activités de sanction	25
Sanctions	
Amendes	À l'exception des amendes journalières émises pour chaque jour où ses décisions ne sont pas appliquées, la DPA ne possède aucun pouvoir de sanction.

DPD	Dans un dossier, la DPA a décidé d'imposer des amendes journalières si certaines procédures n'étaient pas modifiées, mais elle a reçu des explications sur des améliorations qui rendaient les amendes superflues.
Chiffres relatifs aux DPD	
Président et/ou collège	s.o.

B. Informations sur la jurisprudence

Le 21 octobre 2010, la Cour suprême d'Islande a rendu un arrêt (affaire nº 13/2010) relatif à l'utilisation présumée par un employeur de la correspondance électronique privée d'un ancien salarié, envoyée à partir de l'adresse de courrier électronique privée de ce dernier. L'affaire concernait un accord sur des paiements à l'ancien salarié à la suite de son licenciement. L'employeur a indiqué que l'ancien salarié avait violé l'accord en envisageant de postuler pour un concurrent et a donc arrêté de verser les paiements. L'ancien salarié a ensuite engagé des poursuites à l'encontre de l'employeur, qui a alors produit la correspondance électronique évoquée ci-dessus comme preuve de la malveillance de son ancien travailleur.

Toutefois, la Cour suprême est arrivée à la conclusion que l'on ne pouvait pas vérifier que la correspondance électronique s'était réellement déroulée entre l'ancien salarié et le concurrent. À la lumière de cette constatation et d'autres circonstances, elle a approuvé la requête de l'ancien salarié d'être payé conformément au contrat.

Dans cette affaire, aucune requête n'a été formulée quant à l'éventuelle illégalité de l'accès à ladite correspondance. Dès lors, aucune décision n'a été rendue à cet égard par la cour dans son arrêt. Ce cas soulève toutefois des questions sur la sécurité de la correspondance électronique privée.

LIECHTENSTEIN

A. Résumé des activités et actualités

Conservation de données

Comme déjà annoncé l'an dernier, le Liechtenstein a inscrit dès 2006 la conservation des données de circulation dans la loi sur la communication (*KomG*)[12], sans qu'il n'existe une obligation de transposition de la directive 2006/24/CE[13]. L'Office pour la protection des données (DSS) était opposé à l'instauration de cette conservation de données au Liechtenstein. Toujours est-il que le gouvernement et la Diète (parlement) ont opté pour une «approche proche du citoyen et respectueuse des droits fondamentaux en matière de protection des données» et le DSS s'est vu attribuer par la *KomG* un pouvoir de contrôle explicite[14]. La mise au point d'un système de contrôle correspondant a donc commencé. La doctrine en vigueur au Liechtenstein qualifie la collecte aux fins de stockage sans finalité précise des données de circulation, en dépit des critères particulièrement sévères régissant l'accès à ces données, de «*problématique du point de vue des libertés fondamentales. Sa qualification éventuelle d'anticonstitutionnelle par la Cour d'État devrait néanmoins dépendre en grande partie de la future jurisprudence étrangère en la matière*»[15]. Reste à voir si la Cour d'État aura l'occasion de prendre position sur cette question.

Google Street View

L'an dernier, le DSS a entretenu des contacts intensifs avec Google dans le cadre du lancement du service *Street View*, notamment au sujet de conditions concrètes d'encadrement des voyages de reconnaissance des voitures de Google au Liechtenstein. Le DSS s'est ici inspiré de ce qui se faisait ailleurs en Europe, notamment au sein du groupe de travail «Article 29» sur la protection des données et plus particulièrement au Luxembourg, en Autriche, en Allemagne, en Grèce, mais également en Suisse. Dans ce cadre, il a également fallu tenir compte comme il se devait d'un communiqué gouvernemental paru à ce sujet. Le DSS a exigé diverses mesures, en particulier concernant l'information de la population quant au moment et à l'itinéraire précis des voyages, ainsi qu'au sujet de la diffusion des images sur l'internet. La question du floutage des visages et des plaques d'immatriculation a été abordée, car lors de la phase initiale de publication, de nombreux visages et plaques d'immatriculation étaient facilement reconnaissables et donc identifiables. À la connaissance du DSS, aucune prise de vue de rues dans le cadre du service *Google Street View* n'avait encore lieu au Liechtenstein à la fin de l'année 2010.

