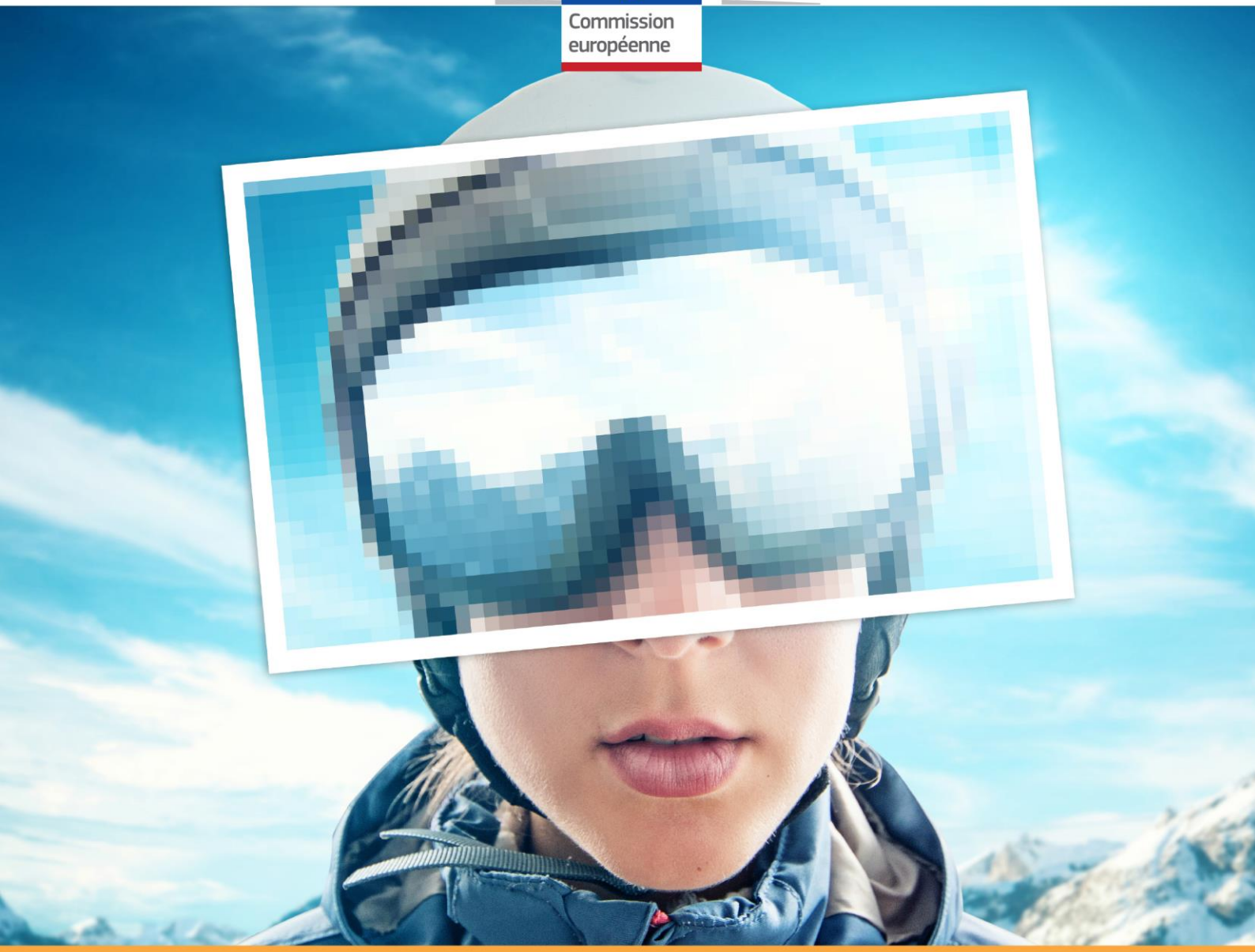
Commission européenne



Quinzième rapport

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

Justice et Consommateurs

Europe Direct est un service destiné à vous aider à trouver des réponses aux questions que vous vous posez sur l'Union européenne.

Un numéro unique gratuit (*)**:**
00 800 6 7 8 9 10 11

(*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

De nombreuses autres 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, 2015

ISBN 978-92-79-38256-7
doi: 10.2838/11069
ISSN: 2363-1007

FR

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

Portant sur l'année 2011

Adopté le 3.12.2013

FR

Table des matières

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

Ce rapport annuel du groupe de travail « Article 29 » sur la protection des personnes dans le cadre du traitement des données personnelles vous offre un aperçu des activités du groupe en 2011. Le groupe de travail est un organe consultatif indépendant au sein duquel sont représentées les 27 autorités nationales en charge de la protection des données dans les États membres de l'Union européenne, le Contrôleur européen de la protection des données et la Commission européenne. Le groupe de travail émet des avis ou des recommandations sur tous les sujets afférents à la protection des données personnelles, contribuant ainsi à l'uniformité de l'application et de l'interprétation des lois sur la protection des données dans les États membres de l'Union européenne.

Ces dernières années, le groupe de travail a consacré beaucoup de temps et de nombreux efforts au processus de réforme de la protection des données. Au moment de la rédaction de ce rapport, la Commission européenne a déjà présenté les propositions de réforme des règles de protection des données, qui consistent en un Règlement général sur la protection des données et en une Directive dans le domaine de l'application du droit pénal. Le groupe de travail a toujours rappelé la nécessité de faire preuve d'exhaustivité et a par conséquent été quelque peu déçu par la présentation de deux instruments différents. Cette exhaustivité peut néanmoins toujours être atteinte si lesdits instruments prévoient les mêmes droits, principes et garanties. Le groupe de travail a participé au processus de réforme et continuera d'y participer à l'avenir.

Les techniques applicables au traitement des données personnelles dans les domaines public et privé étant de plus en plus nombreuses, la protection des données personnelles d'une personne exige une attention encore plus grande. Une étude réalisée à l'échelle européenne par Eurobaromètre sur les attitudes des citoyens européens à l'égard de la protection des données et de l'identité électronique[1] montre qu'en règle générale, les personnes n'ont pas le sentiment de maîtriser ce qui touche à leurs données personnelles.[2]

Dans la mesure où les données personnelles sont devenues une nouvelle forme de devise (prenons pour exemple la valeur actionnariale de sociétés faisant le commerce de données personnelles, telles que Facebook, Google et Twitter, notamment), ce secteur semble extrêmement intéressé par la collecte d'autant de données personnelles de consommateurs que possible. Souvent, les organisations dressent le profil de personnes afin de les cibler personnellement et ainsi optimiser leurs profits ou minimiser leurs risques. L'étude d'Eurobaromètre montre, en sus des contacts réguliers entre les citoyens et les autorités chargées de la protection des données (DPA), que les personnes n'ont le plus souvent pas conscience de la collecte de leurs données. Lorsque les citoyens ont conscience des volumes de données personnelles collectées, ils se sentent mal à l'aise et ne savent pas comment changer cet état de fait.

Cette ignorance des citoyens concernant le traitement de leurs données personnelles par des tiers est d'autant plus choquante que la protection des données est un droit humain fondamental au sein de l'UE. Il est par conséquent incontestable que les citoyens doivent donner leur consentement explicite à la collecte ou au traitement de leurs données personnelles par des tiers lorsque les actes de celles-ci ne reposent sur aucun autre fondement juridique. Dans son avis sur le consentement, le groupe de travail a souligné que

[1] Eurobaromètre, Rapport Eurobaromètre spécial 359, *Attitudes à l'égard de la protection des données et de l'identité électronique dans l'Union européenne*, juin 2011,

[2] Le rapport indique que, d'un côté, 74 % des Européens considèrent la divulgation d'informations personnelles comme faisant de plus en plus partie de la vie moderne, surtout lorsqu'ils utilisent Internet. D'un autre côté, les citoyens européens n'ont pas le sentiment de maîtriser la divulgation d'informations personnelles : à peine 26 % des utilisateurs de réseaux sociaux et 18 % des acheteurs en ligne ont le sentiment d'une maîtrise complète. 70 % des citoyens suspectent les entreprises d'avoir l'intention d'utiliser leurs données personnelles à des fins autres que celles pour lesquelles elles ont été collectées.

seule une déclaration ou une action, et non l'absence de réaction ou l'inaction des citoyens concernés, constituait un consentement valide. En donnant leur consentement explicite, les personnes retrouvent la maîtrise du traitement de leurs données personnelles.

Cette obligation de recueil du consentement explicite des personnes par les entreprises n'est pas toujours respectée. En 2011, un nouveau code d'autorégulation sur la publicité comportementale en ligne (OBA) a été développé par le secteur de l'OBA. Le groupe de travail a examiné ce cadre et a conclu qu'il ne garantissait pas le respect de la législation européenne relative à la protection des données. Le groupe de travail a averti qu'il convenait d'éviter une situation où le respect d'un code de conduite ne permettrait pas de garantir le respect du droit européen relatif à la protection de la vie privée.

Le groupe de travail a par ailleurs fait part de son inquiétude quant à deux propositions de la Commission européenne relatives à l'accès des forces de l'ordre aux données détenues par des sociétés privées. La première proposition visait à mettre en place un système européen permettant aux autorités policières d'avoir accès aux données des dossiers passagers (PNR) enregistrées par les compagnies aériennes pour les vols arrivant ou partant d'un État membre. Selon les autorités européennes en charge de la protection des données, la nécessité du système proposé n'a pas été prouvée. Tel que proposé, le système ne respecte pas la vie privée et ses objectifs pourraient être atteints de manière différente, sans violation du droit relatif à la protection de la vie privée.

Le groupe de travail a également fait part de son inquiétude quant à la proposition de création d'un système européen de surveillance du financement du terrorisme (SSFT) conçu pour représenter l'équivalent européen de l'actuel programme (TFTP) des États-Unis. Le programme permet à certaines autorités policières d'avoir accès à des informations sur les transactions bancaires internationales réalisées au sein de l'UE. Les données sont stockées dans de grandes bases de données et peuvent être utilisées afin de remonter les pistes de financement de possibles activités terroristes. Les DPA ne sont pas convaincues de la nécessité ou de la proportionnalité du SSFT et ont clairement fait savoir que la simple valeur ajoutée des informations tirées du système n'était pas suffisante. Dans un courrier adressé à la Commission européenne, le groupe de travail appelle la Commission à fournir de telles preuves, lors de l'éventuelle présentation d'une proposition finale.

L'étude Eurobaromètre susmentionnée montre que les personnes s'inquiètent de la manière dont leurs données personnelles sont collectées, traitées et stockées. C'est pourquoi il est essentiel que le traitement des données personnelles par les organisations privées comme publiques soit conforme à la législation européenne relative à la protection des données. Les autorités en charge de la protection des données appliqueront cette loi lorsque nécessaire, de manière individuelle et conjointe.

Jacob Kohnstamm.

Chapitre premier
Questions examinées par le groupe de travail « Article 29 » sur la protection des données[3]

[3] 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/dataprotection/article-29/documentation/opinion-recommandation/index_en.htm#h2-2

1.1 TRANSFERT DE DONNÉES VERS DES PAYS TIERS

1.1.1 Données des dossiers passagers / PNR

Avis 10/2011 (WP181) sur la proposition de Directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers à des fins de prévention, de détection, de recherche et de poursuite des infractions terroristes et des infractions pénales graves

Le 2 février 2011, la Commission européenne a publié sa proposition de Directive sur l'utilisation des données des dossiers passagers à des fins de prévention, de détection, de recherche et de poursuite des infractions terroristes et des infractions pénales graves. Le groupe de travail a émis un avis sur la précédente proposition PNR de l'UE (Proposition de décision-cadre du Conseil sur l'utilisation des données des dossiers passagers (PNR) à des fins policières), présentée par la Commission le 6 novembre 2007. Le groupe de travail s'est déjà largement exprimé, dans le cadre de plusieurs avis, sur les différents accords PNR mis en place entre l'UE et des pays tiers et sur l'approche de la Commission telle que décrite dans sa communication du 21 septembre 2010. Le groupe de travail a également réitéré ses inquiétudes sur les questions liées aux PNR dans divers courriers adressés au Commissaire Barrot, au Commissaire Malmström, au Directeur général Faull et au Comité LIBE du Parlement européen.

Le présent avis s'adresse aux parties associées aux discussions et à l'élaboration de la dernière proposition, à savoir la Commission, le groupe de travail GENVAL du Conseil et le Parlement européen.

Conclusion

Le groupe de travail considère que la nécessité d'un système PNR européen n'a pas encore été prouvée et que les mesures proposées ne cadrent pas avec le principe de proportionnalité, en particulier dans la mesure où le système envisage la collecte et la rétention de toutes les données disponibles sur tous les voyageurs de tous les vols. Le groupe de travail a en outre de sérieux doutes quant à la proportionnalité du rapprochement systématique entre l'ensemble des passagers et des critères prédéterminés.

Le groupe de travail recommande en premier lieu d'évaluer les méthodes de coopération et les systèmes existants ainsi que la manière dont ils se complètent pour identifier les lacunes de sécurité. Une fois celles-ci identifiées, la meilleure manière de les combler devra ensuite être analysée, ce qui n'implique pas nécessairement l'introduction d'un système entièrement nouveau. Les mécanismes existants pourraient être mieux exploités et améliorés.

Si cette proposition de Directive entre en vigueur, elle devra assurer la mise en œuvre de garanties et de mesures de protection des données appropriées et adéquates. La Commission devra également déterminer s'il existe des systèmes pouvant être abolis, tels que la Directive API, afin d'éviter les mesures redondantes.

1.1.2. Adéquation

Avis 11/2011 (WP182) relatif au niveau de protection des données à caractère personnel assuré en Nouvelle-Zélande

Il a été demandé au groupe de travail de considérer l'adéquation de la législation néo-zélandaise en matière de protection des données en 2009 et ce mandat a été confié au sous-groupe concerné à l'occasion de la séance plénière de décembre 2009.

Chapitre premier **Questions examinées par le groupe de travail « Article 29 » sur la protection des données**

La Commission européenne a présenté un rapport qu'elle avait demandé sur l'adéquation de la protection des données personnelles en Nouvelle-Zélande, rédigé par le Professeur Roth, de la Faculté de Droit de l'Université d'Otago à Dunedin en Nouvelle-Zélande, sous la supervision du Centre de Recherches Informatique et Droit (CRID) de l'Université de Namur. Ce rapport analyse le degré de conformité du système juridique de la Nouvelle-Zélande avec les exigences de fond en termes de législation et la mise en œuvre de mécanismes d'application des règlements protégeant les données personnelles, énoncées dans le document de travail « Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données », approuvé par le groupe de travail « Article 29 » le 24 juillet 1998 (WP 12). Il tient également compte des règles non juridiques, de l'application pratique et de la culture administrative et d'entreprise générale qui existe dans le domaine du respect de la vie privée.

Le sous-groupe a examiné ce rapport ainsi que les commentaires qu'il a suscités de la part des DPA néo-zélandaises et du ministère de la Justice néo-zélandais et le courrier du ministère de la Justice concernant la loi de 2010 portant modification de la loi sur la protection de la vie privée (informations transfrontalières). Le sous-groupe a également demandé au Commissaire à la protection de la vie privée de Nouvelle-Zélande (l'autorité de contrôle nationale) de plus amples informations et une clarification de certains aspects, tels que visés ci-dessous. Le sous-groupe a alors examiné les informations reçues, qui contiennent des conseils du Commissaire à la protection de la vie privée sur l'application de la loi portant modification de la loi sur la protection de la vie privée (informations transfrontalières) suite à son entrée en vigueur le 7 septembre 2010.

Le présent avis s'appuie largement sur le rapport du Professeur Roth, qui a été rédigé et structuré de manière suffisamment claire pour comparer la législation de la Nouvelle-Zélande à chacune des exigences du WP 12.

Résultat de l'évaluation

La loi néo-zélandaise sur la protection des données personnelles et de la vie privée est largement antérieure à la Directive européenne et met en œuvre les lignes directrices de l'OCDE. De récents amendements y ont néanmoins été apportés afin de répondre spécifiquement aux problèmes « d'adéquation » des transferts de données personnelles depuis l'UE. Le groupe de travail rappelle que, même si certains problèmes demeurent, le principe d'adéquation n'est pas pour autant synonyme d'équivalence avec la Directive.

C'est la raison pour laquelle le groupe de travail considère que la Nouvelle-Zélande assure un niveau adéquat de protection au sens de l'Article 25(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.

Néanmoins, le groupe de travail encourage également les autorités néo-zélandaises à prendre les mesures nécessaires pour résoudre les faiblesses du cadre juridique actuel. En particulier, le groupe de travail encourage le Commissaire à la protection de la vie privée à maintenir son appel en faveur du renforcement de la loi vis-à-vis du marketing direct et du maintien de l'efficacité des contrôles des transferts depuis la Nouvelle-Zélande vers des pays tiers ne faisant pas eux-mêmes l'objet d'un constat d'adéquation. Le groupe de travail demande également qu'outre les lignes directrices de l'OCDE et la Directive européenne, le Commissaire à la protection de la vie privée tienne également compte des décisions pertinentes de la Commission européenne et des conseils du groupe de travail « Article 29 » lorsqu'il prendra sa décision relative à l'émission d'un avis d'interdiction de transfert.

Le groupe de travail souligne également le fait que, lors de toute décision prise par la Commission, il suivra de près l'évolution de la protection des données en Nouvelle-Zélande et la manière dont le Bureau du Commissaire à la protection de la vie privée applique les principes de protection des données visés au document WP12 et au présent document.

1.2. COMMUNICATIONS ÉLECTRONIQUES, INTERNET ET NOUVELLES TECHNOLOGIES

Avis 12/2011 (WP183) sur les compteurs intelligents

L'objectif du groupe de travail « Article 29 », dans le présent avis, est de clarifier le cadre juridique applicable au fonctionnement de la technologie de comptage intelligent dans le secteur énergétique. Le présent avis n'est pas destiné à présenter un aperçu complet de tous les aspects spécifiques des programmes de comptage intelligent dans les États membres, la disparité de la situation actuelle ne le permettant pas. Les compteurs intelligents offrent de nouvelles fonctionnalités, comme la production d'informations détaillées sur la consommation d'énergie, la possibilité d'effectuer des relevés à distance, l'élaboration de nouveaux tarifs et services sur la base des profils énergétiques et la possibilité d'interrompre la fourniture à distance.

Les réseaux intelligents ouvrent encore davantage de perspectives de développement et de traitement de données à caractère plus personnel. À ce stade, le groupe de travail n'a pas l'intention d'inclure la fonction de réseau intelligent dans le champ d'application du présent avis. Nous n'excluons pas, cependant, d'approfondir notre analyse du réseau intelligent quand la situation se précisera.

La Directive communautaire relative à l'efficacité énergétique dans les utilisations finales et aux services énergétiques (2006/32/CE) fixe des objectifs à adopter par chaque État membre en matière d'économie d'énergie. Afin d'atteindre ces objectifs, et sous réserve d'un nombre limité d'exceptions, l'article 13 de la directive oblige les États membres à mettre à la disposition des consommateurs des compteurs qui mesurent avec précision leur consommation effective et qui fournissent des informations sur le moment où l'énergie a été utilisée. Ces compteurs intelligents s'inscrivent dans le cadre des efforts pour réaliser les objectifs que l'Union européenne s'est fixés en vue de garantir un approvisionnement énergétique durable d'ici à 2020.

Conclusions

L'arrivée de compteurs intelligents, qui ouvre la voie au réseau intelligent, apporte avec elle un modèle d'interrelations entièrement nouveau et complexe qui soulève des questions concernant l'application du droit en matière de protection des données. Les réponses au questionnaire de la direction générale de l'énergie ont fait apparaître une grande diversité de situations entre les États membres de l'UE, en ce qui concerne tant l'avancement dans la mise en place des systèmes que les modalités de fourniture d'énergie, ce qui complique encore le scénario. Il ne fait cependant aucun doute que le déploiement des compteurs intelligents s'opère à très grande échelle : il est prévu que la grande majorité des citoyens européens en auront un chez eux avant la fin de cette décennie.

Le présent avis explique dans quelle mesure le droit en matière de protection des données est applicable : il a été démontré que des données à caractère personnel sont traitées par les compteurs et que, par conséquent, les législations relatives à la protection des données s'appliquent. Le présent avis a indiqué que les systèmes de relevés intelligents offrent un grand nombre de possibilités nouvelles pour traiter les données et fournir des services aux consommateurs. Quel que soit le traitement, qu'il soit similaire à ce qui existait auparavant ou sans précédent, le responsable du traitement des données doit être clairement

identifié et doit avoir connaissance des obligations que lui impose la législation en matière de protection des données, notamment du point de vue de la prise en compte du respect de la vie privée dès la conception (*privacy by design*), de la sécurité et des droits des personnes concernées. Ces personnes doivent être correctement informées de la façon dont sont traitées leurs données et avoir conscience des différences fondamentales dans les modes de traitement pour être en mesure de donner valablement leur consentement.

Avis 13/2011 (WP185) sur les services de géolocalisation des dispositifs mobiles intelligents

Les informations géographiques jouent un rôle important dans notre société. La plupart des activités et décisions humaines ont une dimension géographique. Lorsque des informations sont liées à une position géographique, elles acquièrent généralement une plus grande valeur. Ces informations peuvent être de toutes sortes : financières, sanitaires ou autres données relatives au comportement du consommateur. En raison de la rapidité de l'évolution technologique des dispositifs mobiles intelligents associée à la généralisation de leur utilisation, une toute nouvelle catégorie de services basés sur la localisation se développe.

Le présent avis a pour objectif de clarifier le cadre juridique applicable aux services de géolocalisation proposés et/ou générés par les dispositifs mobiles intelligents capables de se connecter à l'internet et équipés de capteurs de localisation tels qu'un GPS. Il peut notamment s'agir de services de cartographie et de navigation, de services géopersonnalisés (y compris les points d'intérêt à proximité), de réalité augmentée, du géomarquage de contenu sur l'internet, de la possibilité de se tenir informé des allées et venues de ses amis, de la surveillance des enfants et de la publicité basée sur la localisation.

Le présent avis aborde également les trois principaux types d'infrastructure utilisés pour offrir ces services de géolocalisation, à savoir le système GPS, les stations de base GSM et le système Wi-Fi. Une attention particulière est accordée à la nouvelle infrastructure basée sur la localisation de points d'accès Wi-Fi.

Le groupe de travail est bien conscient qu'il existe de nombreux autres services capables de traiter des données de localisation qui peuvent également susciter des inquiétudes en matière de protection des données. Il s'agit entre autres des systèmes de billetterie électronique, des systèmes de péage pour voitures et des services de navigation par satellite, du repérage de position à l'aide, par exemple, de caméras et de la géolocalisation d'adresses IP. Cependant, en raison de la rapidité de l'évolution technologique, notamment en matière de mappage de points d'accès sans fil, associée au fait que de nouveaux arrivants sur le marché se préparent à mettre au point de nouveaux services de localisation basés sur un mélange de données issues des stations de base et des systèmes GPS et Wi-Fi, le groupe de travail a décidé de clarifier de manière spécifique les conditions juridiques que doivent remplir ces services en vertu de la directive sur la protection des données.