Publicité

Dans le cadre de la Journée européenne de la protection des données, le 28 janvier, le DSS a organisé, avec le concours de l'institut d'informatique de gestion de l'université du Liechtenstein, une manifestation publique axée sur le thème des moteurs de recherche sur l'internet, intitulée «Une plongée dans le monde de Google & Co: chasseurs d'informations et collecteurs de données».

Afin de toucher une part aussi large que possible de la population, le DSS a fait appel à plusieurs canaux. Outre les diverses manifestations, formations et publications, ainsi que le site web, le rapport d'activités[16] annuel fait lui aussi partie des principaux outils d'information. Le site web du DSS[17] constitue pour sa part un outil d'information essentiel et économique. Le nombre de visites démontre l'intérêt porté à cette offre, qui fait par conséquent l'objet d'améliorations et d'enrichissements permanents. Les visiteurs y trouvent, entre autres outils, des tests à effectuer eux-mêmes, ainsi que différentes aides liées au thème de la protection des données.

---

12 Dans le cadre de la dernière révision de la loi sur la communication, LGBl. 2006 n° 91.

13 La directive 2006/24/CE n'étant pas (encore) couverte par l'accord EEE, il n'existe aucune obligation de transposition.

14 Art. 52, *KomG*. Voir également le rapport d'activités 2010 du DSS, point 1.3, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

15 Voir Hoch, Hilmar, "Die Regelung des staatlichen Zugriffs auf Fernmeldedaten im Kommunikationsgesetz aus grundrechtlicher Sich", LJZ, n° 4/2009, p. 103, http://www.juristenzeitung.li/papers/showpdf/LJZ_2009_04.pdf.

16 http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

17 www.dss.llv.li.

Organisation	
Président et/ou collège	Dr Philipp Mittelberger
Budget	470 000 EUR
Personnel	2,2 ETP de juristes; 1,0 ETP d'agent technique et 0,8 ETP d'agent administratif
Activités générales	
Décisions, avis, recommandations	26 avis relatifs à des projets de loi[18] 23 autorisations relatives à des installations de vidéosurveillance
Notifications	s. o.; au total 542 collectes de données enregistrées
Examens préalables	s.o.
Demandes émanant des personnes concernées	85
Plaintes émanant des personnes concernées	s.o.
Conseils sollicités par le Parlement ou le gouvernement	Communiqué[19] gouvernemental relatif à *Google Street View*
Autres renseignements relatifs aux activités générales	Le nombre de questions reçues a progressé de 20 %; 523 demandes ont été reçues contre 431 en 2009[20].
Activités d'inspection	
Contrôles, enquêtes	s. o.; contrôles en préparation
Activités de sanction	
Sanctions	s. o.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Autorisations liées aux installations de vidéosurveillance

[18] Voir aussi le rapport d'activités 2010 du DSS, chapitre 3, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

[19] En vertu de l'article 30, par. 1, de la loi sur la protection des données (*DSG*).

[20] Voir les statistiques reprises dans le rapport d'activités 2010 du DSS, chapitre IV, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

Depuis le 1er juillet 2009, le recours à la vidéosurveillance dans l'espace public est soumis à l'octroi d'une autorisation délivrée par le DSS[21].

Vidéosurveillance à grande échelle: à la fin de l'année 2009, la commune de Vaduz a sollicité auprès du DSS une autorisation portant sur une installation de vidéosurveillance existante dans la **ville de Vaduz**. Cette demande portait sur 15 caméras couleurs destinées à surveiller une superficie d'environ 3000 m² grâce à un champ de vision fixe et une exploitation permanente, sauf du lundi au vendredi de 10 heures à 18 heures, permettant la transmission d'images en temps réel, leur enregistrement et d'autres possibilités de traitement, ainsi qu'une durée de conservation de quatre jours. Le DSS avait alors refusé cette demande *ex officio* en justifiant essentiellement sa décision par le fait que l'installation de vidéosurveillance concernée ne s'avérait pas nécessaire, faute de preuves suffisantes, et s'avérait donc disproportionnée. Ultérieurement, à la suite d'une visite du DSS sur place, l'angle de vision de plusieurs caméras a été modifié, de même que les heures d'enregistrement de certaines autres; d'autres encore ont été simplement déconnectés et mises sous scellés.

La commune de Vaduz a introduit un recours contre la décision du DSS auprès de la Commission de la protection des données (DSK). Dans sa décision[22] de décembre dernier, celle-ci confirme globalement l'avis du DSS mais autorise néanmoins quelques caméras contre l'avis du DSS. La DSK a par exemple justifié l'autorisation d'installation de deux caméras dans la zone d'accès à la maison communale en invoquant le fait que ce bâtiment public faisait également souvent office de lieu de réunion et de manifestation et que des visiteurs autochtones ou non, plus ou moins célèbres, circulaient devant cet édifice. Selon l'expérience commune, cet endroit présentait donc un risque potentiel accru et il n'était pas nécessaire, de l'avis de la DSK, d'attendre des cas concrets, par exemple une attaque visant une personne publique exposée, pour s'en convaincre. Le contrôle des autorisations d'accès, de même que la garantie et l'amélioration de la sécurité des visiteurs de la maison communale rendaient donc nécessaire une vidéosurveillance, celle-ci pouvant dès lors être autorisée. Toujours selon la DSK, il n'était pas davantage nécessaire d'attendre un cas concret pour utiliser la caméra demandée au niveau de la gare routière, dans la mesure où l'expérience commune démontre que ces endroits «font souvent l'objet de rassemblements plus ou moins importants, souvent confus par nature, de personnes de diverses nationalités et représentent donc, en vertu de l'expérience, un risque accru pour la sécurité».

En ce qui concerne les caméras débranchées et placées sous scellés, la DSK s'est ralliée à la lecture juridique du DSS et a confirmé que ces caméras devaient être considérées comme constituant une ingérence disproportionnée dans la vie privée et devaient par conséquent être démontées. Leur présence pourrait donner aux passants la fausse impression d'être surveillés, ce qui est contraire au principe de bonne foi. Il en va de même pour les modèles factices.

21 Voir également la contribution du Liechtenstein au 13e rapport annuel du groupe de travail «Article 29» sur la protection des données ainsi que, pour plus de détails, le rapport d'activités 2009 du DSS, chapitre 1.5, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2009.pdf.

22 DSK 2010/2; la décision complète ainsi que les autres décisions prises par la DSK peuvent être consultées à l'adresse suivante: http://www.llv.li/amtsstellen/llv-dss-datenschutzkommission/llv-dss-entscheiddatenbank-dsk.htm.

C. Autres informations importantes

Le DSS ne se veut pas uniquement un point de contact réactif: il envisage également sa mission de manière active. C'est dans cette optique qu'il a incité le gouvernement à commander une étude[23] portant sur les flux de données dans le secteur des prestations sociales, ce qui a également été abordé et confirmé lors des débats à la Diète portant sur le rapport d'activités 2010 du DSS. Cette demande se fondait sur la réception d'une plainte portant sur l'échange de données de santé entre diverses autorités. Ce cas démontrait clairement à quel point il est difficile de conserver d'assurer le suivi du traitement des données à travers les méandres du système des prestations sociales et des échanges d'informations correspondants. Or les informations en question sont absolument indispensables aux fins de distribution et de revendication de prestations sociales. Selon le DSS, il faudrait mener en la matière une étude d'envergure nationale pour déterminer la nature des interconnexions entre les différents organismes payeurs et des informations échangées entre eux. Une telle étude devrait permettre de mieux comprendre les aspects juridiques liés à la protection des données et contribuer à une plus grande transparence. Cela permettrait aussi d'éviter d'éventuels abus et de réduire les doubles emplois.