Le présent avis commence par décrire les technologies concernées, puis identifie et évalue les risques d'atteinte à la vie privée, et enfin présente des conclusions concernant l'application des articles juridiques pertinents à divers responsables du traitement qui recueillent et traitent les données de localisation provenant de dispositifs mobiles. Il s'agit, par exemple, des fournisseurs d'infrastructure de géolocalisation, des fabricants de téléphones intelligents et des développeurs d'applications basées sur la géolocalisation.

Le présent avis n'évaluera pas la technologie de géomarquage spécifique associée à ce que l'on appelle le Web 2.0, selon laquelle les utilisateurs intègrent des informations géoréférencées sur des réseaux sociaux tels que Facebook ou Twitter. Le présent avis n'entrera pas non plus dans les détails de certaines autres technologies de géolocalisation qui sont utilisées pour interconnecter des dispositifs situés dans

une zone relativement petite (centres commerciaux, aéroports, immeubles de bureaux, etc.), telles que les technologies Bluetooth, ZigBee, le gardiennage virtuel et les étiquettes RFID utilisant la technologie Wi-Fi, bien qu'une grande partie des conclusions du présent avis relatives aux motifs légitimes, à l'information et aux droits des personnes concernées s'appliquent également à ces technologies lorsqu'elles servent à établir la position géographique de personnes par l'intermédiaire de leurs dispositifs.

Avec l'aide de technologies de géolocalisation telles que les données de stations de base, le système GPS et les points d'accès Wi-Fi mappés, les dispositifs mobiles intelligents peuvent être localisés par toutes sortes de responsables du traitement, à des fins allant de la publicité comportementale à la surveillance des enfants.

Étant donné que les téléphones intelligents et les tablettes électroniques sont inextricablement liés à leur propriétaire, les schémas de déplacement des dispositifs donnent une vision détaillée et intime de la vie privée des propriétaires. L'un des principaux risques est que ces propriétaires ignorent qu'ils transmettent leur position, et à qui ils la transmettent. Un autre risque associé est que l'autorisation donnée à certaines applications d'utiliser les données de localisation n'est pas valable, car les informations concernant les éléments clés du traitement sont incompréhensibles, désuètes ou inadéquates.

Les obligations diffèrent en fonction des opérateurs, qui vont des développeurs des systèmes d'exploitation aux fournisseurs d'application et parties concernées telles que les sites de réseaux sociaux qui intègrent dans leurs plates-formes des fonctions de localisation destinées à des dispositifs mobiles.

Conclusions

Cadre juridique

- Le cadre juridique de l'UE pour l'utilisation des données de géolocalisation provenant de dispositifs mobiles intelligents est fourni principalement par la directive sur la protection des données. Les données de localisation provenant de dispositifs mobiles intelligents sont des données à caractère personnel. La combinaison de l'adresse MAC unique et de la position calculée d'un point d'accès Wi-Fi devrait être traitée de la même manière que des données à caractère personnel;

- De plus, la directive 2002/58/CE révisée sur la vie privée et les communications électroniques ne s'applique qu'au traitement de données de stations de base par des opérateurs de télécommunications.

Responsables du traitement

- Il est possible de distinguer trois types de responsables du traitement : les responsables d'infrastructure de géolocalisation (notamment les responsables de points d'accès Wi-Fi mappés) ; les fournisseurs d'applications et de services de géolocalisation ; et les développeurs de système d'exploitation de dispositifs mobiles intelligents.

Motifs légitimes

- Étant donné que les données de dispositifs mobiles intelligents révèlent des détails intimes sur la vie privée de leur propriétaire, le principal motif légitime applicable est le consentement préalable en connaissance de cause;

- Le consentement ne peut pas être obtenu par l'intermédiaire de l'acceptation des conditions générales;

- Le consentement doit être spécifique pour chacune des différentes finalités pour lesquelles les données sont traitées, par exemple l'établissement de profils et/ou le ciblage comportemental par le responsable du traitement. Si les finalités du traitement changent de manière significative, le responsable du traitement doit chercher à obtenir une nouvelle fois le consentement spécifique;

- Par défaut, les services de localisation doivent être désactivés. Le fait de proposer la possibilité de renoncer au transfert de données ne constitue pas un mécanisme adéquat pour obtenir le consentement en connaissance de cause d'un utilisateur;

- Le consentement pose problème en ce qui concerne les travailleurs et les enfants. En ce qui concerne les travailleurs, les employeurs ne peuvent utiliser cette technologie que lorsqu'il est possible de prouver qu'elle est nécessaire pour une finalité légitime, et que les mêmes objectifs ne peuvent pas être atteints à l'aide de moyens moins intrusifs. En ce qui concerne les enfants, c'est à leurs parents de juger si l'utilisation d'une telle application est justifiée dans certaines circonstances. Les parents doivent à tout le moins informer leurs enfants, et dès que raisonnablement possible, permettre à leurs enfants de participer à la décision d'utiliser une telle application;

- Le groupe de travail recommande de limiter la portée du consentement dans le temps et de recontacter les utilisateurs au moins une fois par an. Le groupe de travail recommande également de détailler suffisamment le consentement en ce qui concerne la précision des données de localisation;

- Les personnes concernées doivent pouvoir retirer facilement leur consentement, sans aucune conséquence négative pour l'utilisation de leur dispositif;

- En ce qui concerne le mappage de points d'accès Wi-Fi, les sociétés peuvent avoir un intérêt légitime à recueillir et à traiter les adresses MAC et les positions calculées de points d'accès Wi-Fi dans le but spécifique d'offrir des services de géolocalisation. La mise en balance des droits du responsable du traitement, d'une part, et des droits des personnes concernées, d'autre part, nécessite que le responsable du traitement accorde aux utilisateurs le droit de renoncer de manière aisée et définitive à participer à la base de données, sans exiger la fourniture de données à caractère personnel supplémentaires.

Informations

- Les informations doivent être claires, exhaustives, compréhensibles pour un large public non initié et accessibles facilement et en permanence. La validité du consentement est inextricablement liée à la qualité des informations concernant le service;

- Les tiers, tels que les navigateurs et les sites de réseaux sociaux ont un rôle essentiel à jouer lorsqu'il s'agit de la visibilité et de la qualité des informations concernant le traitement des données de géolocalisation.

Droits des personnes concernées

- Les différents responsables du traitement d'informations de géolocalisation provenant de dispositifs mobiles doivent permettre à leurs clients d'accéder à leurs données de localisation dans une version directement lisible et les autoriser à les rectifier ou à les supprimer sans recueillir une quantité excessive de données à caractère personnel;

- Les personnes concernées ont également le droit d'accéder aux éventuels profils établis sur la base de ces données de localisation, de les rectifier et de les supprimer;

- Le groupe de travail recommande la création d'un accès en ligne (sécurisé).

Délais de conservation

- Les fournisseurs d'applications ou de services de géolocalisation doivent mettre en œuvre des politiques de conservation garantissant que des données de géolocalisation ou des profils découlant de telles données sont supprimés après une période de temps justifiée;

- Si le développeur du système d'exploitation et/ou le responsable du traitement de l'infrastructure de géolocalisation traitent un numéro unique tel qu'une adresse MAC ou un identifiant UDID en rapport avec des données de localisation, le numéro d'identification unique ne peut être stocké que pour une période maximale de 24 heures, à des fins opérationnelles.

Avis 16/2011 (WP188) sur le code de bonnes pratiques de l'AEEP et de l'IAB en matière de publicité comportementale en ligne

En novembre 2009, le Parlement européen et le Conseil ont adopté la directive 2009/136/CE portant révision de la directive « Vie privée et communications électroniques » de 2002 (2002/58/CE). L'une des modifications essentielles concernait les mécanismes de stockage d'informations dans le terminal de l'utilisateur. Le régime d'« opt-out » existant, permettant à un utilisateur de s'opposer au traitement d'informations collectées par l'intermédiaire d'un équipement terminal (par exemple, au moyen de « cookies » ou témoins de connexion), a été rejeté. En revanche, le « consentement informé » est devenu la norme. Ces modifications ont une incidence importante sur la publicité comportementale en ligne, étant donné que ce secteur repose largement sur l'utilisation de cookies et de dispositifs similaires qui stockent des informations dans le terminal de l'utilisateur et permettent d'accéder à des informations qui y sont déjà stockées.

L'introduction de cette obligation de « consentement informé » faisait suite aux préoccupations croissantes exprimées par les citoyens, la classe politique, les autorités chargées de la protection des données, les associations de consommateurs et les décideurs politiques, à l'égard du rapide développement des techniques permettant de suivre (« tracking ») la navigation d'internautes sur une longue période et sur plusieurs sites internet différents. De surcroît, les moyens dont disposaient les citoyens pour protéger leur vie privée et les données à caractère personnel les concernant contre ce type de procédés ne permettaient plus de suivre cette évolution. En 2009, les décideurs politiques ont émis des doutes sérieux quant à la possibilité de s'en remettre au secteur publicitaire en question pour sensibiliser davantage le grand public et renforcer le choix de l'utilisateur à l'égard de la publicité comportementale en ligne. Il ressort toujours de nombreuses enquêtes d'opinion que l'internaute moyen n'a pas connaissance du fait que des cookies ou d'autres identifiants uniques permettent de garder une trace de son comportement en ligne. Il ne sait pas non plus qui a utilisé ces cookies ni à quelle fin. Or ce manque d'information contraste fortement avec l'importance croissante que prend l'internet dans la vie quotidienne de nombreux citoyens européens, notamment pour faire des achats, lire, communiquer avec des amis ou rechercher des informations. En outre, de plus en plus d'activités « hors ligne », telles que l'accès à certains services publics, sont remplacées par des activités en ligne. Enfin, le rapide remplacement de l'accès internet « fixe » par l'accès « mobile » complique encore la situation pour les internautes en matière de protection à l'aide de moyens techniques.

Peu de temps après que le consentement informé fut devenu la norme légale européenne, le groupe de travail « Article 29 » a adopté l'avis 2/2010 sur la publicité comportementale en ligne (OBA)[4] (ci-après dénommé l'Avis 2/2010). Cet avis décrit les rôles et responsabilités des différents acteurs du secteur de la publicité comportementale en ligne et précise le cadre juridique applicable. Il porte essentiellement sur le suivi de la navigation d'internautes sur une longe période et sur plusieurs sites internet différents, en tant que principale source de préoccupation en ce qui concerne la publicité comportementale en ligne.

En avril 2011, les acteurs concernés du secteur de la publicité comportementale en ligne, représentés à la fois par l'Alliance européenne pour l'éthique en publicité (AEEP ou EASA en anglais) et l'Internet Advertising Bureau Europe (IAB), ont adopté un code de bonnes pratiques en matière de publicité comportementale en ligne (Best Practice Recommendation on online behavioural advertising, ci-après dénommé « le code de l'AEEP/IAB »)[5]. En août 2011, le groupe de travail « Article 29 » a adressé une lettre ouverte[6] à l'AEEP et à l'IAB faisant valoir ses craintes, en matière de protection des données, à l'égard de l'approche d'« opt-out » proposée dans le code de l'AEEP/IAP. Lors d'une réunion ultérieure avec le groupe de travail « Article 29 », des représentants de l'AEEP et de l'IAB ont déclaré que « le code visait essentiellement à égaliser les conditions de concurrence » et que son objet n'était pas la mise en conformité avec la directive « Vie privée et communications électroniques » révisée[7].

Le groupe de travail « Article 29 » se félicite, comme indiqué dans son avis 2/2010, des initiatives prises par le secteur de la publicité comportementale en matière d'autorégulation. Le code de l'AEEP/IAB contient en effet des pistes intéressantes (telles que le Principe V – Éducation) qui, si elles sont encore élaborées et mises en œuvre, peuvent rendre les mécanismes de consentement plus effectifs. Ce code, en soi, est néanmoins insuffisant pour assurer la conformité avec le cadre juridique européen en vigueur en matière de protection des données. Afin de prévenir tout malentendu, le groupe de travail « Article 29 » a décidé de fournir une analyse spécifique de la mesure dans laquelle ce code, tel qu'il est complété par le site internet www.youronlinechoices.eu, respecte les dispositions légales pertinentes.

En particulier, le présent avis porte essentiellement sur les deux premiers principes énoncés dans le code de l'AEEP/IAB et leur application pratique sur le site internet www.youronlinechoices.eu, à savoir le Principe I (L'information de l'utilisateur) et le Principe II (Le libre choix de l'utilisateur). Il examine, en outre, d'autres principes du code ainsi que des sujets de préoccupation (tels que la conservation des données). Enfin, le groupe de travail « Article 29 » saisit cette occasion pour mettre en évidence la distinction qui existe entre les cookies traceurs et les autres types de cookies pouvant être exemptés de l'obligation de consentement, en donnant des exemples concrets de cookies exemptés et en indiquant des approches possibles pour recueillir d'une manière licite le consentement de l'internaute lorsque celui-ci est requis.

Conclusions

Ainsi qu'il l'avait souligné dans son avis 2/2010, le groupe de travail « Article 29 » ne remet pas en cause les avantages économiques que les parties prenantes peuvent tirer de la publicité comportementale, mais il est fermement convaincu que cette pratique ne saurait exister aux dépens du droit des personnes à la

[4] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf

[5] http://www.easa-alliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download

[6] Lettre du groupe de travail « Article 29 », du 3 août 2011, adressée au secteur de la publicité comportementale en ligne concernant son système d'autorégulation http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf

[7] Communiqué de presse du groupe de travail « Article 29 » du 14 septembre 2011 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20110914_press_release_oba_industry_final_en.pdf

protection de leurs données et de leur vie privée. Le cadre réglementaire de l'UE en matière de protection des données, qui établit des garanties spécifiques, doit être respecté.

L'adhésion au code de l'AEEP/IAB en matière de publicité comportementale en ligne et la participation au site internet www.youronlinechoices.eu ne permettent pas de se conformer à la directive « Vie privée et communications électroniques » en vigueur. Qui plus est, ce code et ce site internet font croire à tort à l'utilisateur qu'il peut choisir de ne pas faire l'objet d'un suivi lorsqu'il surfe sur l'internet. Or cette présomption erronée peut être préjudiciable non seulement aux utilisateurs, mais aussi aux opérateurs du secteur concerné s'ils pensent satisfaire aux exigences de la directive en appliquant ce code.

Le secteur publicitaire doit se conformer aux obligations précises qui lui incombent en vertu de la directive « Vie privée et communications électroniques », et le présent avis montre que de nombreuses solutions pratiques existent pour garantir à la fois un niveau élevé de conformité ainsi qu'une bonne expérience de navigation à l'utilisateur.

1.3. RFID

Avis 9/2011 (WP180) sur la proposition révisée 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 présent avis s'inscrit dans le cadre du suivi de l'Avis 5/2010 (WP 175) 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). Si cette introduction réitère certains éléments de contexte nécessaires pour saisir la finalité et la portée du présent avis, le lecteur est néanmoins invité à se reporter à l'Avis 5/2010 pour plus de détails.

Le 12 mai 2009, la Commission européenne a publié une Recommandation sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence. Dans cette recommandation, elle invitait les États membres à veiller à ce que les entreprises, en collaboration avec les parties intéressées, élaborent un cadre pour l'évaluation d'impact sur la protection des données et de la vie privée, cadre qui devait être soumis pour approbation au groupe de travail « Article 29 » sur la protection des données. Une fois le cadre pour l'évaluation d'impact sur la protection des données et de la vie privée (EIP) défini, les États membres doivent s'assurer que les exploitants d'applications RFID réalisent une évaluation des incidences sur la protection des données et de la vie privée des applications RFID, avant la mise en œuvre de celles-ci. Les États membres doivent également veiller à ce que les opérateurs d'applications RFID mettent les rapports d'évaluation ainsi établis à la disposition de l'autorité compétente.

Le 31 mars 2010, les représentants du secteur ont remis leur proposition de cadre d'évaluation de l'impact sur la protection des données et de la vie privée au groupe de travail « Article 29 » en vue de son approbation. Cependant, bien que cette proposition ait constitué un bon point de départ, elle n'a pas recueilli le plein soutien du groupe de travail, notamment en raison de l'absence de trois éléments essentiels dans le cadre proposé :

1. Une méthode d'évaluation des risques clairement définie.

2. La prise en compte des étiquettes RFID portées par des personnes au-delà du périmètre opérationnel de l'application.

3. Un moyen de tenir compte explicitement des principes de désactivation des étiquettes dans le secteur de la distribution, tels qu'énoncés dans la recommandation de la Commission européenne sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence.

Le 13 juillet 2010, le groupe de travail a synthétisé ces éléments, ainsi que d'autres sujets de préoccupation, dans l'Avis 5/2010, dans lequel il invitait les entreprises du secteur à soumettre une proposition révisée de cadre d'évaluation de l'impact des applications RFID sur la protection des données et de la vie privée. En ce qui concerne l'évaluation des risques, le groupe de travail encourageait vivement les entreprises à s'inspirer de l'expertise acquise en la matière par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

Au cours du même mois, l'ENISA a publié un avis indépendant dans lequel elle formulait des recommandations concrètes pour améliorer le cadre proposé. Elle y proposait notamment une première série de lignes directrices en vue de l'adoption d'une approche méthodologique exhaustive et reconnue de l'évaluation des risques, et y suggérait plusieurs améliorations structurelles.

Dans les mois qui ont suivi, les entreprises ont revu leur proposition de cadre d'EIP en tenant compte à la fois des remarques du groupe de travail et de celles de l'ENISA. Le 12 janvier 2011, ce cadre révisé a été soumis pour approbation au groupe de travail « Article 29 » sur la protection des données.

Le présent avis constitue la réponse officielle du groupe de travail à cette nouvelle proposition.

Ci-après, la « recommandation RFID » désignera la recommandation de la Commission européenne sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence, publiée le 12 mai 2009. La « proposition révisée de cadre », ou simplement le « cadre », désignera le cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications RFID remis au groupe de travail « Article 29 » le 12 janvier 2011 et reproduit en annexe du présent avis.

Conclusions

Le groupe de travail approuve la proposition révisée de cadre présentée le 12 janvier 2011. Ce cadre prendra effet au plus tard six mois après la publication du présent avis.

Une EIP est un outil qui contribue à assurer le respect de la vie privée dès la conception (*privacy by design*), à mieux informer les particuliers, et qui favorise la transparence et le dialogue avec les autorités compétentes. Par conséquent, comme certaines applications RFID seront mises en œuvre dans plusieurs États membres, il est important que les rapports d'évaluation soient traduits et mis à la disposition des autorités compétentes dans leur langue officielle.

Le groupe de travail poursuivra sa contribution au dialogue à venir avec les entreprises, en améliorant et en clarifiant la structure et la mise en œuvre du cadre d'EIP des applications RFID sur la base de l'expérience acquise et des informations renvoyées par toutes les parties prenantes.

1.4. DONNÉES PERSONNELLES

Avis 14/2011 (WP186) sur les questions de protection des données relatives à la prévention du blanchiment de capitaux et du financement du terrorisme

Le groupe de travail « Article 29 » sur la protection des données (le « groupe de travail ») a formulé 44 recommandations concernant la protection de la vie privée et des données dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (« LBC/FT »). Ces recommandations ont été jointes en Annexe du présent avis.

Le groupe de travail 29 assurera un suivi des recommandations ci-jointes ainsi que des évolutions pertinentes dans la législation et les pratiques dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme et dans celui de la protection de la vie privée et des données.

Avis 15/2011 (WP187) sur la définition du consentement

Cet avis fournit une analyse approfondie du concept de consentement, tel qu'il est actuellement utilisé dans les directives « Protection des données » et « Vie privée et communications électroniques ». S'appuyant sur l'expérience des membres du groupe de travail « Article 29 », l'avis présente de nombreux exemples de consentement valable et non valable en se concentrant sur ses éléments fondamentaux tels que le sens des termes « manifestation de volonté », « libre », « spécifique », « indubitable », « explicite » et « informée », etc. Il précise aussi certains aspects liés à la notion de consentement, comme le moment où celui-ci doit être obtenu, la différence entre le droit d'opposition et le consentement, etc.

Le consentement est l'un des fondements juridiques du traitement de données à caractère personnel. Il joue un rôle important, mais cela n'exclut pas la possibilité que, compte tenu du contexte, d'autres fondements juridiques puissent être jugés plus appropriés par le responsable du traitement ou la personne concernée. S'il est utilisé à bon escient, le consentement est un instrument qui permet à la personne concernée de contrôler le traitement de ses données. S'il est mal utilisé, en revanche, le contrôle de la personne concernée devient illusoire et le consentement constitue alors une base inappropriée pour le traitement de données.

Cet avis répond notamment à une demande formulée par la Commission dans le cadre de la révision en cours de la directive « Protection des données ». Il contient donc des recommandations à prendre en compte aux fins de cette révision. Parmi celles-ci, on retiendra qu'il y a lieu:

i. De clarifier le sens de l'expression « consentement indubitable » et d'expliquer que seul un consentement fondé sur des déclarations ou des actions marquant un accord peut être considéré comme valable.

ii. D'exiger des responsables du traitement qu'ils mettent en place des mécanismes pour démontrer le consentement (dans le cadre de l'obligation générale de rendre compte).

iii. D'ajouter une exigence explicite concernant la qualité et l'accessibilité des informations servant de base au consentement, ainsi que.

iv. De considérer les propositions formulées concernant les mineurs et d'autres personnes juridiquement incapables.

Appréciation globale

Le groupe de travail considère que le cadre actuel de la protection des données comporte un ensemble bien pensé de règles fixant les conditions d'un consentement valable, pour légitimer un traitement de données. Ces conditions s'appliquent aussi bien à l'environnement hors ligne qu'à l'environnement en ligne. Plus particulièrement :

Le cadre actuel parvient à trouver un juste milieu entre une série de préoccupations. D'une part, il garantit que seul un consentement réel et informé soit réputé comme tel. À cet égard, l'Article 2(h), qui requiert explicitement que le consentement soit libre, spécifique et informé, est pertinent et satisfaisant. D'autre part, cette exigence n'est pas un carcan rigide, mais offre une souplesse suffisante en évitant des règles spécifiques sur le plan technique, comme l'illustre ce même Article 2(h), qui définit le consentement comme toute manifestation de la volonté de la personne concernée. Cela laisse une marge de manœuvre suffisante en ce qui concerne les façons dont cette manifestation peut être exprimée. Les Articles 7 et 8, qui requièrent, respectivement, un consentement indubitable et explicite, saisissent bien la nécessité de trouver un équilibre entre ces deux aspects, en apportant une certaine souplesse et en évitant des structures excessivement rigides tout en garantissant une protection.

Il en résulte un cadre qui, s'il est correctement appliqué et mis en œuvre, est de nature à s'adapter au large éventail de traitements de données qui découlent bien souvent de l'évolution technologique.