Dans le cadre du groupe international sur la protection des données dans les télécommunications (*International Working Group on Data Protection in Telecommunications*, IWGDPT), le DSS a proposé une base de discussion[24] sur le thème de la protection des données sur les terminaux mobiles (téléphones mobiles, ordinateurs portables, etc.). La compacité et le faible poids de ces terminaux mobiles génèrent en effet des risques spécifiques en matière de sécurité des données, notamment des risques de manipulation, de perte ou de vol des données qu'ils contiennent.

[23] Dès 2005, le gouvernement avait commandé une étude portant sur le système de sécurité sociale du Liechtenstein (*Analyse Sozialstaat Liechtenstein*) sur la base de 25 prestations d'aide sociale. L'étude proposée pourrait s'en inspirer.

[24] http://www.datenschutz-berlin.de/attachments/724/WP_Mobile_Verarbeitung_und_Datensicherheit_final_clean_675_41_19.pdf?1292412668.

NORVÈGE

A. Résumé des activités et actualités

Le problème le plus important posé durant l'année a été le débat relatif à la directive sur la conservation des données. Sans surprise, la DPA norvégienne s'est opposée à la mise en œuvre de cette directive. Cela a entraîné le débat parlementaire le plus long depuis des années au sujet des données à caractère personnel.

Notre service juridique par téléphone et par courriel a géré plus de 7 300 appels et courriers électroniques, 17 % des demandes étant liées à la protection des données sur le lieu de travail.

En termes de sensibilisation, nous avons poursuivi notre campagne *Du bestemmer* («C'est à toi de décider»), traduite en plusieurs langues. Toute personne qui souhaiterait consulter ces documents peut simplement nous contacter.

Nous avons également contribué à la mise au point d'un test d'évaluation de la vulnérabilité au vol d'identité, qui est disponible sur notre site web. D'autres pays sont en train d'adopter ce test.

Le gouvernement s'est montré très actif dans le domaine de la santé. De nombreuses propositions ont été formulées sur la création de nouveaux registres médicaux, considérés par la DPA comme néfastes pour la protection des données à caractère personnel. Les individus ont très peu de contrôle, voire aucun, sur l'utilisation de leurs données à caractère personnel qui sont contenues dans ces registres.

En collaboration avec l'organisation Finance Norway, la DPA a produit une autorisation révisée pour toutes les banques basées en Norvège. Cela a représenté 251 examens préalables sur les 357 effectués au total.

Au cours de l'année, nous avons entamé un projet sur les sites de réseaux sociaux. Le rapport correspondant est disponible sur notre site web. Dans le cadre de ce travail, nous avons examiné quatre réseaux sociaux différents.

Organisation	Datatilsynet – Bureau norvégien de protection des données
Président et/ou collège	
Budget	32 000 000 NOK (environ 4 000 000 EUR)
Personnel	32 000 000 NOK (environ 4 000 000 EUR)
Activités générales	
Décisions, avis, recommandations	s.o.
Notifications	3 693
Examens préalables	357
Demandes émanant des personnes concernées	449 (nombre de dossiers écrits soumis par des particuliers)
Plaintes émanant des personnes concernées	Comprises dans le chiffre indiqué ci-dessus
Conseils sollicités par le Parlement ou le gouvernement	125
Autres renseignements relatifs aux activités générales	