Or, dans la pratique, il n'est pas toujours aisé de déterminer quand un consentement est nécessaire et, plus précisément, quelles sont les conditions à satisfaire pour que le consentement soit valable, faute de règles uniformes dans les États membres. Les mesures de transposition adoptées dans les États membres ont abouti à des approches différentes. Des lacunes plus spécifiques ont été recensées lors des discussions du groupe de travail « Article 29 » qui ont donné lieu au présent avis. Ces lacunes sont décrites ci-après.

Modifications éventuelles

- La notion de consentement indubitable contribue à la mise en place d'un système qui, sans être exagérément rigide, offre un niveau élevé de protection. Si elle est de nature à déboucher sur un système raisonnable, elle est hélas souvent mal comprise ou purement et simplement ignorée. Si les explications et exemples donnés ci-dessus devraient contribuer à renforcer la sécurité juridique et la protection des droits des personnes concernées lorsqu'un consentement est utilisé comme base juridique, la situation actuelle semble néanmoins appeler un certain nombre de modifications;

- En particulier, le groupe de travail « Article 29 » considère que le libellé proprement dit (« indubitable ») mériterait d'être précisé dans le contexte de la révision du cadre général applicable à la protection des données. Cette clarification devrait insister sur le fait qu'un consentement indubitable impose de recourir à des mécanismes qui ne laissent aucun doute sur l'intention de la personne concernée de consentir au traitement. Dans le même temps, il conviendrait d'expliquer que l'utilisation d'options par défaut, que la personne concernée doit modifier pour refuser le traitement (consentement fondé sur le silence), ne constitue pas, en soi, un consentement indubitable. Cette observation vaut tout particulièrement dans l'environnement en ligne;

- Outre ce besoin de clarification, le groupe de travail « Article 29 » formule les propositions suivantes:

  i. *Premièrement*, inclure dans la définition du consentement visé à l'Article 2(h), le qualificatif « indubitable » (ou un équivalent) afin de renforcer l'idée que seul un consentement fondé sur

une déclaration ou une action destinée à marquer un accord constitue un consentement valable. En plus de clarifier les choses, cet ajout permettrait d'aligner la notion de consentement au sens de l'Article 2(h), sur les conditions de validité du consentement énoncées à l'Article 7. En outre, la signification de l'adjectif « indubitable » pourrait être précisée dans un considérant du futur cadre juridique.

ii. *Deuxièmement*, dans le cadre de l'obligation générale de rendre compte, les responsables du traitement devraient être en mesure de démontrer qu'un consentement a été obtenu. En effet, si la charge de la preuve est renforcée de telle sorte que les responsables du traitement soient tenus de prouver qu'ils ont effectivement obtenu le consentement de la personne concernée, ils seront contraints de mettre en place des pratiques et des mécanismes types pour demander un consentement indubitable et le prouver. La nature de ces mécanismes dépendra du contexte et devrait tenir compte des faits et des circonstances liées au traitement et, plus particulièrement, des risques qu'il comporte.

- Le groupe de travail « Article 29 » n'est pas persuadé que le cadre juridique doive exiger un consentement explicite en tant que règle générale pour tous les types de traitement, y compris ceux actuellement couverts par l'Article 7 de la directive. Il considère en effet qu'un consentement indubitable pouvant consister soit en un consentement explicite soit en un consentement découlant d'*actions* indubitables devrait rester la norme. Ce choix offrirait aux responsables du traitement une plus grande souplesse dans l'obtention du consentement, et la procédure complète pourrait s'en trouver accélérée et devenir plus facile à utiliser;

- Plusieurs aspects du cadre juridique applicable au consentement sont déduits du libellé, de la genèse législative ou ont été développés par la jurisprudence et les avis du groupe de travail « Article 29 ». Néanmoins, la sécurité juridique se verrait renforcée si ces aspects étaient expressément intégrés dans le nouveau cadre législatif applicable à la protection des données. Les éléments suivants pourraient être pris en compte:

  i. L'insertion d'une clause expresse instituant le droit de la personne concernée à retirer son consentement.

  ii. Le renforcement de la notion selon laquelle le consentement doit être donné avant le début du traitement ou avant toute utilisation ultérieure des données pour des finalités qui n'étaient pas couvertes par le consentement initial, lorsqu'il n'existe pas d'autre fondement juridique au traitement.

  iii. L'ajout d'exigences explicites concernant la qualité (obligation de fournir des informations sur le traitement des données d'une manière aisément compréhensible et dans un langage clair et simple) et l'accessibilité des informations (obligation que les informations soient évidentes, visibles et directement accessibles). Ceci est essentiel pour permettre aux personnes concernées de prendre une décision en toute connaissance de cause.

- Enfin, s'agissant des personnes ne jouissant pas de la capacité juridique, des dispositions pourraient être prévues afin de renforcer leur protection, par exemple:

  i. Des précisions sur les circonstances dans lesquelles le consentement des parents ou du tuteur légal d'une personne incapable est requis, y compris l'âge en dessous duquel ce consentement serait obligatoire.

  ii. L'obligation d'utiliser des mécanismes de vérification de l'âge, qui pourraient varier en fonction de circonstances telles que l'âge de l'enfant, la nature du traitement, les risques possibles, la

conservation ou non des informations par le responsable du traitement ou encore leur transmission ou non à des tiers.

iii. L'obligation d'adapter les informations fournies aux enfants dans la mesure où cela leur permettrait de mieux comprendre ce que recouvre la collecte de données et faciliterait leur décision de consentir ou non au traitement.

iv. Des garanties spécifiques à certains traitements de données, tels que la publicité comportementale, pour lesquels le consentement ne devrait pas pouvoir servir de fondement pour légitimer le traitement de données à caractère personnel.

Le groupe de travail « Article 29 » réexaminera la question du consentement. Plus précisément, les autorités nationales chargées de la protection des données et le groupe de travail pourraient décider ultérieurement d'élaborer des lignes directrices sur la base du présent avis, en donnant des exemples concrets supplémentaires.

Document de travail 01/2011 (WP184) concernant le cadre juridique relatif aux violations de données à caractère personnel actuellement en vigueur dans l'UE et présentant des recommandations quant aux actions à entreprendre à l'avenir

Le présent document du groupe de travail « Article 29 » fait le point de la situation et passe en revue la manière dont les États membres transposent dans leur législation nationale les dispositions relatives aux violations de données à caractère personnel de la directive « Vie privée et communications électroniques »[8].

Cet exercice poursuit trois objectifs.

Premièrement, le groupe de travail « Article 29 » souhaite avoir une vue d'ensemble de la situation actuelle dans ce domaine. Celle-ci englobe à la fois des éléments fondamentaux, comme la situation en matière de transposition, et des questions plus complexes, relevant des différences d'approche initiale dans certains domaines (portée de l'obligation, adoption prévue ou non de lignes directrices nationales développant certains aspects de la directive « Vie privée et communications électroniques », autorité nationale compétente, etc.). Même à ce stade tardif, l'identification des différences d'approche qui se dessinent au niveau national pourrait aider les États membre à aligner leurs vues et à assurer une mise en œuvre uniforme.

Deuxièmement, ces travaux permettent aux autorités nationales chargées de la protection des données de prendre connaissance des conclusions formulées et ont attiré leur attention sur la nécessité d'entreprendre les activités de suivi décrites dans le présent document de travail. Il en ressort que les autorités compétentes doivent poursuivre les efforts visant à définir les règles et procédures internes auxquelles les responsables du traitement sont soumis lorsqu'ils notifient des violations aux particuliers et aux autorités compétentes. De plus, étant donné que les responsables du traitement seront de plus en plus souvent amenés à notifier des violations transfrontalières de données à caractère personnel, il est indispensable que les autorités définissent ensemble une méthode de coopération.

En outre, cet exercice a permis au groupe de travail « Article 29 » de poursuivre ses réflexions sur la question et de parvenir à une série de conclusions quant aux mesures qui devraient être prises dans le

[8] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, Journal Officiel L337/11, 18.12.2009.

domaine de la notification des violations de données à caractère personnel. Ces conclusions, qui viennent compléter les avis émis sur le sujet à d'autres occasions par le groupe de travail « Article 29 »[9], s'appuient sur l'expérience acquise dans le domaine de la notification des failles de sécurité par les autorités nationales chargées de la protection des données à caractère personnel qui se conforment déjà aux exigences en matière de notification des violations de données à caractère personnel. Le groupe de travail « Article 29 » souhaite que ces conclusions soient prises en compte dans le cadre des mesures qui seront prises à l'avenir en matière de violations de données à caractère personnel. De telles mesures sont notamment attendues à deux égards:

a) Pour compléter le cadre juridique relatif aux violations de données à caractère personnel instauré par la directive « Vie privée et communications électroniques ». L'Article 4(5) de cette directive délègue à la Commission le pouvoir d'adopter des mesures techniques d'application (depuis l'adoption du traité de Lisbonne, il s'agit des « pouvoirs délégués » en vertu de l'article 290 du TFUE) en vue d'assurer, à certains égards (à savoir les circonstances, le format et les procédures applicables aux exigences en matière d'information et de notification), une mise en œuvre et une application cohérentes du cadre juridique relatif aux violations de données à caractère personnel;

b) Pour élargir le cadre juridique relatif aux violations de données à caractère personnel de la directive « Vie privée et communications électroniques » à l'occasion de la révision de la directive 95/46. La Commission s'est engagée devant le Parlement européen à lancer sans retard les travaux préparatoires appropriés, y compris une consultation des parties prenantes, afin de soumettre des propositions adéquates en la matière d'ici la fin 2011... [10]. Elle a confirmé cet engagement dans sa communication intitulée « Une approche globale de la protection des données à caractère personnel dans l'Union européenne »[11].

Les éléments évoqués ci-dessus sont présentés de la manière suivante : après une synthèse des principaux éléments des dispositions en matière de violations des données à caractère personnel contenues dans la directive « Vie privée et communications électroniques » (section II), le présent document de travail résume la législation applicable en la matière dans les États membres (section III). Ce résumé s'appuie sur les informations communiquées par les autorités nationales chargées de la protection des données (ci-après « DPA »), qui ne seront pas reproduites ici étant donné que la situation en matière de transposition ne cesse d'évoluer. La Section IV présente plusieurs mesures à mettre en œuvre par les autorités compétentes et par le groupe de travail « Article 29 » en vue de développer des procédures internes et d'instaurer des procédures de coopération. Les Sections V et VI, qui sont consacrées aux actions futures, rappellent la portée générale des mesures attendues en matière de violations de données à caractère personnel, décrivent les procédures à respecter et formulent des recommandations stratégiques.

L'avis exprimé dans le présent document est sans préjudice des éventuelles lignes directrices plus spécifiques qui pourraient être publiées à l'avenir, notamment dans le cadre des mesures techniques d'application adoptées par la Commission en vertu de l'Article 4(5) de la directive « Vie privée et communications électroniques ».

---

[9] Voir le document du groupe de travail « Article 29 » intitulé « L'avenir de la protection de la vie privée : Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel », adopté le 1.12.2009 (WP 168) ; l'Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive « Vie privée et communications électroniques »), adopté le 10.2.2009 (WP 159) ; et l'Avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (directive « Vie privée et communications électroniques »), adopté le 15.5.2008 (WP 150).

[10] Voir la déclaration de la Commission concernant la notification de violations de données présentée au Parlement européen en 2009 dans le contexte de la réforme du cadre réglementaire relatif aux communications électroniques. Consultable sur http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-ta-2009-

[11] COM(2010) 609 final, adopté le 4.11.2010.

Chapitre deux

Principaux développements au sein des États membres

ALLEMAGNE

A. Résumé des activités et actualités

Veuillez noter ce qui suit : En Allemagne, le Commissaire fédéral à la protection des données et au droit à l'information n'est pas la seule entité agissant en tant qu'autorité chargée de la protection des données. Au niveau des États fédérés (« *Länder* »), il existe des bureaux des Commissaires à la protection des données et la Bavière possède en outre une autorité de contrôle distincte dédiée au secteur privé.

Le tableau ci-dessous ne concerne que le bureau du Commissaire fédéral à la protection des données et au droit à l'information.

Organisation	Commissaire fédéral à la protection des données et au droit à l'information
Président et/ou collège	Peter Schaar
Budget	8 765 000 EUR
Personnel	85 au total Bureau central : 4 Département I : 4 Département II : 13 Département III : 8 Département IV : 7 Département V : 6 Département VI : 9 Département VII : 7 Département VIII : 9 Département IX : 4 Services centraux : 12 Bureau de presse : 2
Activités générales	
Décisions, avis, recommandations	s. o.

Notifications	s. o.
Examens préalables	s. o.
Demandes émanant des personnes concernées	9 143
Plaintes émanant des personnes concernées	5 161
Conseils sollicités par le Parlement ou le gouvernement	s. o.
Autres renseignements relatifs aux activités générales	s. o.
Activités d'inspection	
Contrôles, enquêtes	s. o.
Activités de sanction	
Sanctions	s. o.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	s. o.

1. Protection des données dans le secteur de l'emploi

En Allemagne, le Bundestag débat encore sur le projet de loi sur la protection des données dans le secteur de l'emploi (complétant la loi fédérale sur la protection des données). Toutefois, compte tenu de l'Article 82 du projet de proposition de l'UE d'un Règlement pour la protection des données générales, on peut se demander si cette loi sera adoptée.

2. Mise en œuvre de la Directive 2005/60/CE – Loi sur l'amélioration de la prévention du blanchiment d'argent

La Loi sur l'amélioration de la prévention du blanchiment d'argent du 22 décembre 2011 (Journal officiel fédéral I 2011, 2959) révise en profondeur la Loi sur le blanchiment d'argent (GwG). Plus important, le principe de diligence raisonnable, les exigences de comptes rendus et les mesures de sécurité internes ont été intensifiés et étendus, et le cercle de ceux qui doivent respecter ces obligations a été élargi. La nouvelle loi a fait baisser le seuil d'intervention en cas de violations des obligations de diligence raisonnable.

Étendre les obligations de diligence raisonnable signifie également que les entreprises, les institutions ou les personnes soumises à cette obligation en vertu de la GwG doivent répondre à des exigences de stockage ou de recueil de données plus complètes, ce qui augmente également leurs charges administratives. Les amendes considérables imposées en cas de violations de l'obligation de diligence raisonnable devraient également faire monter la pression de manière à ce que ceux qui doivent la respecter soient plus enclins à recueillir les données de leurs partenaires contractuels et, si nécessaire, à les transmettre à l'Office fédéral de la police judiciaire et aux autorités policières afin d'éviter ces amendes. Cette approche sape également les principes de restriction et d'économie des données, dans la mesure où la combinaison des obligations de diligence raisonnable étendues et de sanctions plus sévères entraîne la collecte de données encore plus nombreuses. Le fait d'augmenter le nombre de secteurs économiques devant respecter ces obligations peut également entraîner le risque d'une collecte de données exhaustive lors de transactions financières. Par ailleurs, le seuil de suspicion des rapports de transactions a été considérablement réduit. En général, le fait d'introduire des obligations de diligence raisonnable plus strictes et de réduire le seuil de suspicion des transactions constitue une sérieuse interférence avec le droit d'une personne de déterminer l'utilisation de ses données découlant de l'Article 2(1) en conjonction avec l'Article 1(1) de la loi de base (GG), les transactions financières faisant de plus en plus l'objet d'une transparence forcée et exhaustive. Il existe par conséquent un risque que la grande portée de la collecte de données personnelles prévue par la loi (quels que soient les niveaux de suspicion) entraîne un contrôle excessif des transactions financières, dans la mesure où les entreprises, les institutions ou les personnes soumises à cette obligation sont encore plus enclines à recueillir des données de manière proactive et à les transmettre aux autorités policières.

B. Informations sur la jurisprudence

1. Dans son jugement du 12 octobre 2011, 2 BvR 236/08, le Tribunal constitutionnel fédéral a décidé la révision des mesures d'enquête discrète dans le cadre des procédures pénales, y compris la différenciation relative à la protection des communications avec des personnes liées par le secret professionnel. Les communications avec la presse et les médecins, par exemple, sont généralement moins bien protégées que les communications avec les membres du clergé. Les règles de protection du noyau inviolable de la sphère privée d'un individu dans le cadre de l'interception de télécommunications ont également été approuvées par le tribunal. Cet amendement a été accueilli par de nombreuses critiques.

2. Dans son jugement du 24 janvier 2012, le Tribunal constitutionnel fédéral a établi qu'une demande d'informations sur les données de télécommunications requiert en toutes circonstances une autorisation de transmission des données et un motif juridique pour la demande. C'est la raison pour laquelle le stockage et la transmission des données de télécommunications aux autorités en charge des enquêtes ont été déclarés anticonstitutionnels, ces autorités ayant accès aux mots de passe et codes PIN. Dès lors, les autorités en charge des enquêtes sont en mesure de lire et de rechercher les données stockées sur un téléphone mobile confisqué alors qu'il n'était pas clairement établi si les autorités étaient autorisées à procéder de la sorte.

Par ailleurs, le Tribunal constitutionnel fédéral a clarifié le fait qu'une demande d'informations sur le souscripteur d'une adresse IP dynamique constitue une violation de la vie privée dans le domaine des télécommunications. Pour identifier une adresse IP dynamique, les entreprises de télécommunications doivent rechercher les données d'appels de leurs clients et accéder à des procédures de télécommunications spécifiques soumises à l'Article 10 de la loi de base. Les législateurs allemands doivent créer des dispositions claires à ce sujet assurant la protection de données d'appels extrêmement sensibles.

C. Autres informations importantes

Projet de loi pour la promotion de l'administration en ligne (loi sur l'administration en ligne)

À l'heure actuelle, un projet de loi pour la promotion de l'administration en ligne (la Loi sur l'administration en ligne), fait l'objet de débats. Cette loi vise à supprimer les obstacles juridiques et à faciliter les communications électroniques, notamment entre les citoyens et l'administration publique. Pour l'essentiel, cet objectif sera atteint grâce à l'adoption de procédures techniquement sûres pour remplacer les documents écrits, telles que l'inclusion de la nouvelle fonctionnalité de carte d'identité en ligne et des possibilités de communications sûres et éprouvées sur Internet. Le projet de loi comprend également les points suivants :

- Demander à l'administration publique de prévoir un accès électronique;
- Permettre aux citoyens de fournir des preuves électroniques dans le cadre de procédures administratives;
- Introduire les fichiers électroniques au niveau des autorités fédérales;
- Fournir des données lisibles par les machines de l'administration (« données publiques ouvertes »).

Le débat sur le projet de loi portera également sur la garantie que la levée des obstacles à la mise en œuvre de processus administratifs électroniques sans incohérence des supports n'entraîne pas une réduction du niveau de protection des données garanti par l'administration publique. C'est la raison pour laquelle la priorité est de concevoir et d'organiser des processus techniques conformes aux normes de protection des données.

.

AUTRICHE

A. Nouveaux développements et activités

Pendant la période de compte rendu, le projet de loi du gouvernement en faveur d'un **amendement de la Loi sur la juridiction administrative [Verwaltungsgerichtsbarkeits-Novelle] 2012** a été adopté.[12] Cet amendement prévoit la dissolution de certaines autorités administratives indépendantes (dont la Commission de la protection des données) fin 2013, et le transfert de leurs activités judiciaires vers des tribunaux administratifs nouvellement créés. La Commission de la protection des données a plusieurs fois critiqué la proposition de sa dissolution. Si la Commission de la protection des données est dissoute, une nouvelle autorité de protection des données devra être établie sur la base de l'Article 28 de la Directive 95/46/CE, et les tâches de la Commission de la protection des données devront lui être transférées. L'idée originale du transfert de décisions juridiques formelles vers un tribunal administratif semble problématique, que ce soit au regard des « pouvoirs effectifs d'intervention » mentionnés à l'Article 28 de la Directive 95/46/CE, mais également de la tendance qui se dégage dans le projet de « Règlement général de protection des données », conçu pour renforcer les autorités de protection des données et normaliser les compétences des autorités européennes de protection des données. Cela pourrait impliquer qu'une procédure juridique passe de l'autorité de protection des données vers un tribunal administratif.

Pendant la période de compte rendu, le projet de « **Loi sur les dossiers médicaux électroniques** » **[ELGA-G]** a été publié par le ministère fédéral de la Santé, auquel la Commission de la protection des données a adressé une réponse détaillée [13]. Le document de travail WP 131 du groupe de travail « Article 29 » sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME) de 2007 a joué un rôle important dans la rédaction du projet de loi. Le projet de loi a par la suite connu de nombreuses révisions.[14]

Pendant la période de compte rendu, la Commission de la protection des données a coopéré à un **projet de jumelage portant sur la protection des données au Monténégro**. L'un des objectifs des projets de jumelage européens est de partager l'expertise des autorités établies concernant la création et l'expansion de structures publiques, avec les pays qui sont ou seront candidats à l'accession. Dans le cas présent, les membres de la Commission de la protection des données et son personnel administratif ont partagé leur expertise dans le cadre de projets à court terme. Le directeur de la Commission de la protection des données a également joué le rôle de gestionnaire de projet pour l'Autriche dans les derniers mois du projet. En 2011, des représentants de l'autorité monténégrine de protection des données ont effectué une visite d'étude auprès de la Commission de la protection des données à Vienne.

Pour la **Journée européenne de la protection des données 2011**, un événement, déjà érigé au rang de tradition et essentiellement consacré à l'avenir de la protection des données à l'ère d'Internet, a été organisé avec le Conseil de la protection des données et la chancellerie fédérale. L'un des sujets particuliers développés lors de cet événement concernait la stratégie de la Commission européenne en faveur d'un nouveau cadre juridique de protection des données.

Organisation	Commission autrichienne de la protection des données
Président et/ou collège	Président : Dr Anton SPENLING

12 Celui-ci a été adopté par l'Assemblée nationale et le Conseil fédéral et publié dans le Journal officiel fédéral (BGBl.) I 51/2012.
13 voir http://www.dsk.gv.at/DocView.axd?CobId=42793
14 Le projet de « Loi sur les dossiers médicaux électroniques » du gouvernement a été adopté en octobre 2012.

	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	84 décisions formelles (plaintes), 220 dossiers déposés auprès du Médiateur, 43 autorisations (transfert de données vers des pays tiers, recherches et enquêtes), 155 décisions formelles dans le cadre de la procédure de notification et 3 recommandations formelles.
Notifications	12 542
Examens préalables	2 167
Demandes émanant des personnes concernées	Par écrit : 1 327 Par téléphone : environ 25 000
Plaintes émanant des personnes concernées	Plaintes ayant mené à une décision formelle : 84
Conseils sollicités par le Parlement ou le gouvernement	Plaintes ayant mené à un éclaircissement ou à une recommandation : 220
Autres renseignements relatifs aux activités générales	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.
Activités d'inspection	
Contrôles, enquêtes	13, la plupart en matière de vidéosurveillance.
Activités de sanction	
Sanctions	Aucune. La DPA autrichienne ne peut imposer de 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. Jurisprudence

Pendant l'année de compte rendu, la procédure d'enregistrement de **Google Street View**, déployée en 2010, a été complétée. La Commission de la protection des données a approuvé l'enregistrement de Google Street View et émis trois recommandations à l'attention de Google Inc. L'extrait du registre et les recommandations ont été adressés à Google Inc. le 21 avril 2011. L'enregistrement a conclu la procédure de détermination des principaux faits relatifs à l'application « Google Street View » enregistrée par Google Inc. (application de cartographie et de publication dans « Google Street View »). Dans le cadre de ce processus, Google Inc. a apporté les améliorations demandées à l'enregistrement.