Activités d'inspection	
Contrôles, enquêtes	135 • Emploi, système de contrôle de l'accès et accès à la boîte de courrier électronique: 11 • Enfants et jeunes: 6 • Systèmes de billetterie: 1 • Finance, paiements: 2 • Assurances, enfants et assurance-vie: 5 • Recherche médicale: 10 • Santé: 14 • Sports, dopage: 7 • Justice, transfert de données à caractère personnel: 7 • Vidéosurveillance, centres commerciaux: 44 • Services municipaux: 7 • Schengen (SIS): 2 • Sites de réseaux sociaux: 4 • Télécommunications: 5 • Éducation: 8 • Sécurité sociale: 2
Activités de sanction	
Sanctions	1 amende coercitive pour défaut de réponse à la DPA
Amendes	3 amendes imposées par la DPA pour un montant total de 120 000 NOK
DPD	
Chiffres relatifs aux DPD	173 DPD approuvés par la DPA
Pr. 30.04.2010	161
Pr. 31.08.2010	168
Pr. 31.12.2010	173

B. Informations sur la jurisprudence

Ces exemples d'affaires qui se sont déroulées en 2010 ont été choisis parmi d'autres en raison de l'intérêt qu'ils pourraient présenter pour nos collègues européens.

Surveillance à l'ambassade des États-Unis

Une chaîne de télévision nationale a révélé que les citoyens norvégiens étaient surveillés pour le compte de l'ambassade américaine. La DPA a entamé un dialogue avec les services de police qui ont enquêté sur l'affaire et qui ont enregistré notre opinion. L'autorité a estimé que l'ambassade devait limiter cette forme de collecte d'informations à une zone limitée autour de l'ambassade.

Partage de fichiers

La chambre d'appel a déclaré qu'un cabinet d'avocats devait être autorisé à poursuivre les individus partageant des fichiers, après le refus de la DPA d'octroyer l'autorisation correspondante. Il est probable qu'une législation sera bientôt mise en place dans ce domaine.

Contrôle de la fourniture de renseignements téléphoniques à la police par les sociétés de télécommunications

La DPA souhaitait vérifier quelles étaient les procédures en place entre les sociétés de télécommunications et la police. Nous souhaitions également inspecter les critères à remplir pour qu'un partage ait lieu. Il s'agit à la fois d'assurer la facilité d'obtention de ces données par la police et de nous préparer à ce que semble nous réserver l'avenir, à savoir l'arrivée de la directive sur la conservation des données.

Accès aux courriels des employés

En 2009, une série de nouvelles règles ont été adoptées concernant l'accès aux courriels des salariés. En 2010, la DPA a mis à l'amende deux sociétés qui avaient enfreint ces règles. Dans le premier cas, un employeur avait transféré tous les courriers électroniques appartenant à un salarié sur son adresse de courriel sans informer le travailleur concerné, puis il avait sauvegardé l'ensemble du contenu. Dans l'autre affaire, l'accès à un compte de courrier électronique d'un salarié malade avait été octroyé à un remplaçant, sans que le salarié ne soit prévenu. Donner ce type d'accès est interdit, même lorsque l'on prévient la personne concernée. Le règlement indique que les comptes de courrier électronique personnels doivent être considérés comme des données à caractère personnel.

Chapitre cinque

Membres et Observateurs du groupe de travail «Article 29» relatif à la protection des données

5. Membres et Observateurs du groupe de travail «Article 29» relatif à la protection des données

MEMBRES DU GROUE DE TRAVAIL ART. 29 RELATIF A LA PROTECTION DES DONNEES EN 2010

Autriche	Belgique
Mme Eva Souhrada-Kirchmayer (à partir de juillet 2010) Mme Waltraut Kotschy (jusqu'à juin 2010) Commission autrichienne de la protection des données (Datenschutzkommission) Hohenstaufengasse 31 - AT - 1014 Wien Tél: +43 1 531 15 / 2525 Fax: +43 1 531 15 / 2690 E-mail: dsk@dsk.gv.at Site web: http://www.dsk.gv.at/	M. Willem Debeuckelaere Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer) Rue Haute, 139 - BE - 1000 Bruxelles Tél: +32(0)2/213.85.40 Fax : +32(0)2/213.85.65 E-mail: commission@privacycommission.be Site web: http://www.privacycommission.be/
Bulgarie	**Chypre**
M. Krassimir Dimitrov Commission de protection des données à caractère personnel (Комисия за защита на личните данни) 15, Acad.Ivan Evstratiev Geshov blvd. BG- 1431 Sofia Tél: +359 2 915 3501 Fax: +359 2 915 3525 E-mail: kzld@government.bg, kzld@cpdp.bg Site web: http://www.cdpd.bg	Mme Panayiota Polychronidou Commissaire à la protection des données à caractère personnel (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str. Athanasia Court, 2nd floor - CY - 1082 Nicosia (P.O. Box 23378 - CY - 1682 Nicosia) Tél: +357 22 818 456 Fax: +357 22 304 565 E-mail: commissioner@dataprotection.gov.cy Site web: http://www.dataprotection.gov.cy
République tchèque	**Danemark**
M. Igor Nemec Bureau de la protection des données à caractère personnel (Úřad pro ochranu osobních údajů) Pplk. Sochora 27 - CZ - 170 00 Praha 7 Tél: +420 234 665 111	Mme Janni Christoffersen Agence danoise de protection des données (Datatilsynet) Borgergade 28, 5th floor - DK - 1300 Koebenhavn K Tél: +45 3319 3200

Fax: +420 234 665 501 E-mail: posta@uoou.cz Site web: http://www.uoou.cz/	Fax: +45 3319 3218 E-mail: dt@datatilsynet.dk Site web: http://www.datatilsynet.dk
Estonie	**Finlande**
M. Viljar Peep Bureau estonien de la protection des données (Andmekaitse Inspektsioon) Väike - Ameerika 19 - EE - 10129 Tallinn Tél: +372 6274 135 Fax: +372 6274 137 E-mail: info@aki.ee Site web: http://www.aki.ee	M. Reijo Aarnio Médiateur chargé de la protection des données (Tietosuojavaltuutetun toimisto) Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki (P.O. Box 315) Tél: +358 10 36 166700 Fax: +358 10 36 166735 E-mail: tietosuoja@om.fi Site web: http://www.tietosuoja.fi
France	**Allemagne**
M. Alex Türk **Président** Président de la Commission Nationale de l'Informatique et des Libertés - CNIL Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02 Tél: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 M. Georges de La Loyère Commission Nationale de l'Informatique et des Libertés - CNIL Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02 Tél: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 E-mail: laloyere@cnil.fr Site web: http://www.cnil.fr	M. Peter Schaar Le Commissaire fédéral à la protection des données et du droit à l'information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) Husarenstraße 30 - DE -53117 Bonn Tél: +49 (0) 228 99-7799-0 Fax: +49 (0) 228 99-7799-550 E-mail: postsTélle@bfdi.bund.de Site web: http://www.datenschutz.bund.de M. Alexander Dix (représentant des états allemands / Bundesländer) Le Commissaire à la protection des données et à la liberté d'information de Berlin (Berliner Beauftragter für Datenschutz und Informationsfreiheit) An der Urania 4-10 – DE – 10787 Berlin Tél: +49 30 13 889 0 Fax: +49 30 215 50 50 E-mail: mailbox@datenschutz-berlin.de Site web: http://www.datenschutz-berlin.de