Outre les engagements déjà pris par Google Inc. lors du processus d'enregistrement et d'audit (notamment, de cacher les visages et les numéros d'immatriculation des véhicules avant de publier les données sur Internet et de fournir les informations au public), les recommandations suivantes ont été faites à Google Inc. :

a) Si des personnes sont photographiées dans des endroits particulièrement sensibles, non seulement les visages, mais également l'image entière des personnes, doivent être rendus méconnaissables. Ces lieux comprennent, notamment, les parvis des églises et autres lieux de culte, les entrées des hôpitaux, des foyers pour femmes et des prisons.

b) Les photographies de propriétés privées qui ne sont pas visibles par les passants, telles que les cours et jardins privés clôturés, doivent être occultées avant leur publication sur Internet.

c) D'après la Section n° 28(2) de la Loi relative à la protection des données [DSG] 2000, la personne concernée dispose d'un droit d'opposition à partir du moment où les données sont collectées. Afin de permettre à la personne concernée de s'opposer à la publication de bâtiments avant même la publication de l'image, les outils appropriés doivent être fournis afin de faciliter l'affirmation simple et non bureaucratique du droit d'opposition. Le droit d'opposition (avant même la publication) et l'outil d'exercice de ce droit doivent également être mentionnés sur le site web de Google Inc.

Les recommandations a) et b) doivent être mises en œuvre au plus tard au moment de la publication des données sur Internet. L'outil et la référence qui y est faite selon la recommandation c) doivent être en place au moins douze semaines avant la publication des données sur Internet.

Google n'a pour l'instant pas publié sur Internet ses données Street View déjà collectées. Selon toute vraisemblance, aucun autre passage des véhicules Street View n'a eu lieu en Autriche.

Dans une plainte, la Commission de la protection des données a discuté des **contrôle d'identité dans le cadre de l'exercice du droit à l'information**. Un demandeur d'informations ayant déjà prouvé son identité en envoyant une copie de sa carte d'identité et un fax de sa signature (outre la demande d'information signée) s'est également vu demander par le client de fournir les prénoms de ses parents afin d'obtenir les informations demandées. La Commission de la protection des données a considéré la preuve d'identité déjà fournie comme étant suffisante. Le fait d'insister pour que soient donnés les prénoms des parents du plaignant et de ne pas communiquer les informations sur la protection des données malgré la preuve d'identité déjà fournie constitue une violation du droit à l'information du plaignant quant à ses propres données.

BELGIQUE

A. Résumé des activités et actualités

Cybersurveillance sur le lieu de travail

La question du contrôle de l'utilisation d'Internet et de courriers électroniques sur le lieu de travail n'a cessé de se poser à la Commission de la protection de la vie privée (CPVP) ces dernières années. Questions, plaintes et demandes de recommandations, de lignes de conduites à suivre pour définir une politique d'entreprise qui soit à la fois légale et praticable, lui étaient régulièrement adressées.

La CPVP a donc pris l'initiative de se prononcer sur ces questions en publiant dans un premier temps, courant 2011, un rapport d'analyse approfondie de la problématique, une sorte de «Livre vert» contenant les éléments sur lesquels s'appuient une série de recommandations pratiques publiées, après une large consultation publique, en mai 2012. Voir sur le site Internet de la CPVP: http://www.privacycommission.be/fr/brochure-information-cybersurveillance

La CPVP y exprime que ces contrôles trouvent leur fondement légitime dans l'autorité sous laquelle l'employé exerce ses prestations en faveur de l'employeur auquel il est lié par un contrat de travail (lien de subordination contractuel). En exécution de son contrat de travail, le travailleur communique par voie électronique avec des tiers, utilisant pour ce faire le système informatique mis à sa disposition par son employeur. Le résultat du travail accompli, réalisé par le biais de l'utilisation des outils informatiques, parmi lesquels Internet et la messagerie de l'employeur, doit évidemment être fourni à ce dernier. L'employeur devrait pouvoir recevoir ces informations de la personne concernée ou devrait pouvoir les rechercher afin d'en prendre connaissance en vue d'assurer la continuité du service et le bon fonctionnement de l'entreprise, en particulier en cas d'absence, de décès ou de départ du travailleur de l'entreprise.

Ces contrôles n'en doivent pas moins s'exercer dans le respect des dispositions légales applicables, dont la *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (La Loi vie privée). Nonobstant ces obligations, l'employeur doit être/rester en mesure de préserver efficacement ses intérêts légitimes (gestion et organisation de ses activités).

Vers plus de transparence en matière d'enquêtes marketing

Comme il l'avait déjà fait à plusieurs reprises par le passé, le département marketing de La Poste (Bpost) a lancé en 2011 une enquête à grande échelle auprès de millions d'habitants en Belgique. Bpost souhaitait ainsi établir un profil de ses clients, afin de pouvoir mener des actions de marketing direct. Les données sont vendues à des entreprises qui envoient ensuite des publicités ciblées. L'enquête publicitaire de La Poste a été jugée agressive, peu transparente, voire trompeuse aux yeux de la CPVP, Bpost mentionnant par exemple trop peu clairement qu'il n'était pas obligatoire de remplir cette enquête purement «marketing». L'enquête était par ailleurs envoyée dans une enveloppe de couleur brune, très similaire à celle utilisée pour l'envoi des déclarations fiscales et précisément à la période de l'envoi de ces mêmes déclarations. Alertée par le public, notamment par des personnes âgées «mises sous pression» par la nature de ce questionnaire, la CPVP a engagé des négociations avec La Poste qui ont permis l'établissement d'un questionnaire et d'une information davantage transparents dans le respect des intérêts légitimes de chacun.

Pour le surplus, l'ensemble des activités de la CPVP est repris dans son Rapport annuel 2011 disponible à l'adresse: http://www.privacycommission.be/sites/privacycommission/files/documents/rapport-annuel-2011.pdf

Organisation	
Président et/ou collège	Nom du président et, le cas échéant, composition du collège. Président : W. Debeuckelaere (magistrate) Vice-président : S. Verschuere Collège effectif : M. Salmon (conseillère Cour d'appel), S. Mertens de Wilmars (enseignant), A. Vander Donckt (notaire), F. Robben (administrateur général de la Banque Carrefour de la sécurité sociale et de la plate-forme e-health), P. Poma (magistrat), A. Junion (avocate). Pour les membres suppléants, voir le site Internet de la CPVP(http://www.privacycommission.be) et son Rapport annuel 2011. Voir aussi l'article 24 § 4 alinéas 3 et 4: *« La Commission est composée de telle façon qu'il existe en son sein un équilibre entre les différents groupes socio-économiques. Outre le président, la Commission comprend au moins, parmi ses membres effectifs et parmi ses membres suppléants, un juriste, un informaticien, une personne pouvant justifier d'une expérience professionnelle dans la gestion de données à caractère personnel relevant du secteur privé, et une personne pouvant justifier d'une expérience professionnelle dans la gestion de données à caractère personnel relevant du secteur public ».*
Budget	Budget alloué et exécuté Budget alloué : 5 516 000 EUR (2011) / 5 684 000 EUR (2012)
Personnel	Nombre de membres du personnel (le cas échéant, par secteur d'emploi) : 52 employés (1 Président – 1 Vice-président) Chefs de sections: 3 Personnel et Organisation (20): comptable (1), traducteurs (5), secrétariat administratif (8), statistiques (1), responsable du personnel (1), logistique (2), support informatique (1), responsable de la communication (1) Etudes et Recherches (18) conseillers juridiques (16), spécialiste IT (1), documentaliste (1) Relations extérieures (Front Office) (11): conseillers juridiques (4), assistants (7)

Activités générales	
Décisions, avis, recommandations	Nombre d'avis et de questions clés : nous compterons ici tout texte produit par les DPA ayant un effet sur la protection des données en général, sur les personnes concernées ou les responsables du traitement de données. Avis (à la demande du pouvoir législatif ou exécutif – voir ci-dessous) : 29 Avis et recommandations d'initiative: 14 Recommandations dans le cadre des déclarations de traitements ultérieurs: 10
Notifications	Nombre de notifications, le cas échéant, conformément à la définition de la législation nationale. En 2011, les responsables de traitement ont introduit 7 169 dossiers de déclarations via l'e-guichet, ce qui représente une augmentation de 92 % par rapport au nombre de dossiers de déclarations introduit en 2010. En 2011, 6 490 nouveaux traitements de données ont été déclarés: - Déclaration ordinaire (19 %) - Déclaration via DPR (adhésion à une déclaration introduite par un organisme « coupole » par exemple) - Déclaration de traitement ultérieur (1 %) - Déclaration thématique pour l'installation et l'utilisation d'une caméra de surveillance (52 %) 372 déclarations de modifications de traitements déjà déclarés 124 corrections de déclaration 306 déclarations de fin de traitement Les principales finalités visées par les traitements déclarés ont été: « surveillance et contrôle » (2 850) ; « surveillance et contrôle des personnes qui travaillent sur un lieu de travail surveillé » (520); « finalités générales» (542), « soins de santé » (104), « autres finalités » (2 043).
Examens préalables	Nombre de contrôles préalables, le cas échéant, compris au sens de la définition de la législation nationale. Même si l'activité d'autorisation des comités sectoriels ne reflète pas exactement l'objet de l'article 20 de la directive 95/46/CE, les

	différents comités sectoriels établis au sein de la Commission ont rendu le nombre d'autorisations suivant : - Comité sectoriel Autorité fédérale: 108 (individuelles et adhésions à des autorisations générales) - Comité sectoriel statistiques: 35 (individuelles) - Comité sectoriel du Registre national: 286 (individuelles et adhésions à des autorisations générales) - Comité sectoriel de la sécurité sociale et de la santé: - Section santé : avis (1) — délibérations (34) - Section sécurité sociale : avis (23) — délibérations (87)
Demandes émanant des personnes concernées	Nombre de demandes reçues par écrit ou par téléphone, le cas échéant, de la part des personnes concernées Les statistiques de la Commission belge de la protection de la vie privée ne font pas de distinction selon que les demandes d'information proviennent de personnes concernées ou de responsables de traitement : Information données par le Front Office: 3 042 dossiers « Questions — réponses » ouverts en 2011 (droit à l'image, principes de protection de la vie privée, économie / crédit à la consommation, vie privée sur le lieu de travail et autorités publiques. La CPVP a en outre traité 2 866 demandes d'information ou de médiation (y compris des dossiers de contrôle) : Ces dossiers peuvent être répartis comme suit : 2447 demandes d'informations émanant tant d'instances publiques et de responsables de traitement actuels ou futurs que de personnes concernées, 296 demandes de médiation et 123 dossiers de contrôle.
Plaintes émanant des personnes concernées	Nombre de plaintes qualifiées (le cas échéant, par type) : Voir supra : 296 demandes de médiation: avant toute médiation ou communication d'information, la CPCP procède toujours à une analyse de recevabilité. Pour 153 dossiers, la demande de médiation s'est avérée irrecevable, souvent en raison d'un manque d'information de la personne concernée (148 dossiers). 215 demandes, soit 9 % ont été adressées erronément à la Commission de la protection de la vie privée, qui s'est toujours efforcée d'orienter le demandeur vers l'institution compétente. Dans près de 75 % des cas, la CPVP y est parvenue. Dans 75 % des questions traitées, des informations relatives à la vie privée ont été communiquées. Dans 3,85 % des dossiers, la plainte s'est avérée infondée ; par contre dans 5,01 % des dossiers,

	une infraction à la vie privée a été constatée et une correction a été obtenue.
Conseils sollicités par le Parlement ou le gouvernement	Tout document texte produit à la demande du Parlement ou du Gouvernement ou produit à l'intention du Gouvernement : La liste des avis émis par la Commission belge en 2011 est disponible sur son site Internet à l'adresse : http://www.privacycommission.be
Autres renseignements relatifs aux activités générales	Nombre de « catégories d'activités pertinentes à déterminer par les DPA » Tout chiffre pertinent reflétant l'activité des DPA, par exemple le nombre de règles d'entreprise contraignantes (BCR) approuvées par les DPA. Voir le rapport annuel de la Commission belge de la protection de la vie privée qui comprend un volet « statistiques » important et détaillé. Ce rapport annuel est disponible sur le site Internet de la Commission: http://www.privacycommission.be
Activités d'inspection	
Contrôles, enquêtes	Nombre de contrôles et/ou d'enquêtes (par questions clés, si possible) ; le cas échéant, conformément à la législation nationale. 123 contrôles (voir infra). Les thèmes les plus fréquemment abordés (information, médiation/plainte et contrôles) sont les suivants : • Traitement d'images dont, surtout, vidéosurveillance • Principes de la protection de la vie privée • Traitements de données par des autorités publiques • Pratiques commerciales (principalement marketing)
Activités de sanction	
Sanctions	Nombre de sanctions décidées par la DPA (si prévues par le droit national) Nombre de procédures juridiques engagées par la DPA à l'encontre des responsables du traitement des données (si prévues par le droit national) La CPVP ne dispose pas de compétence de sanction propre. Elle peut toutefois transmettre les dossiers dans lesquels elle constate des infractions au parquet.

Amendes	Montants (indication si imposées par un tribunal ou DPA) : La CPVP ne dispose pas de compétence de sanction propre. Elle peut toutefois transmettre les dossiers dans lesquels elle constate des infractions au parquet.
DPD	
Chiffres relatifs aux DPD	Différents chiffres sont admissibles suivant les informations disponibles dans les États membres. Si non prévu par le droit national, la cellule devra comporter la mention « s. o. ». La CPVP ne dispose pas de cette information.

B. Informations sur la jurisprudence

Google poursuivi par le parquet dans le cadre de « l'incident WI-FI » de Google Street View

La CPVP n'est pas habilitée à imposer des amendes aux responsables de traitements qui contreviennent à la « Loi vie privée ». Elle n'en est pas moins tenue de dénoncer au Procureur du Roi (parquet) les infractions dont elle a connaissance. S'agissant de l'incident « Wi-Fi – Google Street View » soit la capture de données personnelles « WI-FI » (nom du réseau, URL, emails entiers et mots de passe parfois également) via des réseaux non protégés par les « Google cars » équipés pour prendre des clichés panoramiques en vue d'alimenter Google Street View, la CPVP a saisi le parquet fédéral. Google a reconnu son erreur et a accepté la proposition de transaction du parquet belge d'un montant de 150 000 EUR.

BULGARIE

A. Résumé des activités et actualités

Organisation	
Président et/ou collège	Commission de protection des données personnelles (CPDP), sa Présidente Mme Veneta Shopova et quatre membres : M. Krassimir Dimitrov, M. Valentin Enev, Mme Mariya Mateva et M. Veselin Tselkov.
Budget	Budget alloué : 2 560 000 BGN (devise bulgare), budget exécuté : 2 344 993 BGN.
Personnel	Nombre d'employés : 76
Activités générales	
Décisions, avis, recommandations	En 2011, 203 décisions ont été publiées, dont 50 étaient des avis et 30 des instructions contraignantes affectant principalement les parties aux procédures administratives. Par ailleurs, la période entre leur publication et leur prise d'effet a été trop courte pour que le responsable du traitement des données puisse tenir compte des recommandations de la CPDP et modifier et améliorer son travail sur la protection des données personnelles. Des parties de ces lois ont fait l'objet de recours devant le tribunal, dont les audiences se poursuivent et retardent l'entrée en vigueur.
Notifications	42 911 responsables du traitement des données personnelles
Examens préalables	1 151
Demandes émanant des personnes concernées	Au total, 458 demandes, plaintes et notifications, dont 102 étaient des demandes, et 15 des plaintes. D'après les demandes reçues, la plupart des allégations de violations de droits relevant de la loi relative à la protection des données à caractère personnel (LPPD) concernaient les secteurs suivants : télécommunications (15), Internet (12), administration publique (11), commerce et services (10). Les déclarations portant sur le secteur financier (5), les médias (2), la santé (2) et les partis politiques (2) sont visiblement moins nombreuses.
Plaintes émanant des personnes concernées	341 – dans les domaines des télécommunications et de la société de l'information – 199 ; des médias – 8 ; de la santé – 5 ; des banques et institutions bancaires – 27 ; des services d'assurance – 11.

Conseils sollicités par le Parlement ou le gouvernement	Trois Avis sur les élections du Président et du Vice-président de la République de Bulgarie et sur les élections des conseils municipaux et des maires en 2011 ; deux Avis sur des demandes d'accès aux données personnelles des NSIS et sur le maintien du registre des dons publics par le ministère de l'Intérieur et la possibilité de publier les données personnelles des donateurs, qui sont des personnes ; trois Avis sur des demandes du Ministère des Affaires étrangères sur la légalité du traitement des données personnelles et leur transfert à des autorités étrangères, et sur la politique de facilitation des procédures de prestation de services administratifs aux citoyens bulgares à l'étranger lorsqu'ils reçoivent des documents d'identification bulgares.
Autres renseignements relatifs aux activités générales	Pour ce qui concerne le transfert de données personnelles, la loi sur la protection des données à caractère personnel prévoit un système d'autorisation et, pour la période de comptes rendus, 21 demandes d'autorisation de transferts de données personnelles vers des pays tiers ont été traitées. Concernant les règles d'entreprise contraignantes (BCR), la CPDP approuve l'autorité responsable et coordonne les documents sur l'approbation des règles d'entreprise en vertu de la procédure de reconnaissance mutuelle et, en 2011, neuf demandes d'approbation ont été déposées.
Activités d'inspection	
Contrôles, enquêtes	En 2011, le nombre total de contrôles effectués a été de 1 252, dont : *ex-ante* – 1 151 ; en cours – 74 et *ex-post* – 27, principalement dans les domaines de la santé – 612 ; du commerce et des services – 153 ; du tourisme – 57 ; des services juridiques et de conseil – 53 ; des transports – 47 ; de l'administration publique – 46 ; des activités sociales – 40 etc.
Activités de sanction	
Sanctions	En 2011, la CPDP a formulé 45 conclusions de violations administratives et imposé 27 amendes.
Amendes	En 2011, la CPDP a imposé des amendes pour un montant de 75 100 BGN.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

1. Concernant les instructions contraignantes formulées et les amendes imposées :

En 2011, des instructions contraignantes ont été formulées dans les secteurs suivants : financier, administration publique, services communaux, transports, médias, commerce et services et télécommunications. Le plus souvent, ces instructions concernaient :

- Les mesures organisationnelles et techniques nécessaires pour garantir que le niveau de protection des données personnelles ne baisse pas – 36 % ;
- Le traitement de données personnelles à des fins autres que les fins déclarées sans notification de ce changement à la CPDP – 21 % ;
- L'interdiction de traiter des catégories de données personnelles spécifiques – 18 % ;
- La non-définition de la période de conservation applicable au stockage de données personnelles – 16 % ;
- La violation des dispositions liées à l'information des personnes – 9 %.

Les violations de la LPPD les plus fréquentes pour lesquelles des déclarations de violations administratives ont été formulées concernaient notamment :

- Des violations des enregistrements des responsables du traitement des données personnelles (à des fins de mise à jour des informations avant la modification des données soumises); – le traitement des données avant la saisie des registres dans le système de la CPDP;
- La violation des dispositions relatives aux mesures de protection des données personnelles (mesures techniques et organisationnelles de protection des données personnelles nécessaires non mises en œuvre par le responsable du traitement, Cf. l'Article 23, paragraphe 4, en relation avec le paragraphe 1 de la LPPD);
- La violation des principes de traitement légal des données personnelles (données à traiter dans le respect de la loi et de bonne foi, proportionnellement et sans excéder la finalité du traitement, Cf. l'Article 2, paragraphe 2, p. 1 et p. 3 de la LPPD).

2. Concernant la publication d'avis, de notifications et de demandes :

En dehors des cas mentionnés dans le tableau, qui étaient soumis à la CPDP par les autorités publiques, les avis suivants présentent un intérêt substantiel :

2.1. Droit d'accès à des enregistrements vidéo d'appareils de vidéosurveillance (dans un hôpital), y compris aux informations relatives à des tiers, et déterminer si les images de vidéosurveillance constituent des données personnelles. La CPDP a publié un avis selon lequel les enregistrements vidéo d'appareils de vidéosurveillance contiennent des données personnelles, parce qu'ils comprennent des informations pouvant divulguer l'identité physique de la personne enregistrée et, à cet égard, toute personne dispose d'un droit d'accès à ses données personnelles (y compris celles enregistrées par les caméras de vidéosurveillance). Les données personnelles de personnes spécifiques enregistrées par des caméras de vidéosurveillance peuvent être fournies s'il est techniquement possible d'effacer temporairement les

données personnelles de tiers susceptibles d'être dévoilées par l'exercice de ce droit d'accès. Si les données de ces tiers ne peuvent techniquement pas être temporairement effacées, le seul motif juridique de l'exercice de ce droit d'accès sera le consentement explicite de toute autre personne ayant fait l'objet de ladite vidéosurveillance.

2.2. La nécessité d'enregistrer les responsables du traitement des données qui ne sont ni établis sur le territoire de la République de Bulgarie, ni sur celui de tout État membre de l'Union européenne :

– demande d'opinion sur la question de savoir si Google/Google Inc. peut enregistrer, sur le territoire de la République de Bulgarie, des objets pour son service Google Street View. La CPDP a émis un avis selon lequel, concernant le traitement de données personnelles aux fins du service Google Street View, le responsable du traitement Google/Google Inc. doit désigner un représentant légal en Bulgarie. Dans cet avis, la CPDP a également formulé des instructions contraignantes devant être prises en compte avant, pendant et après le processus d'enregistrement : pendant l'enregistrement des vues de rues, les caméras ne sont pas autorisées à collecter des données Wi-Fi (données sur les points d'accès sans fil) ; des mesures doivent être prises pour empêcher l'enregistrement de données utiles et autres données directement liées aux personnes (adresses électroniques, mots de passe, etc.) ; le public doit être informé des droits des personnes en matière de traitement de leurs données personnelles aux fins du service Google Street View, et des mesures plus restrictives doivent être prises, telles que la technologie de floutage des images des personnes se trouvant dans des lieux connectés ou pouvant être connectés avec le traitement de catégories spéciales de données etc.

3. Pour ce qui concerne les demandes de transfert de données, les cas suivants sont intéressants :

3.1. Demande d'autorisation de transfert de données biométriques scannées à une société et à une autre entité juridique non commerciale aux États-Unis en relation avec des examens sur ordinateur passés en Bulgarie aux fins de l'admission d'étudiants dans des écoles de commerce à l'international. L'une des principales exigences de scannage des empreintes palmaires des candidats visait à prévenir tout changement et/ou substitution de candidats et à maintenir la confiance dans les écoles de commerce auxquelles l'admission était accordée en cas de réussite aux tests. La CPDP a émis une opinion permettant au responsable du traitement des données / à son représentant local de transférer les images des paumes scannées (données biométriques des candidats) vers les États-Unis. Le motif légal de l'autorisation du transfert de données dans ce cas était l'existence du consentement explicite des candidats aux tests, dont les données biométriques faisaient l'objet du transfert.