Grèce	Hongrie
M. Christos Yeraris Le Commissaire à la protection des données et à la liberté d'information de Berlin (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 Athens - Greece Tél: +30 210 6475608 Fax: +30 210 6475789 E-mail: christosyeraris@dpa.gr Site web: http://www.dpa.gr	M. András Jóri Commissaire parlamentaire à la protection des données (Adatvédelmi Biztos) Nador u. 22 - HU - 1051 Budapest Tél:+36 1 475 7186 Fax: +36 1 269 3541 E-mail: adatved@obh.hu Site web: www.adatvedelmibiztos.hu
Irlande	**Italie**
M. Billy Hawkes Commissaire à la protection des données (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlington, IE -Co.Laois Tél: +353 57 868 4800 Fax:+353 57 868 4757 E-mail: info@dataprotection.ie Site web: http://www.dataprotection.ie	M. Francesco Pizzetti Autorité italienne de protection des données (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 - IT - 00186 Roma Tél: +39 06.69677.1 Fax: +39 06.69677.785 E-mail: garante@garanteprivacy.it, f.pizzetti@garanteprivacy.it Site web: http://www.garanteprivacy.it
Lettonie	**Lituanie**
Mme Signe Plumina Inspection nationale des données (Datu valsts inspekcija) Blaumana str. 11/13 – 15, Riga, LV-1011, Latvia Tél: +371 6722 31 31 Fax: +371 6722 35 56 E-mail: signe.plumina@dvi.gov.lv, info@dvi.gov.lv Site web: http://www.dvi.gov.lv	M. Algirdas Kunčinas Inspection de protection des données (Valstybinė duomenų apsaugos inspekcija) A.Juozapaviciaus str. 6 / Slucko str. 2, LT-01102 Vilnius Tél: +370 5 279 14 45 Fax: + 370 5 261 94 94 E-mail: ada@ada.lt Site web: http://www.ada.lt

Luxembourg	Malte
M. Gérard Lommel Commission nationale pour la Protection des Données - CNPD 41, avenue de la Gare - L - 1611 Luxembourg Tél: +352 26 10 60 -1 Fax: +352 26 10 60 – 29 E-mail: info@cnpd.lu Site web: http://www.cnpd.lu	M. Joseph Ebejer Commissaire à la protection des données Bureau du Commissaire à la protection des données (Office of the Information and Data Protection Commissioner) 2, Airways House, High Street, Sliema SLM 1549 MALTE Tél: +356 2328 7100 Fax: +356 23287198 E-mail: joseph.ebejer@gov.mt Site web: http://www.idpc.gov.mt
Pays-Bas	**Pologne**
M. Jacob Kohnstamm Autorité néerlandaise de protection des données (College Bescherming Persoonsgegevens - CBP) Juliana van Stolberglaan 4-10, P.O Box 93374 2509 AJ The Hague Tél: +31 70 8888500 Fax: +31 70 8888501 E-mail: info@cbpweb.nl Site web: http://www.cbpweb.nl http://www.mijnprivacy.nl	M. Wojciech Rafał Wiewiórowski Inspector général pour la protection des données à caractère personnel (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Warsaw Tél: +48 22 860 7312; +48 22 860 70 81 Fax: +48 22 860 73 13 E-mail: desiwm@giodo.gov.pl Site web: http://www.giodo.gov.pl
Portugal	**Romanie**
M. Luís Novais Lingnau da Silveira Commission nationale de protection des données (Comissão Nacional de Protecção de Dados - CNPD) Rua de São Bento, 148, 3º PT - 1 200-821 Lisboa Tél: +351 21 392 84 00 Fax: +351 21 397 68 32 E-mail: geral@cnpd.pt Site web: http://www.cnpd.pt	Mme Georgeta Basarabescu Autorité natinale de contrôle du traitement des données à caractère personnel (Autoritatea Națională de Supraveghere a Prelucrării DaTélor cu Caracter Personal) Olari Street no. 32, Sector 2, RO - Bucharest Tél: +40 21 252 5599 Fax: +40 21 252 5757 E-mail: georgeta.basarabescu@dataprotection.ro international@dataprotection.ro Site web: www.dataprotection.ro
Slovaqui	**Slovenie**