3.2. Demande d'autorisation de transfert d'images et d'enregistrements vidéo des visiteurs et employés du responsable du traitement sur le lieu de travail de la société mère aux États-Unis. Lors de la procédure administrative, la CPDP a observé les lacunes suivantes : le traitement ne présentait aucune condition d'admissibilité ; la nécessité du transfert des données des visiteurs n'était pas établie ; les données étaient excessives et leur traitement était incompatible avec les fins spécifiques de la demande en matière de gestion des ressources humaines. La CPDP a refusé d'approuver ce transfert de données.

C. Autres informations importantes

1. Concernant les activités de la CPDP liées à la mise en œuvre de la Directive 2006/24/CE dans la législation bulgare

La Directive 2006/24/CE (directive sur la conservation des données) a été transposée dans la législation bulgare en 2010 avec les amendements et suppléments de la Loi sur les communications électroniques (LCE). À l'entrée en vigueur de ces amendements, toutes les parties au processus de conservation et d'accès aux données relatives au trafic ont été déterminées sur un plan juridique, et la CPDP a été désignée en tant qu'autorité de contrôle de la sécurité des données. Conformément à ses compétences découlant de la LCE, la CPDP a, pour la première fois en 2011, résumé et fourni des informations statistiques conformément aux exigences de la loi, de la Commission européenne et de l'Assemblée nationale dans les délais visés par la LCE.

À cet égard, 4 réunions distinctes de la CPDP avec les parties intéressées, à savoir les autorités compétentes en vertu de la LCE, les entreprises fournissant des réseaux et/ou services de communication électronique, le parquet et les tribunaux, ont été organisées aux mois de septembre-décembre 2011.

La CPDP a proposé que soient discutées et clarifiées des questions telles que l'utilité de l'obtention de données pour la détection et la poursuite de crimes en procédant à des recherches de personnes, ainsi que les informations relatives aux acquittements et inculpations ; la portée de la soumission, à des fins d'analyse et de synthèse d'informations sur des types spécifiques de crimes ou délits courants, pour la plupart desquels un accès aux données relatives au trafic est requis ; la portée de la synthèse d'informations sur les motifs légaux et les fins pour lesquelles l'accès est généralement requis ; le respect de l'obligation de conserver des registres pour les demandes d'accès, les refus, les autorisations des tribunaux et les demandes émises ; la portée des demandes relatives aux périodes de conservation relativement longues (6 mois) conformément à l'Article 250(a), paragraphe 5 de la LPPD ; les cas de refus par les entreprises de soumettre des données ; la période de conservation des données (âge des données) ; la clarification de la période de compte rendu pour les entreprises soumettant des informations statistiques à la CPDP ; la clarification de la portée, pour les entreprises, de la soumission d'informations plus détaillées à la CPDP ; la clarification des procédures d'accès aux données relatives au trafic en vertu du Code de procédure pénale aux fins de procédures préjudicielles et judiciaires.

2. Concernant l'activité de la CPDP en termes de formation des responsables du traitement des données sur la mise en œuvre des dispositions de la loi relative à la protection des données à caractère personnel et autres questions spécifiques

En 2011, la CPDP a adopté un concept et un plan de formation, et organisé une campagne de formation approfondie. Pour la préparation et l'organisation de la campagne de formation, les priorités et objectifs nationaux en vigueur ont été pris en compte, ce qui a donné lieu à une série de séances de formation visant à améliorer le niveau de préparation professionnelle des responsables du contrôle et du traitement des données personnelles ayant accès au Système d'information Schengen (SIS), en vue de l'accession prévue de la République de Bulgarie à l'espace Schengen. Simultanément à l'organisation de la formation au SIS, et suite aux exercices de 2010, des séminaires ont été organisés avec des représentants des autorités autonomes locales et de l'administration de l'Assemblée nationale de la République de Bulgarie. La CPDP a également pris part à des cours de formation de l'Institut Diplomatique et de l'Université de bibliothéconomie et de technologies de l'information.

En 2011, les séances de formation de la CPDP ont été suivies par des responsables du traitement de données du secteur public, d'entreprises privées et de la communauté universitaire. 22 séminaires ont été organisés, dont 12 à destination de fonctionnaires d'institutions ayant accès au NSIS ; 3 séminaires avec

les autorités locales et l'Association Nationale des Municipalités de la République de Bulgarie ; 2 séances de formation du personnel de l'Assemblée nationale ; 1 pour l'Institut Diplomatique ; 1 pour la communauté universitaire ; 2 pour les représentants de sociétés commerciales (NPP Kozloduy et EVN), et 1 pour les représentants de branches professionnelles (l'Union des pharmaciens bulgares). Au total, 106 institutions ont envoyé leurs représentants participer aux séances de formation, dont 47 institutions publiques, 55 tribunaux, 2 sociétés privées et une organisation professionnelle. Le nombre de personnes formées s'élève à 481 responsables du contrôle et du traitement des données personnelles, dont 333 ont pris part à la formation des responsables du contrôle et du traitement ayant accès aux NSIS.

CHYPRE

A. Résumé des activités et actualités

En septembre 2011, M. Yiannos Danielides a été désigné Commissaire à la protection des données à caractère personnel. M. Danielides succédait dans ces fonctions à Mme Panayiota Polychronidou, démissionnaire au mois de juin.

Au titre des efforts déployés par notre bureau à des fins de sensibilisation, dans le cadre des activités organisées pour la Journée européenne de la protection des données à caractère personnel, notre Bureau a utilisé un budget de 4 878 EUR pour distribuer des prospectus, des mètres ruban et des pochettes de protection de CD aux visiteurs de centres commerciaux, le 28 janvier. Le message du jour portait sur les « mesures de protection ».

Un document de travail (avant-projet de loi) pour la transposition de la Décision cadre 2008/977/JAI sur la protection des données personnelles traitées dans le cadre de la coopération avec les autorités policières et judiciaires en matière pénale a été préparé par notre Bureau en coopération avec la police chypriote.

En décembre 2010, un réfugié reconnu a déposé une plainte à l'encontre d'un site web d'information qui avait publié des copies de sa carte d'identité et d'autres documents des services sociaux révélant les noms, les adresses et les prestations sociales que lui et d'autres réfugiés percevaient mensuellement de la part des services sociaux. Suite à l'examen de la plainte, le Commissaire, compte tenu des points de vue exposés par les avocats du site web et des dommages subis par le plaignant, a formulé une décision concluant que la publication en cours des données susmentionnées constituait une violation de la Loi et a imposé deux sanctions administratives au site web, une amende de 3 000 EUR et la destruction des données ainsi que la cessation de leur traitement. Le site web n'ayant pas respecté cette décision, en avril, le Commissaire, conformément aux pouvoirs qui lui sont conférés par la Section 23(a) de la Loi, a porté l'affaire devant le Chef de la Police afin qu'il examine la possibilité d'un délit commis par le site web, conformément à l'Article 26 de la Loi.

Notre Bureau a examiné une plainte à l'encontre de l'Autorité des télécommunications de Chypre (CYTA) de la part d'un employé auquel avait été refusé le droit d'accès à des informations relatives à une procédure disciplinaire initiée à son encontre à la suite d'une accusation et, notamment, au nom de son accusateur. La CYTA a conclu que l'accusation n'était pas fondée, n'a procédé à aucune enquête disciplinaire et a fourni tous les documents appropriés au plaignant, en refusant néanmoins de lui divulguer l'identité de son accusateur, comme l'avait demandé le plaignant en vue d'intenter une action contre lui. Le Commissaire a émis une décision concluant que toutes données incluses dans un courrier d'accusation constituent des données personnelles relatives à la personne concernée et que, dans ce cas, la demande d'accès avait été en partie satisfaite. La CYTA a été appelée à fournir au plaignant une copie du courrier de l'accusateur et à lui divulguer son identité.

En vue de la/des proposition(s) de la Commission à venir pour la réforme de la législation européenne relative à la protection des données, notre Bureau a accepté la demande du ministère de la Justice et de l'Ordre public de représenter la République au DAPIX, le groupe de travail du Conseil qui devait discuter de la/des proposition(s) sous la présidence polonaise. Un certain nombre de fonctionnaires ont suivi une formation spécialisée à l'Académie de l'administration publique conçue pour les aider dans le cadre de leurs nouvelles responsabilités au Conseil et de leurs responsabilités à venir avec la présidence de Chypre, et des discussions avec le ministère et la police ont été initiées afin de formuler une procédure pour l'adoption de positions communes.

Organisation	Bureau du Commissaire à la protection des données à caractère personnel
Président et/ou collège	M. Yiannos Danielides
Budget	Budget attribué 297 033 EUR et budget exécuté 28 472 EUR
Personnel	Agents administratifs : 7 Agents informaticiens : 2 Secrétaires : 6 Agents auxiliaires : 2
Activités générales	
Décisions, avis, recommandations	Nombre d'avis : 11 Nombre de décisions : 7 Nombre de recommandations : 4
Notifications	Nombre de notifications : 162
Examens préalables	Nombre d'examens préalables : s. o.
Demandes émanant des personnes concernées	Nombre de demandes reçues par écrit ou par téléphone de la part des personnes concernées : s. o.
Plaintes émanant des personnes concernées	Nombre de plaintes qualifiées : 469
Conseils sollicités par le Parlement ou le gouvernement	En 8 occasions, notre Bureau a été invité par la Chambre des Représentants de Chypre à des fins de consultation et de participation à des réunions devant les comités parlementaires compétents.
Autres renseignements relatifs aux activités générales	Nombre d'autorisations de regroupement de systèmes de fichiers : 18 Nombre d'autorisations de transmission vers des pays tiers : 48
Activités d'inspection	
Contrôles, enquêtes	Nombre de contrôles et/ou d'enquêtes : 22 En 2009, des contrôles du secteur bancaire ont été menés. En 2010, notre Bureau a émis des lignes directrices pertinentes et initié un contrôle de suivi visant à vérifier le respect de la conformité par les banques, conclu en 2011. Le rapport sur les résultats du suivi a montré que, sur 18 banques commerciales actives à Chypre, 16

	respectaient les lignes directrices. Les 4 autres contrôles réalisés portaient sur l'examen de plaintes relatives à l'installation de systèmes de vidéosurveillance.
Activités de sanction	
Sanctions	Nombre de sanctions décidées par la DPA : 7 Nombre de mesures juridiques prises à l'initiative de la DPA à l'encontre de responsables du traitement de données pour la collecte d'amendes : 2
Amendes	Montants imposés par la DPA : 13 000 EUR
DPD	
Chiffres relatifs aux DPD	s. o.

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, sous la conduite d'un Directeur. Les affaires particulièrement intéressantes (une quinzaine par an) sont soumises à la décision du Conseil. Le Conseil est présidé par un juge de la Cour suprême.
Budget	20,3 millions de DKK
Personnel	Environ 35
Activités générales	
Avis, recommandations	s. o. (inclus dans les chiffres ci-dessous)
Notifications	2 602
Examens préalables	2 602
Demandes émanant des personnes concernées	1 965 (ce nombre couvre l'ensemble des demandes et plaintes déposées devant la DPA danoise)
Plaintes émanant des personnes concernées	Voir ci-dessus
Conseils sollicités par le Parlement ou le gouvernement	339
Autres renseignements relatifs aux activités générales	51 affaires liées à la sécurité
Activités d'inspection	
Enquêtes	54
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 imposées dans 2 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

Utilisation d'empreintes digitales pour enregistrer la participation à un cours obligatoire afin de recevoir des prestations sociales

Un syndicat danois souhaitait porter plainte au nom de l'un de ses membres. La municipalité locale avait commencé à déployer une pratique en vertu de laquelle les personnes sans emploi participant à un cours devaient enregistrer leurs empreintes digitales afin de prouver leur participation.

La municipalité a expliqué que ce traitement des informations avait pour objet d'enregistrer la présence aux cours des personnes sans emploi de la municipalité afin que celles-ci puissent prétendre au versement de prestations sociales.

La municipalité a en outre expliqué que seule une version numérique de l'empreinte digitale (modélisée) était collectée et traitée par le système.

La municipalité a enfin expliqué qu'il lui était nécessaire d'utiliser les empreintes digitales afin d'administrer efficacement la participation des personnes aux cours et d'éviter les abus, et qu'elle estimait l'emploi d'informations biométriques conforme à la loi danoise sur le traitement des informations personnelles.

La DPA danoise a estimé que ce traitement était nécessaire pour l'exécution d'une tâche dans l'exercice de l'autorité publique en raison des obligations de la Municipalité et la DPA ne s'est pas opposée à l'emploi, par la municipalité, d'empreintes digitales pour enregistrer les participants sans le consentement des personnes concernées conformément à l'Article 6, alinéa 6, de la Loi danoise sur le traitement des données à caractère personnel.

Accompagnement des enfants et jeunes endeuillés

En 2011, la DPA danoise a autorisé un centre d'accompagnement à porter assistance à des enfants et jeunes endeuillés.

Ce centre d'accompagnement avait pour principal objectif de réconforter et conseiller des enfants et jeunes personnes ayant fait l'expérience de décès ou de maladies graves dans leur entourage immédiat.

Le centre d'accompagnement souhaitait traiter les informations personnelles des enfants et des jeunes, mais également de leurs proches. Les informations relatives aux enfants bénéficiant de l'accompagnement devaient être traitées sur la base légale de leur consentement. Concernant les membres de leur famille, morts ou vivants, il n'était ni possible ni réalisable de demander leur consentement.

La DPA danoise a décidé que le traitement des informations personnelles relatives aux membres de la famille devait être autorisé et a appliqué pour la première fois l'Article 7, alinéa 7, de la Loi danoise sur le traitement des données à caractère personnel, qui s'appuie sur l'Article 8, paragraphe 4 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des

personnes en ce qui concerne le traitement des données personnelles et la libre circulation de ces données.

La DPA danoise a estimé que, dans ce cas, la finalité respectait l'exigence d'intérêt public visée à l'Article 8, paragraphe 4 de la Directive.

C. Autres informations importantes

Journée internationale de la protection des données

La DPA danoise a consacré la journée internationale de la protection des données à essayer d'éduquer et d'informer le public d'un centre commercial sur la protection des données. Le personnel a répondu à des questions, distribué des prospectus contenant des informations pertinentes aux visiteurs du centre et facilité l'organisation d'un quiz en ligne sur la protection des données. Cette journée a connu un franc succès auprès du personnel comme des visiteurs, qui ont affiché de bonnes connaissances et un grand intérêt pour la protection des données.

BCR danoises

En 2011, la DPA danoise a complété les premières BCR (règles d'entreprise contraignantes) lorsque la société danoise Novo Nordisk A/S a reçu les siennes. Le travail sur les BCR de Novo a commencé en 2007, et la DPA danoise a par la suite été contactée par d'autres sociétés danoises qui souhaitaient également disposer de BCR.

ESPAGNE

A. Résumé des activités et actualités

Information des citoyens et protection de leurs droits

L'activité de l'AEPD directement liée à l'information et à la protection des citoyens a fortement augmenté en 2011. Le nombre de demandes d'informations reçues sur le service d'assistance téléphonique aux citoyens a augmenté de 30 % (avec près de 135 000 demandes) et le site web a enregistré trois millions de visites au total. Parallèlement, le nombre de réclamations[15] a augmenté de 35 % en 2011, avec un total de 2 230 demandes. Plus de 60 % des décisions prises par l'AEPD en réponse à ces demandes traitaient des droits d'effacement ou d'objection. Cette tendance est également suivie par des réclamations sur le « droit à l'oubli », avec des chiffres en pleine évolution depuis les trois réclamations enregistrées en 2007, contre 160 en 2011. En outre, le nombre de plaintes[16] était supérieur de 50 % à ce qu'il était en 2010, avec près de 5 500 plaintes.

La protection des enfants est l'une des priorités de l'AEPD. En 2011, l'ensemble des DPA existant en Espagne (l'AEPD et les agences de Catalogne, de Madrid et du Pays Basque) ont mis à disposition un outil de formation appelé « S'inscrire, entrer, se désinscrire. Protégez vos droits et contrôlez vos données ». Cet outil est une adaptation à l'environnement espagnol des documents originaux conçus par le Commissaire à la protection des données personnelles irlandais. Ces ressources éducatives seront suivies d'un outil plus complet qui sera lancé en 2013.

Facilitation de la mise en œuvre de la loi

Les responsables du traitement des données peuvent demander des clarifications des dispositions de la Loi sur la protection des données dans les cas les plus complexes. L'AEPD a émis près de 500 rapports juridiques en 2011. L'AEPD a également émis plus de 100 rapports sur des projets de législations et mesures réglementaires. Les rapports sont obligatoires pour le Gouvernement et bien que non contraignants légalement, sont influents pour le processus législatif.

En avril 2011, l'AEPD a lancé un nouveau système d'information (RENO) développé pour améliorer l'efficacité des opérations associées aux notifications, à l'enregistrement des fichiers et à l'autorisation des transferts internationaux. L'application comprend des systèmes de signature électronique individuelle et de sceau électronique afin de faciliter l'émission et la notification de résolutions, notamment.

Évolutions juridiques

Au mois de mars, la Loi sur la protection des données espagnole (LOPD) a été amendée par la Loi 2/2011 sur l'économie durable. Les amendements ont affecté le système de sanctions de diverses manières. D'une part, la classification des infractions a été modifiée. Les catégories (sans gravité, grave et très grave) restent les mêmes, mais les activités incluses dans chaque catégorie ont été ajustées. Les montants minimum et maximum des amendes possibles pour chaque type d'infraction ont également été

[15] Demandes de décision de l'Agence afin d'assurer le droit de protection des données de l'auteur de la réclamation en cas de non-respect de la part d'un responsable du traitement des données spécifique

[16] Demandes de décision de l'Agence déclarant l'existence d'une infraction à la loi, ordonnant la fin de cette infraction et imposant une sanction.

légèrement modifiés. Il est particulièrement intéressant de noter que les dispositions amendées fixent des critères objectifs pour la modulation des sanctions, prévoient la possibilité d'une réduction des sanctions en cas de mise en place de mesures préventives / proactives et introduisent un « avertissement préventif » susceptible de remplacer les amendes dans des cas spécifiques (première infraction si elle n'est pas « très grave » et respecte d'autres conditions).

Coopération internationale

En juin 2009, l'AEPD a été choisie comme chef de file d'un projet de jumelage devant être réalisé en Croatie. Ce projet établit un cadre de coopération entre les DPA espagnole et croate en vue de la préparation de l'accession de la Croatie à l'UE. En 2011, l'AEPD et l'Agence croate ont conjointement réalisé les activités couvertes par le Projet, qui devait avoir été complété en 2012.

Organisation	Agence espagnole de protection des données
Président et/ou collège	M. José Luis Rodríguez
Budget	14 437 970,00 EUR
Personnel	156 (154 fonctionnaires – 2 employés publics) et 1 Commissaire
Activités générales	
Décisions, avis, recommandations	Nombre de décisions relatives à des réclamations de citoyens : 7 233 ; rapports juridiques : 140
Notifications	638 533 notifications relatives aux dossiers publics et privés Nombre total de dossiers notifiés fin 2011 : 2 609 471
Examens préalables	s. o.
Demandes émanant des personnes concernées	134 635 demandes reçues par la ligne d'assistance (par écrit, par téléphone, par Internet ou au guichet) 484 demandes de rapports adressées au Service juridique (246 de la part d'administrations publiques et 238 émanant de personnes physiques ou d'entités privées)
Plaintes émanant des personnes concernées	5 389 plaintes déposées par des personnes concernées. Les secteurs tels que ceux des télécommunications et de la vidéosurveillance ont présenté de substantielles augmentations (17,78 % et 6,35 % respectivement), ainsi que d'autres domaines tels qu'Internet et la publicité commerciale...
Conseils sollicités par le Parlement ou le gouvernement	L'AEPD a émis des avis juridiques sur un total de 110 projets de textes juridiques généraux ou amendements de textes juridiques existants, dont la Loi sur la transparence, la Loi sur la supervision de l'assurance privée, la Loi générale sur les télécommunications et la

	Loi antidopage.
Autres renseignements relatifs aux activités générales	2 892 516 actes d'accès par Internet (7 923 par jour en moyenne) 3 500 883 consultations du Registre public en ligne 175 autorisations de transferts internationaux ont été approuvées par le Directeur
Activités d'inspection	
Contrôles, enquêtes	5 389 enquêtes préalables et 2 230 procédures de protection des droits. 7 233 résolutions de procédures de contrôle, dont 1 939 liées à des réclamations concernant la protection des droits (d'accès, de rectification, de suppression et d'opposition) et 5 294 procédures relatives au pouvoir de sanction. Le service de contrôle a également mené des enquêtes d'office dans différents domaines : - l'informatique en nuage - le transfert de données commerciales – le contrôle de la cession de titres de créance par des opérateurs de télécommunications et des institutions financières (en cours). - les mandats d'arrêt européens en Espagne - l'analyse des clauses contractuelles des opérateurs de télécommunications
Activités de sanction	
Sanctions	Sur 898 résolutions de sanction, 96,46 % avaient trait à la Loi sur la protection des données ; 3,02 % s'appuyaient sur la Loi sur les services de la société de l'information (spam) et seulement 0,52 % sur la Loi générale sur les télécommunications (publicités par fax)
Amendes	19 597 905,97 EUR (+12 % par rapport à 2010)
DPD	s. o.
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

La notion « d'avertissement préventif » introduite par l'amendement de la Loi sur la protection des données a beaucoup servi en 2011. Près de 40 % de l'ensemble des décisions déclarant l'existence d'une infraction ont été closes par un avertissement plutôt qu'une amende. Les cas dans lesquels un « avertissement préventif » a été appliqué comprennent généralement des erreurs non intentionnelles, des

infractions de la part de personnes physiques dues à une connaissance insuffisante de la Loi sur la protection des données et des infractions impliquant des violations d'exigences formelles ou administratives. Des éléments tels que le degré de coopération du responsable du traitement des données pour mettre un terme à la violation, la sensibilité des données affectées, l'impact économique de l'infraction ou la relation des opérations de traitement des données avec l'activité principale du responsable sont régulièrement pris en compte pour décider s'il convient d'émettre un avertissement ou d'imposer une amende.

Jurisprudence, tribunal national:

En 2011, plusieurs jugements décidant de l'équilibre entre le droit à la protection des données et d'autres droits et libertés fondamentaux ont été particulièrement intéressants.

- Concernant le droit à l'information, un jugement du tribunal national en date du 29 septembre a déclaré conforme à la LOPD la publication dans les médias de photographies d'une victime des attaques terroristes de mars 2004 à Madrid, considérant que ces images étaient pertinentes par rapport aux informations que souhaitaient relayer les médias.

- Le droit à la liberté d'association et syndicale a été considéré comme prévalant sur le droit à la protection des données lorsque des informations utiles aux travailleurs sont rendues publiques et que cette publication est limitée au lieu de travail.

Jurisprudence, Cour suprême

Le 24 novembre, un jugement de la Cour de justice de l'UE a déclaré que l'Article 7(f) de la Directive 45/96 ne pouvait être interprété de la même manière que la LOPD (*Ley Orgánica* 15/1999, *de Protección de Datos*). Ce jugement résout une question posée par la Cour suprême espagnole dans le contexte d'un appel en vertu duquel des entreprises mettaient en cause plusieurs articles du règlement administratif mettant en œuvre l'Article de la LOPD qui transpose l'Article 7(f) de la Directive. Bien que le cas concerne le règlement administratif, la Cour suprême a également demandé à la Cour européenne si l'Article de la Loi sur laquelle s'appuie le règlement était compatible avec la Directive européenne. Le jugement de la Cour européenne considère que l'Article 7(f) a un effet direct et rend par conséquent l'Article correspondant de la Loi sur la protection des données espagnole inapplicable. La Cour suprême espagnole a par ailleurs déclaré nulles et non avenues plusieurs dispositions du règlement contesté.

ESTONIE

A. Résumé des activités et actualités

Organisation	
Président et/ou collège	Inspection estonienne de la protection des données
Budget	592 446 EUR
Personnel	18 (les services de soutien, tels que l'informatique et la comptabilité, sont sous-traités)
Activités générales	
Décisions, avis, recommandations	Décisions : 354 décisions en matière de surveillance (dont 114 refus d'initier et 38 préceptes) ; 58 décisions relatives à des délits mineurs ; 9 décisions en appel et 18 décisions d'autorisation (7 autorisations de recherches scientifiques et 11 autorisations de transfert de données). Avis (instructions) : **3** (Protection des données au travail ; Instructions pour les employés en ressources humaines : les Données personnelles dans les relations professionnelles et Informations sur les enfants ayant besoin d'aide et sur la protection des données). Recommandations : **130** pour une meilleure organisation de la protection des données
Notifications	327 (traitement de données sensibles)
Examens préalables	0
Demandes émanant des personnes concernées	**687** par courrier électronique/courrier (195 concernaient le secteur public ; 257 le secteur privé ; 110 le secteur des organisations à but non lucratif ; 37 les médias ; 53 les réseaux sociaux ; 35 le spam et **615** les appels à des lignes d'assistance)
Plaintes émanant des personnes concernées	**413**
Conseils sollicités par le Parlement ou le gouvernement	**2** (sur la Loi relative au registre de la population et la Loi sur les communications électroniques)
Autres renseignements relatifs aux activités générales	**41** avis sur des projets de lois, sur demande du gouvernement

Activités d'inspection	
Contrôles, enquêtes	Contrôles : 77 sur place Enquêtes : 7 (audits de conformité et d'adéquation) Contrôles comparatifs : 3 (parmi les employeurs ; mesures de sécurité au sein des municipalités ; marketing direct)
Activités de sanction	
Sanctions	38 paiements coercitifs et amendes pour des infractions
Amendes	382 488 (par la DPA)
DPD	
Chiffres relatifs aux DPD	126 nouvelles notifications de DPD + 9 changements de DPD

B. Informations sur la jurisprudence

Coopération Estonie-Lettonie – supervision conjointe de Stockmann

Les DPA estonienne et lettone ont conjointement contrôlé les grandes surfaces Stockmann en Estonie et en Lettonie en matière de protection des données dans le cadre des relations professionnelles et avec les clients, y compris en matière de marketing direct.

Les contrôleurs ont suggéré que les filiales du Groupe Stockmann notifient plus clairement leurs clients en matière de collecte de données, de leurs conditions de marketing direct et de clôture et suppression des données des clients sur demande. Les DPA ont par ailleurs suggéré que Stockmann distingue les champs de données obligatoires devant être communiquées afin de participer au programme de fidélité de Stockmann. Les autorités ont demandé à Stockmann d'ajouter une section contenant des informations sur les possibilités de supprimer les données personnelles de la base de données.

Les contrôleurs ont en outre souligné que si le client donnait son accord pour recevoir des informations commerciales, Stockmann n'était autorisé à demander que les coordonnées (postales, courrier électronique, téléphone mobile etc.) destinées à l'envoi de messages. Une autre question nécessitant d'être résolue portait sur le profilage des clients, qui doivent en être informés afin de prendre une décision quant à leur adhésion au programme de fidélité de Stockmann.

C. Autres informations importantes

Nous avons mené un **audit interne exhaustif des procédures administratives et analysé les jugements des tribunaux et la documentation juridique.** L'objectif consistait à harmoniser les pratiques juridiques de l'Inspection, à garantir leur compréhensibilité et leur légitimité, et à réduire les erreurs procédurales. Nous avons conçu notre manuel détaillé de procédures administratives.

L'autre grand sujet analysé concernait la **relation entre vie privée et liberté d'expression**. Peu d'affaires de ce genre sont portées devant les tribunaux, et elles concernent essentiellement le problème de la

diffamation. Restreindre la liberté d'expression doit être une décision mûrement réfléchie. Nous avons réalisé une analyse approfondie des jugements rendus par la Cour européenne des droits de l'homme, de la documentation existante (réduite à sa portion congrue en Estonie) et des jugements rendus par la Cour suprême. Nous pouvons aujourd'hui nous appuyer sur les résultats de ces analyses pour résoudre les plaintes et justifier nos décisions. Nous avons également organisé un séminaire conjoint avec l'Association des journaux estoniens, qui s'est tenu en avril de cette année.

Les échanges d'information avec l'Office de police et des gardes-frontières et le ministère de l'Intérieur pour la surveillance des utilisations frauduleuses des bases de données de la police et du Registre de la population, respectivement, reposent sur des bases solides. Les cas d'utilisation abusive du Registre de la population augmentant, nous avons discuté du problème dans les médias et déployé une politique répressive plus stricte.

Nous avons également initié l'échange régulier d'informations avec la Fondation estonienne de cybersanté afin de surveiller les cas d'utilisation abusive de données des patients.

FINLANDE

A. Résumé des activités et actualités

Le travail était principalement axé sur des opérations préventives. Nous avons cherché à en accroître l'impact grâce au ciblage précis des lignes directrices générales et à l'intégration fonctionnelle avec différents groupes, comités et autres organisations similaires. Un représentant du Bureau du Médiateur chargé de la protection des données a participé au travail d'environ 80 comités consultatifs, groupes de travail et autres organismes coopératifs au total. Le Médiateur chargé de la protection des données a été membre ou membre expert du groupe pour la sécurité des informations de la Société de l'information dans le cadre du programme Everyday Life, qui a pris fin le 28 février 2011, ainsi qu'au Conseil de gestion de la sécurité de l'information dans l'administration VAHTI. Il fait également partie d'un groupe de surveillance de la codification de la société de l'information, établi par le ministère des Transports et des Communications le 9 décembre 2011. Le mandat du groupe de surveillance se poursuit jusqu'au 31 octobre 2014. Le 14 octobre 2011, le ministère de la Justice a invité le Médiateur chargé de la protection des données à participer au travail d'une commission dans le cadre de la préparation d'un programme d'action national en faveur des droits de l'homme. La durée du mandat de cette commission allait du 14 octobre 2011 au 31 janvier 2012.

Les représentants du Bureau ont participé à plusieurs groupes de travail du Conseil de gestion de la sécurité de l'information dans l'administration VAHTI ainsi qu'à la trentaine de groupes de travail et de pilotage établis par différents secteurs administratifs. La coopération s'est en outre poursuivie afin d'établir des codes de conduite ou autres lignes directrices spécifiques à certains secteurs, notamment.

À la fin de la 24e année d'opérations pour le Bureau du Médiateur chargé de la protection des données, une vague sans précédent de violations de la protection des données a déferlé sur la Finlande. Des informations et révélations sur des fuites d'informations personnelles étaient alors publiées pratiquement chaque semaine. Pourtant, d'après les informations réunies par l'unité CERT de notre partenaire, l'autorité finlandaise de régulation des communications, les cas évoqués publiquement ne représentaient qu'une petite partie de toutes les fuites de données observées sur cette même période. Le fait que la réglementation finlandaise n'inclue pas de véritable obligation de rendre compte de ces fuites aux personnes dont les informations ont fait l'objet d'une fuite a été considéré comme un problème d'intérêt particulier. La confiance que les citoyens placent dans les services de la société de l'information a été sérieusement remise en question.

La semaine pour un Internet plus sûr portait sur les réseaux sociaux et la vie privée sur Internet

Le Bureau du Médiateur chargé de la protection des données a participé une nouvelle fois aux activités de la journée et de la semaine pour un Internet plus sûr le 8 février 2011. Organisée pour la huitième fois, la journée pour un Internet plus sûr fait partie de la stratégie nationale de sécurité de l'information. Cette année, la campagne était axée sur le respect de la vie privée sur Internet. La sécurité des informations sur les réseaux sociaux a également été abordée d'un point de vue plus général.

Du fait des médias sociaux, l'utilisateur ordinaire est plus étroitement concerné par les problèmes de sécurité des informations en ligne. L'utilisation sûre des communautés en ligne requiert prudence et attention, et la protection de la vie privée gagne en importance. Avant la journée pour un Internet plus sûr, le site web du Guide de sécurité des informations a été mis à jour avec de nouvelles informations sur les liens frauduleux, la protection de la vie privée et l'utilisation sûre des médias sociaux.

Les écoliers et les adolescents sont souvent des utilisateurs plus expérimentés des communautés en ligne que les adultes, mais ont néanmoins besoin d'au moins autant de conseils en matière de navigation sûre et de protection de leur vie privée. Divers exercices sur le sujet ont été publiés pour les écoles, et un concours organisé sur le site de l'école de la sécurité en ligne (www.tietoturvakoulu.fi).

La journée pour un Internet plus sûr a également gagné en visibilité sur Internet. Le forum de discussion Suomi24 a créé une rubrique spécialisée sur la journée pour un Internet plus sûr durant tout le mois de février. Dans cette rubrique, des spécialistes participant à la campagne de la journée pour un Internet plus sûr ont répondu aux questions des utilisateurs sur la sécurité de l'information.

Le tableau suivant synthétise les principaux chiffres du Bureau 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 s'élève à environ 1 585 000 EUR
Personnel	L'effectif total comprend 20 personnes
Activités générales	
Décisions, avis, recommandations	2 630
Notifications	377
Examens préalables	Voir notifications
Demandes émanant des personnes concernées	950
Plaintes émanant des personnes concernées	(Accès et rectifications) 189
Conseils sollicités par le Parlement ou le gouvernement	93
Autres renseignements relatifs aux activités générales	Collaboration avec les responsables du traitement des données dans les secteurs suivants : éducation, soins de santé, affaires sociales, télécommunications, emploi et économie

Activités d'inspection	
Contrôles, enquêtes	654
Activités de sanction	75
Sanctions	s. o.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	> 1 000

B. Informations sur la jurisprudence

– Un demandeur, dans le cadre de l'exercice de son droit d'accès, a demandé au responsable du traitement des données de lui fournir les enregistrements de ses appels à l'entreprise en tant que client.

Le droit d'accès du demandeur, tel que défini à l'Article 26 de la loi sur les données à caractère personnel, s'applique aux enregistrements des appels de clients existants, sauf en cas de restriction de ce droit d'accès en vertu de l'Article 27 de la loi sur les données à caractère personnel. Dans son explication, le responsable du traitement ne s'appuie pas sur ces bases pour restreindre le droit d'accès du demandeur aux enregistrements en question. Aussi le responsable du traitement est-il tenu de fournir les informations en question au demandeur, tel que spécifié à l'Article 28.2 de la Loi sur les données à caractère personnel. Le responsable du traitement a été obligé soit de donner au demandeur l'opportunité d'écouter les enregistrements de ses appels, soit de fournir au demandeur un compte rendu écrit du contenu de ces enregistrements.

– Une personne a demandé au Médiateur chargé de la protection des données de prendre des mesures suite à un message qu'il avait adressé aux services de BTP municipaux ayant également été envoyé aux services d'aménagement urbain et, par conséquent, rendu public. Le message portait sur l'entretien des rues et le stationnement dans les rues de la ville.

Le niveau de publicité d'un document remis à un fonctionnaire est défini sur la base de la Loi sur l'ouverture des activités publiques (621/1999). Chaque fonctionnaire prend des décisions indépendantes sur la confidentialité de documents et autres aspects en vertu de la Loi sur l'ouverture des activités publiques. Le Médiateur chargé de la protection des données n'a pas d'obligation générale de guider ou de contrôler la conformité à la Loi sur l'ouverture des activités publiques, ni le droit d'interférer avec les décisions basées sur celle-ci prises par d'autres fonctionnaires.

– L'Institut national de la santé et de la sécurité sociale avait réservé au Médiateur chargé de la protection des données une opportunité d'être entendu de la manière visée à l'Article 4, alinéa 1 de la Loi sur les registres nationaux de patients (556/1989, révisée en 38/1993). Une déclaration a été exigée sur la demande d'un groupe de chercheurs souhaitant des informations pour leur étude sur les registres HILMO (Care Registers for Social Welfare and Health Care), gérés par l'Institut national de la santé et de la sécurité sociale.

Les explications complémentaires reçues montrant qu'il n'était pas dans l'intention de connecter les informations ou les échantillons recueillis auprès des sujets de recherche avec leur permission au registre de données faisant l'objet de la demande, il semblait n'y avoir aucun obstacle au transfert des informations après confirmation du caractère adéquat de certaines imprécisions mentionnées dans la demande, et d'autres données de recherche ont été obtenues en toute légalité.

– *Le Médiateur chargé de la protection des données a reçu une question sur la légalité de caméras de surveillance utilisées à l'extérieur et à l'intérieur, dans les espaces communs d'un foyer d'accueil professionnel. Ce foyer d'accueil professionnel était également le foyer de personnes qui y travaillaient 24 heures par jour. Aucun signe n'indiquait la présence des caméras de surveillance. Il existait une description du fichier, qui n'était cependant pas disponible au foyer. Le consentement pour la surveillance à l'intérieur du foyer n'avait pas non plus été demandé.*

La principale question est de savoir si la vidéosurveillance dans les espaces communs du foyer d'accueil était en général autorisée sur la base des stipulations légales sur les droits fondamentaux, le droit pénal, la Loi sur la protection de l'enfance ou toute autre législation particulière. Les activités des foyers d'accueil sont organisées en conformité avec la Loi sur la protection de l'enfance, ce qui signifie que le ministère des Affaires sociales et de la Santé est habilité à déterminer les situations dans lesquelles la présence de caméras de surveillance peut être justifiée. D'après le Médiateur chargé de la protection des données, la question de savoir si, en vertu de la Loi sur les données à caractère personnel (523/1999) ou de La loi sur la protection de la vie privée au travail, il est permissible de traiter les données personnelles des habitants et du personnel par le biais de caméras de surveillance ne revêtait qu'une importance secondaire.

C. Autres informations importantes

Exécution de la première EIP (évaluation de l'impact sur la vie privée)

Une grande enseigne de vente au détail finlandaise conservant une base de données de ses clients réguliers a modifié son système de cartes de fidélité. En même temps, elle a adopté la technologie RFID pour ses cartes. Suite à ce changement, l'entreprise a réalisé une EIP dont elle a remis les résultats au Médiateur chargé de la protection des données aux fins d'évaluation.

En Finlande, il existe également un groupe de travail chargé d'évaluer le besoin potentiel d'une législation sur la technologie NFC (*Near Field Communication*). Le groupe de travail a décidé que la couverture de la législation générale sur la protection des données était également applicable à la technologie NFC.

Mesures d'amélioration de la gestion nationale de l'information

Le Gouvernement finlandais a émis une décision de principe sur la disponibilité des documents publics contenant des données, avec pour objectif d'améliorer les occasions d'utiliser de façon plus extensive nos bases de données nationales (données ouvertes), tout en maintenant le respect de la protection des données personnelles. La présentation a également été soutenue par la nouvelle Loi sur l'administration des données, qui vise l'adoption d'une architecture nationale des informations composée d'éléments compatibles.

La mise en œuvre d'un décret sur la protection des données basé sur la Loi sur l'ouverture des activités publiques, qui réglemente l'administration appropriée des données pour les documents contenant des informations officielles et les fichiers contenant des données personnelles, a également eu lieu pendant

l'année considérée. L'objectif est de s'assurer que toutes les unités administratives atteignent un certain niveau de sécurité de l'information correspondant à leurs opérations.

Protection des données dans différents domaines

Le Bureau du Médiateur chargé de la protection des données a organisé et supervisé la collaboration des parties concernées, notamment dans les domaines de l'éducation, de la communication de données, de la santé et de la sécurité sociale, du marketing et de la recherche scientifique. Ces groupes de travail ont discuté des problèmes liés aux thèmes tels que les services de bien-être pour la jeunesse, les systèmes d'information utilisés à des fins éducatives, la certification mobile et l'utilisation de registres de données finlandais basiques dans le cadre de recherches.

Des études spécifiques à certains domaines ont été réalisées afin d'examiner le niveau de protection des données dans différents secteurs. Ces études ont également représenté l'opportunité de diffuser des informations et des conseils sur ce sujet aux responsables du traitement.

FRANCE

A. Résumé des activités et actualités

Révision de la Directive 95/46: réussir l'Europe de la protection des données

Priorité stratégique pour la commission européenne, ce sujet l'est également pour la CNIL, qui est allée à la rencontre des services de la Commission européenne en charge de la rédaction du nouvel instrument. Prenant appui sur son expérience de plus de 30 ans, la CNIL défend un système de protection des données tout à la fois participatif et décentralisé qui lui paraît plus adapté au monde numérique et à la diversité des situations rencontrées sur le terrain, imbriquant plusieurs pans du droit, qu'il s'agisse de droit du travail, droit pénal, fiscal, des affaires… que seules les autorités nationales sont à même de connaître. La gouvernance européenne de la protection des données, pour être efficace et démocratique, doit reposer sur une coopération approfondie entre autorités souveraines compétentes.

La CNIL a estimé utile de rencontrer plusieurs eurodéputés en mai 2011 dans le cadre du projet de rapport parlementaire sur la communication de la Commission européenne. Enfin, la Présidente de la CNIL s'est entretenue avec Mme Reding à Paris le 26 novembre 2011. Cette rencontre a été l'occasion pour la CNIL de réitérer ses positions vis-à-vis des orientations retenues sur le projet de règlement.

Le suivi des évolutions technologiques

Le cloud

En octobre 2011, la CNIL a lancé une consultation autour du « *Cloud computing* » auprès des professionnels, afin d'envisager toutes les solutions juridiques et techniques permettant de garantir un haut niveau de protection des données, tout en tenant compte des enjeux économiques liés. Les questions étaient orientées autour de cinq thèmes: définition du «*Cloud*», qualification du prestataire de «*Cloud*», détermination de la loi applicable, encadrement des transferts et sécurité du «*Cloud*». A l'issue de cette consultation, l'ensemble des contributions obtenues à l'occasion de cette consultation sont publiées sur le site de la CNIL (www.cnil.fr) et ont pu être exploitées dans le cadre des travaux du G29 sur ce sujet.

Les labels

Les deux premiers référentiels publics d'évaluation permettant à la CNIL de labelliser des procédures d'audit de traitements de données et des formations « Informatique et libertés » ont été publiés le 3 novembre 2011.

Tout organisme dont la procédure d'audit de traitements ou la formation correspond au contenu défini par les référentiels adoptés par la CNIL peut dès aujourd'hui déposer une demande de label. Il lui suffit pour cela de compléter le formulaire prévu à cet effet et de communiquer tous les éléments d'information demandés.

Le label constitue ainsi une double garantie de qualité et de conformité aux exigences fixées par la loi et par la CNIL. La démarche est présentée sur une page du site de la CNIL (www.cnil.fr) dédiée aux «*Labels CNIL*». Une page spécifique à chaque label complète la description du dispositif.

Google

Enfin, la CNIL a sanctionné la société Google pour collecte massive de données techniques Wi-Fi à l'insu des personnes concernées et la captation de données dites « *de contenu* » (identifiants, mots de passe, données de connexion, échanges de courriels). La CNIL a donc mis en demeure la société GOOGLE, en mai 2010, de régulariser sa situation. Estimant qu'il n'avait pas été répondu à ses demandes dans les délais impartis, la formation contentieuse de la CNIL a prononcé à l'encontre de la société, le 17 mars 2011, une amende de 100 000 EUR.

Actions de contrôle et de sensibilisation

Le contrôle de tous les systèmes de vidéosurveillance

La loi d'orientation et de programmation pour la sécurité intérieure (LOPPSI) du 14 mars 2011 a conféré à la CNIL le pouvoir de contrôler l'ensemble des systèmes de vidéosurveillance installés sur la voie publique ou dans des lieux ouverts au public. Auparavant, la CNIL n'était compétente que pour contrôler les systèmes installés dans les lieux qui ne sont pas librement accessibles. Cette évolution longuement attendue permet désormais la mise en œuvre d'un contrôle cohérent et indépendant sur l'ensemble des systèmes de vidéosurveillance installés en France.

Des guides pratiques

Par ailleurs, la CNIL a poursuivi son travail de sensibilisation en 2011, en publiant notamment deux guides pratiques (pour les avocats et pour les professionnels de santé), ainsi qu'une recommandation sur la communication politique.

Organisation	
Président et/ou collège	Président : Isabelle FALQUE-PIERROTIN Vice-présidents : Emmanuel de GIVRY, Jean-Paul AMOUDRY 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).
Budget	Montant total des crédits pour 2011 (en millions d'EUR) : 15,8
Personnel	Effectif : 159
Activités générales	
Décisions, avis, recommandations	1 969 décisions (+ 25,5 % par rapport à 2010) / 93 avis / 1 recommandation

Notifications	82 243 notifications à la CNIL, dont : 5 993 notifications pour des systèmes de vidéosurveillance (+ 37 % par rapport à 2010) 4 483 notifications pour des systèmes de géolocalisation (+ 33,5% par rapport à 2010)
Examens préalables	Autorisations : 1 759 en 2011, dont : 249 autorisations adoptées en séance plénière, 887 autorisations de transfert de données vers des États non membres de l'UE, 6 autorisations cadres, 744 autorisations de systèmes biométriques (+ 5,4 % par rapport à 2010), 503 autorisations de traitement de données personnelles à des fins de recherche médicale, et 120 autorisations de traitement de données personnelles aux fins de l'évaluation ou de l'analyse de pratiques ou d'activités de soins et de prévention.
Demandes émanant des personnes concernées	Demandes émanant du public : En 2011, la CNIL a reçu 32 743 demandes écrites (+ 10 % par rapport à 2010) et 138 979 appels téléphoniques (+ 4,6 % par rapport à 2010).
Plaintes émanant des personnes concernées	La CNIL a reçu 5 738 plaintes en 2011 (+ 19 % par rapport à 2010). Il s'agit du nombre de plaintes le plus élevé qu'ait reçu la CNIL à ce jour. Ces plaintes portaient essentiellement sur le droit à l'oubli et les systèmes de vidéosurveillance. Demandes émanant des personnes concernées : 2 099 demandes d'accès indirect dans le cas où le traitement des données concerne la sécurité de l'État, la défense nationale ou la sécurité publique (+ 12 % par rapport à 2010).
Conseils sollicités par le Parlement ou le gouvernement	En 2011, la CNIL a adopté 92 avis sur des projets nationaux de réglementation (soit 20 % des 425 avis au total adoptés en séance plénière). La CNIL a par ailleurs été auditionnée à 23 reprises par des Membres du Parlement français, et a participé à 10 réunions avec des membres du Parlement français pour un échange de vues sur des questions de protection des données.
Autres renseignements relatifs aux activités générales	-
Activités d'inspection	
Contrôles, enquêtes	385 enquêtes (+ 25 % par rapport à 2010), dont 151 enquêtes relatives à des systèmes de vidéosurveillance.
Activités de sanction	
Sanctions	18 sanctions imposées par la CNIL en 2011. Actions en justice à l'encontre des responsables de données : 83 (65 mises en demeure, 5 amendes, 13 avertissements), 2

	décharges.
Amendes	Amendes imposées par la CNIL en 2011 pour un montant total de 190 000 EUR.
DPD	
Chiffres relatifs aux DPD	8 635 organisations ont désigné un DPD (+ 25 % par rapport à 2010).