M. Gyula Veszelei le Bureau de protection des données à caractère personnel de la République Slovaque (Úrad na ochranu osobných údajov Slovenskej republiky) Odborárske námestie 3 - SK - 81760 Bratislava 15 Tél: +421 2 5023 9418 Fax: +421 2 5023 9441 E-mail: statny.dozor@pdp.gov.sk Site web: http://www.dataprotection.gov.sk	Mme Natasa Pirc Musar Commissaire à l'information (Informacijski pooblaščenec) Vošnjakova 1, SI - 1000 Ljubljana Tél: +386 1 230 97 30 Fax: +386 1 230 97 78 E-mail: gp.ip@ip-rs.si Site web: http://www.ip-rs.si
Espagne	**Suède**
M. José Luis Rodriguez Álvarez Agence espagnole de protection des données (Agencia Española de Protección de Datos) C/ Jorge Juan, 6 ES - 28001 Madrid Tél: +34 91 399 6219/20 Fax: + +34 91 445 56 99 E-mail: director@agpd.es Site web: http://www.agpd.es	M. Göran Gräslund Inspection des données (Datainspektionen) Fleminggatan, 14 (Box 8114) - SE - 104 20 Stockholm Tél: +46 8 657 61 57 Fax: +46 8 652 86 52 E-mail: datainspektionen@datainspektionen.se, goran.graslund@datainspektionen.se Site web: http://www.datainspektionen.se
Royaume-Uni	**Contrôleur européen de protection des données**
M. Christopher Graham Contrôleur européen de protection des données Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tél: +44 1625 545700 Fax: +44 1625 524510 E-mail: Veuillez compléter le formulaire sur notre site internet Site web: http://www.ico.gov.uk	M. Peter Hustinx Contrôleur Européen de la Protection des Données (CEPD) Adresse postale: 60, rue Wiertz, BE - 1047 Brussels Bureau: rue Montoyer, 63, BE - 1047 Brussels Tél: +32 2 283 1900 Fax: +32 2 283 1950 E-mail: edps@edps.europa.eu Site web: http://www.edps.europa.eu

OBSERVATEURS DU GROUPE DE TRAVAIL ART. 29 SUR LA PROTECTION DES DONNEES EN 2010

Islande	Norvège
Mme Sigrun Johannesdottir Autorité de protection des données (Persónuvernd) Raudararstigur 10 - IS - 105 Reykjavik Tél: +354 510 9600 Fax: +354 510 9606 E-mail: postur@personuvernd.is Site web: http://www.personuvernd.is	M. Kim Ellertsen Autorité de protection des données (Datatilsynet) P.O.Box 8177 Dep - NO - 0034 Oslo Tél: +47 22 396900 Fax: +47 22 422350 E-mail: postkasse@datatilsynet.no Site web: http://www.datatilsynet.no
Liechtenstein	**République de Croatie**
M. Philipp MitTélberger Commissaire chargé de la protection des données Bureau de protection des données (DatenschutzsTélle, DSS) Kirchstrasse 8, Postfach 684 – FL -9490 Vaduz Tél: +423 236 6090 Fax: +423 236 6099 E-mail: info@dss.llv.li Site web http://www.dss.llv.li	M. Franjo Lacko Directeur Mme Sanja Vuk Chef du département des affaires juridiques Agence Croate de protection des données à caractère personnel (Agencija za zaštitu osobnih podataka - AZOP) Republike Austrije 25, 10000 Zagreb Tél. +385 1 4609 000 Fax +385 1 4609 099 e-mail: azop@azop.hr or info@azop.hr Site web: http://www.azop.hr/default.asp
ancienne République yougoslave de Macédoine	
M. Dimitar Gjeorgjievski Direction de protection des données à caractère personnel (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tél: +389 2 3230 635 Fax: +389 2 3230 635 E-mail: info@dzlp.mk Site web: www.dzlp.mk	

Secrétariat du groupe de travail Art. 29
Mme Marie-Hélène Boulanger Chef d'unité Commission européenne Direction générale de la justice Unité de protection des données Bureau: MO59 02/13 - BE - 1049 Brussels 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/data-protection/index_en.htm

Commission européenne - Direction générale de la justice
Quatorzième rapport du groupe de travail «Article 29» sur la protection des données

Luxembourg: Office des publications de l'Union européenne
2013 — 134 p. — 21 × 29.7 cm

ISBN 978-92-79-29770-0
doi: 10.2838/29618

DS-AA-13-001-FR-C
doi: 10.2838/29618

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.

Office des publications

ISBN 978-92-79-29770-0