B. Informations sur la jurisprudence

Vous trouverez ci-dessous une liste des principales décisions rendues par les juridictions françaises touchant à la protection des données à caractère personnel.

- CA Caen, 3e chambre, section sociale 1, CHSCT de la société Benoît GIRARD c/ CFDT des salariés des industries métallurgiques de la région caennaise, 0903336 (23 septembre 2011)
- CA Montpellier, chambre 5, section A, Marie-Cécile C c/ Google inc, 1100832 (29 septembre 2011)
- CA Paris, Pôle 5, chambre 11, SAS ANTIK BATIK c/ SA SAFETIC, 0920824 (9 septembre 2011)
- Ccass, 1ère chambre civile, Société NORD-OUEST et autres c/ Société DAILYMOTION, 0967896165 (17 février 2011)
- Ccass, chambre commerciale, Ceramconcept c/ Administration des impôts, 1015014 (27 avril 2011)
- Ccass, chambre criminelle, Movsar X et Zarea Y, 1084344 (11 mai 2011)
- Ccass, chambre criminelle, Schering-Plough c/ DGCCRF, 1085479 (29 juin 2011)
- Ccass, chambre sociale, M D c/ Société MOREAU incendies, 1018036 (3 novembre 2011)
- Ccass, chambre sociale, M. X. c/ Méditerranéenne de nettoiement groupe Nicollin, 1014869 (21 septembre 2011)
- Ccass, chambre sociale, Mme T c/ Société UFIFRANCE gestion, 1014685 (5 juillet 2011) .
- CE, Association pour la promotion de l'image et autres, 317827 (26 octobre 2011)
- TA Clermont-Ferrand, SA Notrefamille.com, 1001584 (13 juillet 2011)
- TA Strasbourg, O A, C M, A Z c/ Préfet du Bas-Rhin, 0902015 (5 octobre 2011)
- TA Strasbourg, O A, C M, A Z c/ Préfet du Bas-Rhin, 0902016 (5 octobre 2011)
- TC Nanterre, Greenpeace c/ Thierry L EDF, (10 novembre 2011)
- TGI Charleville-Mézières, Philippe D et al c/ Jean-Luc P et al, 10349000004 (24 février 2011)

- TGI Coutances, René L c/ Stanislas L, 1000822 (6 octobre 2011)

GRÈCE

A. Résumé des activités et actualités

Le Parlement hellénique a récemment adopté la loi 4055/2012, qui comprend certaines dispositions régulant des sujets liés à l'exploitation des autorités indépendantes protégées par la constitution en général et, en particulier, l'autorité de protection des données. La loi susmentionnée présente une proposition préalable de la Commission parlementaire des institutions et de la transparence à la Conférence des présidents du Parlement pour la sélection des présidents et des membres des autorités à un mandat de six ans non renouvelable. Elle stipule en outre que le statut professionnel exclusif à plein temps est également étendu au vice-président de chaque autorité indépendante, avec la possibilité d'une extension de ce statut à un certain nombre de membres du conseil de chaque autorité. Elle prévoit également que le statut professionnel des membres du personnel scientifique responsables de la mission principale de chaque autorité soit le même pour l'ensemble des autorités indépendantes. En outre, la loi 3917/2011 : a) intégrait à notre droit national la Directive 2006/24/CE, b) comprenait des dispositions relatives à l'emploi de systèmes de vidéosurveillance dans les lieux publics et c) portait modification de certaines dispositions de la loi sur la protection des données 2472/1997, dont la plus importante autorisait la DPA à établir des priorités pour le traitement des plaintes et des demandes en fonction de l'importance et de l'intérêt général de la question à traiter. Le reste des amendements concernait des sujets sur la composition de la DPA et sur le détachement d'employés publics au profit de la DPA. Enfin, des amendements ont été apportés à certaines dispositions de la loi 3471/2006 relative à la réception licite de communications non sollicitées avec ou sans intervention humaine.

Une fois de plus, le sérieux problème du manque de personnel, que l'AHPD a connu dès sa création, n'a pas pu être résolu au cours de l'année 2011 en raison de la situation actuelle des finances publiques.

En outre, la baisse continue du budget octroyé à la DPA pour ses besoins opérationnels restreint les capacités de l'AHPD à répondre de manière suffisante à ses obligations.

Plus spécifiquement, l'AHPD a émis deux lignes directrices : a) la Ligne directrice 1/2011 sur l'emploi de systèmes de vidéosurveillance pour la protection des personnes et des marchandises dans des lieux privés accessibles au public et b) la Ligne directrice 2/2011 sur le consentement en ligne relatif aux communications commerciales envoyées par voie électronique (voir la jurisprudence).

L'AHPD a également donné des conseils au gouvernement, au Parlement et autres autorités indépendantes via les Avis et Décisions suivants : a) suite aux demandes du ministère des Finances et du Parlement, l'AHPD a donné son avis sur un certain nombre de questions fiscales concernant, notamment, la publication de données fiscales sur Internet (Avis 1/2011, Avis 4/2011, Avis 7/2011, Décision 54/2011 – voir la jurisprudence), b) l'AHPD a participé à un Comité législatif du ministère de la Justice sur l'incorporation de la Directive 2009/136/CE au droit national et l'amendement de la Loi 3471/2006 sur la protection des données personnelles et de la vie privée dans le cadre des communications électroniques, c) l'AHPD a contribué à la consultation publique sur le projet de règlement de l'Autorité hellénique pour la garantie du secret des communications, une autorité administrative indépendante, d) sur demande du Parlement hellénique, l'AHPD a exprimé son point de vue sur la Proposition de règlement du Parlement européen et du Conseil concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur (« règlement IMI »), e) l'AHPD a exprimé son point de vue à l'Autorité réglementaire de l'énergie, une autre autorité administrative indépendante, sur les mesures proposées pour l'administration de la dette des clients des fournisseurs d'électricité.

Elle a par ailleurs publié la Décision 50/2011 sur le traitement des demandes de règlement extrajudiciaire par « Tiresias Bank Information Systems S.A. », la Décision 52/2011 sur le recensement de la population et des logements conduit par l'Autorité hellénique des statistiques et la Décision 53/2011 sur « Google Maps Service » (voir la jurisprudence).

À l'occasion de la Journée européenne de la protection des données 2011, la DPA hellénique a ajouté une section spéciale à son site web afin de sensibiliser les écoliers du secondaire à une utilisation sûre des services Internet. Par ailleurs, un outil instructif d'auto-évaluation sur le vol d'identité a été créé à destination de tous les groupes d'âge. Le ministère de l'Éducation a apporté son aide à cette initiative en invitant les écoles secondaires à utiliser cette documentation au bénéfice de leurs élèves. En outre, les experts de l'AHPD ont visité des écoles sélectionnées. Enfin, un bulletin a été publié sur le site web, et un communiqué de presse a été édité.

Organisation	
Président et/ou collège	Christos Yeraris (Président) jusqu'en mai 2011 Petros Christoforos (Président) depuis août 2011
Budget	2 339 500 EUR
Personnel	Département des contrôleurs : 16 juristes et 11 experts en informatique (dont cinq (5) en congés maternité, un (1) ayant été détaché une partie de l'année auprès du CEPD en tant qu'expert national, un (1) en congés de formation et un (1) ayant démissionné). Département des communications et des relations publiques : 5 personnes (dont une (1) en congés maternité et formation pour la moitié de l'année), Département des ressources humaines et des finances : 16 personnes et un (1) détachement d'un autre service public.
Activités générales	
Décisions, avis, recommandations	L'AHPD a émis 168 décisions, 7 avis et 2 lignes directrices, dont 6 décisions, 5 avis et 2 lignes directrices ayant un impact sur la protection des données en général.
Notifications	L'AHPD a examiné 702 notifications (dont 414 concernaient l'installation et l'utilisation de systèmes de vidéosurveillance et 70 des transferts de données vers des pays en dehors de l'UE)
Examens préalables	L'AHPD a octroyé ou renouvelé 63 autorisations de traitement de données sensibles, d'interconnexion de fichiers et de transfert de données vers des pays en dehors de l'UE)
Demandes émanant des personnes concernées et des responsables du traitement des	1 011

données	
Plaintes émanant des personnes concernées	812 (autorités judiciaires et policières nationales : 76, défense nationale : 2, administration publique et gouvernement local : 33, fiscalité – ministère des Finances : 4, santé : 20, sécurité sociale : 9, éducation et recherche : 5, banques : 51, secteur privé : 163, communications électroniques : 131, relations professionnelles : 25, moyens de communication de masse : 7, autres : 286)
Conseils sollicités par le Parlement ou le gouvernement	9 (Avis 1/2011, Avis 4/2011, Avis 7/2011, Décision 50/2011, Décision 52/2011 – voir également la section A – synthèse)
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	7 contrôles (dont 3 : ministère de l'Éducation, 1 : unité Eurodac nationale, 1 : autorité antiblanchiment d'argent, 1 : sécurité sociale (système de prescription en ligne) et 1 : secteur privé.
Activités de sanction	
Sanctions	22 sanctions (18 avertissements, 4 amendes) décidées par la DPA dans les secteurs suivants : soins de santé (13) sécurité sociale/assurance (2), spam (2), vidéosurveillance (2), télécommunications (1), banques (1), secteur public (1).
Amendes	Montants : 3 000 EUR – 10 000 EUR (au total, 27 000 EUR) ont été imposés par l'AHPD
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Ligne directrice 1/2011

L'AHPD a publié la Ligne directrice 1/2011 sur l'utilisation de systèmes de vidéosurveillance pour la protection des personnes et des biens dans des lieux privés accessibles au public, remplaçant la précédente. Celle-ci comprend des dispositions générales et spécifiques sur différentes catégories de responsables du traitement, une attention particulière ayant été portée à l'application du principe de proportionnalité.

Ligne directrice 2/2011

L'AHPD a publié la Ligne directrice 2/2011 sur le consentement en ligne relatif aux communications commerciales envoyées par voie électronique. Celle-ci définit la procédure de consentement des utilisateurs pour qu'il soit considéré comme valide, et donne des conseils aux responsables du traitement

des données sur la procédure et les moyens techniques dont ils devraient disposer pour prouver qu'un consentement a été donné en ligne.

Avis 1/2011

Un avis a été donné quant à la légalité de deux applications différentes prévues par le Secrétariat général des systèmes d'information, du ministère des Finances, pour la publication de listes de contribuables sur Internet. Dans le premier cas, l'Autorité a jugé que la publication de listes de contribuables dans les bureaux du fisc, des municipalités, dans les médias et sur Internet aux fins de la lutte contre l'évasion fiscale n'était pas conforme au principe de proportionnalité. Concernant la deuxième application, l'AHPD a jugé que le service de validation des données du registre de contribuables était conforme aux Articles 9(a) et 25, alinéa 1, de la Constitution dans la mesure où aucune information sur les revenus des contribuables et les impôts correspondants n'était révélée.

Avis 4/2011

L'AHPD a jugé que la publication de la liste des créditeurs en souffrance de l'État grec sur Internet par le Secrétariat général des systèmes d'information, du ministère des Finances, pour laquelle le législateur grec avait opté, dans la difficile situation financière publique actuelle, en tant que mesure appropriée en principe pour l'exécution des obligations fiscales des citoyens envers l'État, représente un traitement des données tolérable sur le plan constitutionnel, qui ne dépasse pas les limites du principe de proportionnalité. Dans ce contexte, l'Autorité a considéré que la publication susmentionnée ne contrevient pas à la règle supérieure de sauvegarde du droit des personnes à la protection de leurs données personnelles, si certaines conditions, définies par l'AHPD, sont réunies.

Avis 7/2011

L'AHPD a publié un avis sur la publication sur Internet de déclarations d'actifs des membres du Parlement sur demande du Parlement grec. Compte tenu de la loi, qui stipule expressément la publication des déclarations des actifs des membres du Parlement, y compris sur le site web du Parlement, l'AHPD a jugé que la limitation du droit personnel est prévue dans la loi, justifiée par des motifs d'intérêt public suffisants, dans la mesure où elle sert à la transparence de la vie politique et publique, où elle respecte les limites de la proportionnalité et sert des intérêts juridiques supérieurs.

Décision 50/2011

Sur une question du Secrétariat général des affaires des consommateurs, l'AHPD a estimé que les données liées à la soumission de demandes de règlements extrajudiciaires, prévue dans la législation grecque, sont collectées en toute légalité par l'agence d'évaluation du crédit, TIRESIAS Bank Information Systems S.A., sans le consentement des personnes concernées. Les institutions de crédit ne peuvent avoir accès à ces données qu'avec le consentement des personnes concernées lorsque celles-ci ont demandé un emprunt.

Décision 52/2011

L'AHPD a estimé que le cadre juridique national concernant la procédure de recensement de la population et des logements, en vigueur lors du recensement de 2011, ne respectait pas les conditions définies par le Conseil d'État grec et la Cour européenne des droits de l'homme eu égard aux limitations des droits

personnels, dans la mesure où les questions de base relatives au recensement général de la population et des logements n'étaient pas clairement et spécifiquement prévues par quelque loi ou décret présidentiel que ce soit. La DPA a par ailleurs défini les spécifications des mesures organisationnelles et techniques requises pour la sécurité de ces données. Résultat : ce vide juridique a été comblé par la loi 3995/2011.

Décision 53/2011

En 2011, Google Inc. a amendé sa notification initiale à l'AHPD concernant le service « Street View », alors en suspens, eu égard à son objet, et désigné un représentant local, Google Greece Applications Ltd. La société a déclaré la cartographie routière des régions grecques comme étant son seul objet, qui servirait également à d'autres fins ou services pertinents, tels que des services de navigation. L'AHPD a considéré que le service « Google Maps » entraînait une forme de traitement de données personnelles dans la mesure où les images prises comprennent des visages, des plaques d'immatriculation de véhicules et des maisons. Ce traitement est licite en vertu de la loi relative à la protection des données, puisque le déploiement d'une activité économique constitue en principe un objet licite. Néanmoins, étant donné que les personnes concernées, qui peuvent être directement ou indirectement identifiées à partir des images, n'ont préalablement eu aucune relation contractuelle ou autre avec le responsable du traitement, le service doit être fourni dans certaines conditions, telles que, notamment : a) le floutage permanent des images de visages, de plaques d'immatriculation et de maisons dans un délai d'un an à compter du jour où les photos ont été prises, b) des mesures de sécurité organisationnelle et technique adéquates pour la protection des données brutes, c) des mesures visant à éviter la collecte et le traitement d'images susceptibles de révéler des données personnelles sensibles, d) la notification préalable adéquate au public par voie d'annonces appropriées dans la presse et sur Internet, et e) le respect du droit d'accès, sous réserve que les personnes concernées donnent des informations adéquates pour localiser les données qui les concernent.

Décision 54/2011

L'AHPD a jugé que la publication, sur le site web du ministère des Finances, de listes de médecins soupçonnés d'évasion fiscale, n'était pas prévue par la loi et était contraire à une disposition légale établissant le secret fiscal, qui ne peut être contournée que dans des cas prévus par des dispositions légales spécifiques. L'Autorité en a conclu que cette publication constituait un traitement illicite des données et a adressé un avertissement au responsable afin qu'il cesse ce traitement dans un délai de quinze (15) jours et retire le communiqué de presse visé du site web du ministère des Finances.

HONGRIE

A. Résumé des activités et actualités

Le Commissaire parlementaire à la protection des données et à la liberté d'information, en tant que responsable de la DPA en 2011, n'a pas complété de rapport annuel ni de base de données statistiques cumulative sur ses activités de 2011. L'Autorité nationale de la protection des données et de la liberté d'information (créée en janvier 2012) fournit ci-dessous les chiffres de 2011 sur la base des registres produits par le bureau du Commissaire.

Organisation	Commissaire parlementaire à la protection des données et à la liberté d'information
Président et/ou collège	Dr András Jóri
Budget	352 381 000 HUF
Personnel	49
Activités générales	
Décisions, avis, recommandations	5 461 (nombre d'affaires, dont des notifications du registre de protection des données). 71 recommandations sont disponibles sur la page web officielle du Commissaire parlementaire depuis 2011.
Notifications	s. o.
Examens préalables	14 (tous liés aux notifications du registre de protection des données)
Demandes émanant des personnes concernées	3 162 (notifications du registre de protection des données)
Plaintes émanant des personnes concernées	949
Conseils sollicités par le Parlement ou le gouvernement	290 (avis donnés sur le projet de loi concernant des problèmes de protection des données ou de liberté de l'information)
Autres renseignements relatifs aux activités générales	797 consultations, 112 cas internationaux (relatifs à des problèmes de protection des données ou de liberté de l'information)
Activités d'inspection	
Contrôles, enquêtes	309 (en relation à des plaintes déposées et justifiées)

Activités de sanction	
Sanctions	Le Commissaire parlementaire n'était pas autorisé à en émettre
Amendes	Le Commissaire parlementaire n'était pas autorisé à en émettre
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Deux exemples importants :

a) *Traitement illicite des données – opérateur de sites web* (www.ingatlandepo.com et www.ingatlanbazar.com)

Le Commissaire à la protection des données (ci-après « la DPA ») a enquêté sur le cas d'un opérateur de sites web (ci-après le « responsable du traitement des données »). Des contrats ont été conclus entre des personnes concernées en Hongrie et le responsable du traitement des données dans le but de promouvoir des biens immobiliers aux noms des personnes concernées sur le site web du responsable du traitement des données.

Une fois les biens immobiliers vendus, les publicités expiraient ou les personnes concernées souhaitaient simplement les effacer (ou les faire effacer par le responsable du traitement des données). Sans succès. Malgré leurs demandes insistantes, le responsable du traitement des données n'a pas effacé les publicités. Le responsable du traitement des données a par ailleurs communiqué les données personnelles des personnes concernées à des sociétés de gestion des réclamations, entre autres.

De nombreuses plaintes ont été reçues par la DPA en raison des problèmes susmentionnés. La DPA a par conséquent lancé une procédure d'enquête et appelé le responsable du traitement des données à faire des déclarations sur son comportement dans un certain délai.

Suite à cette procédure, la DPA a conclu que le responsable du traitement des données avait violé le droit à la vie privée des personnes concernées en de multiples occasions. Le responsable du traitement des données a notamment enfreint le principe de proportionnalité, le droit à l'information, le droit des personnes concernées d'effacer leurs données personnelles ou de les faire effacer par le responsable du traitement des données, ainsi que le principe de limitation de la finalité. Le responsable du traitement des données a par ailleurs négligé les multiples objections des personnes concernées par rapport au traitement des données par le responsable des données. C'est pourquoi le responsable du traitement des données ne disposait pas des bases légales essentielles pour ses différentes activités de traitement des données.

La DPA a par conséquent publié un communiqué de presse et une déclaration affirmant que la divulgation des publicités pour des biens immobiliers impliquant également le traitement de données personnelles, était illégale malgré le consentement explicite des clients. Ces méthodes ne sauraient en outre servir de sanction en cas de réclamation à l'encontre de clients. La DPA a rappelé aux clients qu'il convenait de consulter attentivement la politique d'un prestataire de service en matière de vie privée avant de lui confier des données personnelles.

b) Identification biométrique dans le cadre de passes d'entrée aux bains publics

Un client, dans sa soumission, a demandé à la DPA de faire une déclaration officielle sur le fait de savoir si le traitement des données d'un opérateur de bains publics pouvait être légal lorsque l'opérateur entend installer un système d'identification biométrique pour ses passes d'entrée. D'après les intentions de l'opérateur, le système biométrique stockerait les empreintes digitales des clients, ce qui permettrait un système d'identification plus efficace et personnalisé pour le prestataire de services.

Dans sa soumission, le client demandait si les empreintes digitales pouvaient être qualifiées de données personnelles pouvant être contrôlées suite à l'obtention du consentement de la personne concernée. Le client demandait également s'il n'existait pas des règles spécifiques et éventuellement plus strictes pour régir le traitement des données des empreintes digitales.

Compte tenu de la réglementation nationale et européenne applicable, il a été conseillé ce qui suit au client :

Les empreintes digitales d'une personne sont considérées comme des données personnelles et la prise d'empreintes digitales ainsi que leur stockage sont considérés comme une forme de traitement de données. Non seulement la législation nationale en vigueur, mais également la Directive européenne relative à la protection des données, stipulent les principes juridiques fondamentaux qui devraient également être pris en compte dans le cadre des activités de traitement de données. Ceux-ci comprennent, notamment, les principes de proportionnalité et de nécessité.

Le groupe de travail (WP 29) sur la protection des données a rappelé la nécessité d'enquêter sur la question de savoir si l'exploitation du système d'identification biométrique était nécessaire à la réalisation des objectifs du prestataire de services. À cet égard, les aspects suivants seront examinés afin de déterminer :

- Si l'installation d'un tel système est indispensable ou simplement rentable et confortable;
- Si l'exploitation d'un tel système sera efficace et, si tel est le cas, dans quelle mesure;
- Si la restriction de la vie privée est proportionnelle aux avantages prévisibles;
- Si les objectifs fixés par le prestataire de services pourraient être atteints par des moyens moins restrictifs.

Enfin, pour conclure, la DPA a estimé qu'un système biométrique (visant à prendre et à stocker les empreintes digitales de clients entrant aux bains publics ou dans un spa) aux fins d'une identification plus efficace des personnes ne respecte pas les exigences de proportionnalité. Une meilleure identification pourrait être assurée d'une autre manière, plus inoffensive et moins restrictive pour la vie privée, telle que des passes d'entrée dotés de photos, etc. Par conséquent, l'introduction d'un système de ce type ne respecterait pas les règles de protection des données.

C. Autres informations importantes

Évolution importante de la législation en Hongrie

En conséquence d'une évolution fondamentale de la structure constitutionnelle de la Hongrie, suite à une décision de l'Assemblée nationale hongroise en 2011, l'ancien bureau du Commissaire à la protection des données a été fermé et un nouvel organisme, appelé Autorité nationale pour la protection des données et

la liberté d'information, a été chargée des responsabilités susmentionnées. Elle devait commencer à travailler le 1er janvier 2012. Le nouvel instrument juridique ayant vocation à régir les domaines de la protection des données et de la liberté de l'information, la Loi CXII de 2011 sur le droit à l'autodétermination informationnelle et la liberté de l'information, a été adoptée par le Parlement le 11 juillet 2011.

IRLANDE

A. Résumé des activités et actualités

Le Bureau du Commissaire à la protection des données a ouvert 1 161 enquêtes officielles sur des plaintes en 2011 (de nombreuses plaintes étant gérées de manière informelle en fournissant au plaignant les informations appropriées sur ses droits). Comme les années précédentes, la grande majorité des plaintes ont été résolues à l'amiable, 17 plaintes seulement donnant lieu à des décisions formelles. Les informations relatives aux poursuites en 2011 figurent dans la Section B du présent rapport. Les notifications de violations de la sécurité des données personnelles adressées au Bureau sont en nette augmentation, principalement suite à l'introduction, en juillet 2010, d'un nouveau Code de bonnes pratiques en matière d'atteintes à la sécurité des données personnelles. Le Commissaire a poursuivi son engagement auprès des grandes organisations du secteur public sur l'ampleur du partage des données dans le secteur public. Sur la base de ces engagements et du contrôle de plusieurs entités du secteur, le Commissaire a convenu d'un ensemble de lignes directrices applicables à toutes les organisations du secteur public, dont les principes directeurs sont la transparence et la proportionnalité. Les autres conseils publiés comprennent les conseils en cas d'atteintes à la sécurité des données à caractère personnel révisés, les conseils sur la sécurité des données révisés et les nouveaux conseils relatifs aux enquêtes sur les employés.

Organisation	Bureau du Commissaire à la protection des données
Président et/ou collège	Billy Hawkes
Budget	1 458 000 EUR (1 516 404,20 EUR)
Personnel	20
Activités générales	
Avis, recommandations	3 (Conseils)
Notifications	Environ 5 000 inscriptions en 2011
Examens préalables	Aucun
Demandes émanant des personnes concernées	15 000
Plaintes émanant des personnes concernées	1 161 (droit d'accès : 48 %, marketing direct par voie électronique : 22 %, divulgation : 10 %, traitement déloyal : 10 %, autres : 10 %).
Conseils sollicités par le Parlement ou le gouvernement	> 100
Autres renseignements relatifs aux activités générales	1 167 notifications d'atteintes à la sécurité des données à caractère personnel provenant de 186 organisations différentes.

Activités d'inspection	
Contrôles	28 audits (contrôles)
Activités de sanction	
Sanctions	54 poursuites en 2011 à l'encontre de 6 entités
Amendes	15 400 EUR + frais (amendes / règlements imposés par les tribunaux)
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Au cours de l'année 2011, plusieurs poursuites engagées par le Commissaire vis-à-vis des droits des personnes concernées en vertu des lois de 1988 et 2003 sur la protection des données et de l'arrêté 535 de 2003 (transposition de la Directive 2002/58/CE en Irlande) ont abouti. Six entités ont été poursuivies pour différents délits en 2011.

C. Autres informations importantes

Transposition de la Directive vie privée et communications électroniques

Le 1er juillet 2011, l'Irlande a transposé la Directive vie privée et communications électroniques révisée via la SI 336 de 2011.

Les Règlements ont introduit une obligation de notification des violations de données pour les fournisseurs et les réseaux de communications électroniques. Ils ont également renforcé les obligations des entités en termes de mesures de sécurité qu'elles doivent prendre pour protéger les données personnelles dont elles sont responsables. Elles doivent, notamment, s'assurer que ces données personnelles sont sûres et à disposition uniquement du personnel approuvé qui en a besoin. Le non-respect de ces exigences peut entraîner des poursuites pénales avec des amendes pouvant s'élever à 5 000 EUR et une inculpation de 250 000 EUR par délit.

L'opportunité a également été saisie, dans le cadre de la nouvelle loi, de clarifier un certain nombre de questions liées aux contacts de marketing direct avec les clients, la plus intéressante étant peut-être que le consentement préalable d'une personne est désormais requis avant de l'appeler sur son téléphone mobile à des fins de marketing, sauf si le numéro est enregistré comme acceptant de recevoir des appels marketing dans les bases de données des annuaires nationaux (NDD), sachant que le nombre de numéros qui y sont enregistrés s'élevait à douze le 13 mars 2012 !

Il est également intéressant de noter qu'un message SMS non-marketing ne peut pas non plus présenter de contenu marketing « balisé » si le destinataire n'a pas donné son consentement préalable à ce type de messages. Les exigences sont en outre étendues à toutes formes de marketing par voie de

communications électroniques publiquement disponibles (y compris, par exemple, la sollicitation d'aide à destination d'œuvres caritatives ou de partis politiques).

ITALIE

A. Résumé des activités et actualités

Actualités et évolution des lois :

D'importantes modifications ont été apportées au Code de protection des données italien en 2011. Celles-ci ont principalement porté sur les points suivants :

- Traitement des données personnelles des personnes morales : La loi contenant des mesures financières urgentes (mai 2011) excluait les personnes morales du champ d'application du Code de protection des données si le traitement était effectué à des fins administratives et de comptabilité et dans le cadre de relations interentreprises (voir Section 5(3) du Code de protection des données). Après l'abolition de cette disposition (en décembre 2011), un nouvel amendement au Code (Section 4), introduit en mai 2012, exclut en fin de compte les personnes morales de la définition de « données à caractère personnel » (les données personnelles étant ainsi « toute information relative à une personne physique » uniquement). Cela signifie qu'à l'heure actuelle, le Code de protection des données ne s'applique pas au traitement de données personnelles de personnes morales (ce qui comprend les associations, fondations, comités, etc.) ; la DPA a néanmoins émis un avis détaillé (publié en octobre 2012) afin de clarifier qu'il convient de ne pas exclure les personnes morales de l'interprétation du Code, dans la mesure où les personnes morales sont « abonnées » à un service de communications électroniques disponible publiquement, conformément aux définitions données par le Code pour ce qui concerne la Directive vie privée et communications électroniques (Article 4(2)f.);

- Télémarketing : En plus du marketing par téléphone, la loi de 2011 sur les mesures financières urgentes a également étendu le régime de retrait au marketing postal non sollicité. Selon ce dernier amendement, les sociétés de marketing direct peuvent désormais se servir des adresses postales figurant dans les annuaires d'abonnés sans avoir à obtenir au préalable le consentement de ces derniers et sous réserve qu'ils ne se soient pas désinscrits de cette activité promotionnelle en entrant leur numéro de téléphone et leur adresse postale dans le registre prévu à cet effet ;

- Document de politique de sécurité : Un autre type de simplification a été introduit par la loi de 2011 afin d'exempter les « entités [qui] ne traitent que des données personnelles non sensibles ou des données sensibles et judiciaires liées à leurs employés et collaborateurs respectifs, y compris les citoyens de pays hors UE et/ou leurs époux/épouses et/ou proches » du « Document de politique de sécurité » (*Documento programmatico per la sicurezza*, DPS) à remettre à la DPA. Cette obligation a été abolie par un amendement du Code de protection des données introduit en mai 2012. Il convient de rappeler que toutes les autres mesures de sécurité restent pleinement applicables;

- D'autres amendements ont été apportés par la loi de 2011 exemptant les entités privées et les organismes publics à but lucratif de l'obtention du consentement préalable pour traiter les données personnelles des CV ou biographies si ceux-ci sont envoyés volontairement par des candidats à des emplois et pour transférer des informations personnelles au sein d'un groupe d'entreprises.

Principaux domaines d'activités au cours de l'année 2011:

Journalisme et informations en ligne : Tout en reconnaissant que la publication de transcriptions judiciaires ne faisait plus l'objet de contraintes de confidentialité et relevait de la liberté d'expression, la

DPA a adressé une injonction à un site web interdisant la diffusion en ligne d'informations excessives et sans rapport avec l'objet spécifique des informations (même si l'ordonnance judiciaire imposait un placement en détention préventive).

Données génétiques : L'autorisation générale accordée par la DPA pour le traitement de données génétiques a été précisée suite à un avis donné au ministère de la Santé italien. La nouvelle autorisation générale tient compte de l'expérience et des contributions des experts faisant autorité en la matière et a par ailleurs été accordée aux organisations de médiation publiques et privées conformément à la législation récemment adoptée.

Traitement à des fins de recherche scientifique : En 2011, les demandes d'autorisation de traitement des données à des fins de recherche scientifique sans le consentement des personnes concernées ont explosé en raison de l'impossibilité alléguée d'informer une grande partie des patients concernés. La DPA a émis une autorisation générale provisoire tenant compte des cas les plus fréquents où il peut être justifié de ne pas informer les personnes concernées (en particulier pour des « raisons éthiques » et/ou en cas « d'impossibilité résultant d'arrangements organisationnels »).

Traitement des données dans le cadre des relations employeur-employé : Plusieurs décisions publiées en 2011 soulignaient les multiples situations où les relations employeur-employé se développent avec la nécessité de considérer soigneusement la pertinence de toutes informations personnelles utilisées dans ce contexte. Les principales décisions concernaient le contrôle de la navigation des employés sur Internet ; l'admissibilité, dans le cadre de procédures disciplinaires, d'informations tirées du web ; l'utilisation de questionnaires sur la personnalité des employés ; la divulgation d'informations sur des allégations de travail au noir (seconds emplois) à l'organisme national d'assurance professionnelle ; la géolocalisation des employés, etc.

Télémarketing: La DPA a clarifié le fait que le rôle joué par les entités qui déploient des activités de télémarketing devrait être déterminé compte tenu des circonstances dans lesquelles le traitement des données personnelles a lieu. En principe, le responsable du traitement des données est l'entité au nom de laquelle les activités promotionnelles sont déployées. La DPA italienne a par conséquent spécifié que toute société sous-traitant ses activités promotionnelles à des prestataires externes tout en gardant le contrôle opérationnel desdites activités devait formellement désigner les promoteurs, agents, etc. en question en tant que responsables du traitement des données conformément à la loi italienne sur la protection des données.

Appels marketing non sollicités, suite à l'établissement du « Registre des numéros à ne pas appeler » pour les utilisateurs ne souhaitant pas recevoir d'appels promotionnels, à la lumière des difficultés de mise en œuvre correspondantes.

Appels « silencieux », c'est-à-dire ces appels téléphoniques, reçus parfois plusieurs fois dans une même journée, où l'utilisateur est laissé seul, sans avertissement ni recours, face au silence de l'appelant. Dans ce contexte, la DPA a ordonné à une société qui employait un système de composition d'appels de mettre en place divers arrangements et mesures visant à prévenir les appels silencieux répétés et à ne pas rappeler un même numéro pendant une période d'au moins 30 jours.

Fax non sollicités : La DPA a conclu que le Code de protection des données italien s'appliquait à une société établie dans un pays tiers qui conservait les données personnelles de clients (prospectifs) dans ledit pays et faisait appel à des mécanismes de gestion des données à distance, dans la mesure où cette société utilisait en substance un équipement de transmission (serveur de fax) localisé en Italie. C'est la raison pour laquelle les fax promotionnels envoyés par cette société sans adresser d'avis d'information et sans obtenir le consentement préalable des destinataires ont été déclarés illégaux et interdits.

Téléphonie : Les principaux domaines d'activité dans ce cas sont liés aux « annuaires d'abonnés en ligne » : plusieurs plaintes ont été déposées à l'encontre d'une société qui avait posté sur Internet un annuaire d'abonnés comprenant des informations « confidentielles ». La DPA a déclaré le traitement en question illégal, dans la mesure où les données personnelles contenues dans l'annuaire n'avaient pas été tirées de la « base de données téléphonique unifiée » (DBU, Database Unico), la seule source légitime d'annuaires d'abonnés au téléphone au regard du droit italien.

Relations avec le Parlement et autres institutions

La DPA a été entendue par le Parlement en plusieurs occasions avant les réunions de Comités et autres Forums parlementaires sur des questions présentées par le Parlement et en connexion avec des initiatives d'observation ou préalablement à l'adoption de lois. Dans tous les cas, la DPA a souligné les possibles implications pour le traitement de données à caractère personnel. Il est possible de se référer en particulier aux points suivants:

Aux lois contenant des dispositions permettant l'implantation d'embryons non utilisés et conservés dans les centres italiens de reproduction médicalement assistée ;

Aux amendements du Code de protection des données italien (voir ci-dessus) ; aux dispositions supplémentaires correspondantes du Décret n° 70/2011 (mesures financières urgentes) ;

Au fonctionnement du système de codage national unifié utilisé en connexion avec l'étude comparative sur l'efficacité, la qualité et le caractère approprié des agences de santé italiennes ;

Aux investigations d'observation des maladies dégénératives d'une importance sociale particulière, notamment au regard du cancer du sein, des maladies rhumatismales chroniques et du syndrome du VIH.

L'avis de la DPA sur la législation secondaire (mesures gouvernementales) et la législation régionale ayant un impact sur la protection des données personnelles (en vertu de l'Article 154(4) du Code de protection des données) devrait également bénéficier d'une attention particulière. Citons ainsi l'Avis sur le Registre des prothèses mammaires ; un règlement qui définit les règles techniques de la mise en œuvre des TIC dans le cadre des procédures civiles et pénales ; les règles techniques de l'identification du propriétaire d'un compte de messagerie électronique certifié via les réseaux électroniques également ; la gestion du Registre des auditeurs et des sociétés d'audit ; les lignes directrices publiées par Digit-PA [l'agence publique en charge de l'hébergement des TIC dans l'administration publique] concernant la reprise après un sinistre dans le secteur public ; les dispositions complétant le code de procédure civile italien quant à la réduction et la simplification des procédures d'observation en vertu du droit civil. Il convient néanmoins de souligner qu'il n'a pas été demandé à la DPA de donner les conseils prescrits par la loi dans tous les cas où des problèmes de protection des données ont été soulevés.

La dimension internationale

Outre sa contribution active au travail du groupe de travail « Article 29 » (WP29), la DPA italienne a poursuivi les développements suivants dans le cadre de la réforme européenne de la protection des données (en particulier via ses contributions au sous-groupe Avenir de la protection de la vie privée du WP29 sur les exigences de notification simplifiées, le traitement des données à caractère personnel et la coopération entre les DPA européennes). La DPA italienne participe aussi activement à des groupes de travail de l'OCDE qui traitent de questions relatives à la vie privée et à la protection des données (en particulier le groupe de travail sur la sécurité de l'information et la vie privée – GTSIVP) ainsi qu'au Comité consultatif et au Bureau du T-PD du Conseil de l'Europe (qui travaille actuellement à une révision de la Convention 108/1981). La DPA fait partie des autorités de contrôle communes compétentes pour

contrôler le fonctionnement des systèmes de partage d'information (Autorité de contrôle commune (ACC) Europol, Autorité de contrôle commune (ACC) Schengen, Autorité de contrôle commune Système d'Information Douanier (SID), groupe de coordination Eurodac). Il convient également de mentionner ses activités liées au Groupe de Berlin (groupe de travail international sur la protection des données dans les télécommunications), où elle a été corapporteur du Document de travail sur le droit à la vie privée et le droit à l'oubli sur Internet, ainsi que sa contribution aux discussions de l'atelier de traitement des dossiers des DPA européennes. Dans le domaine de la coopération avec les autorités policières et judiciaires en matière pénale, la DPA a poursuivi ses activités de soutien en faveur du WPPJ (groupe de travail sur la police et la justice) et de son Président, le Professeur Pizzetti, jusqu'à la dissolution dudit groupe de travail.

Autres domaines d'activité

La DPA a poursuivi ses initiatives de sensibilisation en se concentrant essentiellement sur les jeunes ; à ces fins, des initiatives de publication ad hoc ont été lancées concernant les réseaux sociaux, l'école et la santé. Un concours, intitulé « *Privacy 2.0: Youths and New Technologies* » (vie privée 2.0 : les jeunes et les nouvelles technologies) a également été organisé à destination des élèves du secondaire, qui ont été invités à créer des courts métrages sur la vie privée et à tenir les rôles de scénaristes, d'acteurs, de réalisateurs, etc.

Organisation	Garante per la protezione dei dati personali (Autorité italienne de protection des données personnelles)
Président et/ou collège	Président : Prof. Francesco Pizetti Collège : Giuseppe Chiaravalloti Mauro Paissan Giuseppe Fortunato
Budget	Environ 8,5 millions d'EUR (financés par le Gouvernement)
Personnel	123
Activités générales	
Décisions, avis, recommandations	Nombre de décisions prises par le Collège : environ 540
Notifications	1 218
Examens préalables	22
Demandes émanant des personnes concernées	Nombre total de demandes : environ 4 450 Demandes d'informations (*quesiti*) : 332 Dénonciations et réclamations (*segnalazioni* et *reclami*) reçues en 2011, émanant des personnes concernées : 4 022
Plaintes émanant des personnes concernées	(Plaintes officielles, réglementées spécifiquement par le Code de protection des données, concernant l'accès à ses propres données

	personnelles) Environ 260
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 : 32 Sujets : police, sécurité publique : 2 Activité judiciaire : 2 Administration en ligne et bases de données : 8 Éducation et formation : 3 Emploi au sein d'organismes publics : 2 Santé : 6 Entreprises : 5 Aides sociales : 2 Registre des naissances, des décès et des mariages : 2
Autres renseignements relatifs aux activités générales	Les services de première ligne de la DPA ont reçu, en 2011, environ 32 000 appels téléphoniques et courriels Autorisations nationales pour des règles d'entreprise contraignantes (BCR) : 1
Activités d'inspection	
Contrôles, enquêtes	Nombre de contrôles et/ou d'enquêtes (sur place) : environ 450 (dont 37 infractions à caractère criminel rapportées aux autorités judiciaires)
Activités de sanction	
Sanctions	Environ 400
Amendes	Montant : environ 3,1 millions d'EUR imposés par la police financière chargée des contrôles au nom de la DPA
DPD	
Chiffres relatifs aux DPD	s. o. (aucun DPD prévu par le système juridique italien)

B. Informations sur la jurisprudence

Relations entre droit de défense et protection de la vie privée

Une décision de la Cour de cassation du 8 février 2011 a fait l'objet de nombreux débats. L'affaire en question concernait le transfert (ou, plus précisément, la diffusion illicite) de données personnelles détenues par un avocat ayant conservé le dossier de son client au-delà de la cessation de leur contrat parce que ses honoraires ne lui avaient pas encore été réglés. Le dossier en question contenait des informations sensibles. La Cour a établi qu'il était nécessaire de tenir compte des « caractéristiques réelles de la relation entre la collecte de données et le/les objets sous-jacents » ; ici, les données en question avaient été collectées « afin d'établir ou de défendre un droit juridique. » Il aurait toutefois fallu établir en première instance si toutes les données détenues par l'avocat étaient *de facto* nécessaires à l'avocat pour défendre sa créance vis-à-vis de son client. En résumé, la Cour de cassation a affirmé la nécessité de respecter les principes d'équité, de pertinence et de non-excessivité des données visés au Code de protection des données et confirmé le fait que quiconque détient des informations sensibles sur une autre personne ne peut en aucun cas diffuser ces informations (sous peine des sanctions prévues à l'Article 167 du Code de protection des données).

La Cour de cassation (Division du droit criminel) a par ailleurs prononcé un jugement similaire le 24 mars 2011. Selon la Cour, « la divulgation d'une conversation enregistrée à d'autres fins que de protéger ses droits ou ceux d'une autre personne » constitue une infraction pénale punie par l'Article 167 du Code de protection des données. Dans l'affaire en question, la conversation avait été enregistrée par un détective privé utilisant un stylo qui contenait un microphone et une micro-caméra invisibles aux yeux des tiers.

Concernant la relation entre l'exercice du droit à la liberté d'information dans le cadre de procédures judiciaires et la législation sur la protection des données personnelles, la jurisprudence semble établir que le droit à la liberté d'information prévaut sur les conflits d'intérêts expressément prévus par le droit (et, notamment, la législation sur la liberté d'information). Plus spécifiquement, le droit à la liberté d'information prévaut sur le droit des tiers à la vie privée même si des informations sensibles sont en cause. Cette opinion a reçu le soutien de différents tribunaux administratifs : le tribunal administratif régional de Toscane, par son jugement du 12 mai 2011 ; le tribunal administratif régional de Ligurie, par son jugement du 1er juin 2011, qui stipule que « protéger le droit à la vie privée ne constitue pas un motif suffisant pour rejeter la demande de produire quelque document que ce soit » ; le tribunal administratif régional de Lombardie, par son jugement du 1er août 2011.

Surveillance dans le contexte de l'emploi

Dans une décision du 22 mars 2011, la Cour de cassation (Division du droit du travail) a jugé que si des appareils audiovisuels avaient été installés dans une société en vertu d'un accord préalable conclu avec les représentants compétents des syndicats, tout enregistrement montrant le comportement d'un employé produit afin de justifier son renvoi (au motif du vol d'actifs de l'entreprise) pouvait être exploité dans le cadre des poursuites judiciaires y afférentes. Par ailleurs, une décision de la Cour de cassation (Division du droit criminel) du 9 août 2011 a clarifié le fait que des enregistrements de la police réalisés à l'intérieur d'une unité de soins de santé étaient admissibles en tant que preuves lors d'un procès, dans la mesure où ils permettaient de démontrer qu'un employé avait manipulé le système de pointage. Du point de vue du plaignant, le lieu de travail étant équivalent au domicile, tout enregistrement audiovisuel doit être autorisé et justifié par l'autorité judiciaire compétente. La Cour a clarifié le concept de « domicile », qui fait référence à une relation particulière avec un lieu où la vie privée d'une personne se déroule d'une manière qui prévient l'exposition de la personne à toute interférence externe en toutes circonstances. À l'inverse, cette vérité ne s'applique pas aux lieux publics, même s'il s'agit du lieu de travail du défendant, et encore

moins s'il s'agit de l'entrée d'une unité de soins de santé, à savoir une zone de transit pour tous les employés et tous les utilisateurs desdits services de santé.

Vie privée et journalisme

Dans un jugement du 28 septembre 2011, la Cour de cassation (Division du droit civil) a confirmé le jugement d'une Cour d'appel qui avait établi que la publication d'un journal n'avait causé aucun tort, les faits en question ayant été avérés. D'après la Cour de cassation, aucun tort n'est causé à l'identité d'une personne si l'article d'un journal se contente de rapporter des circonstances factuelles qui ont réellement eu lieu.

LETTONIE

A. Résumé des activités et actualités

En 2011, une évolution importante a porté sur une nouvelle fonction confiée à l'Inspection nationale des données de Lettonie afin d'assurer la mise en œuvre de la Directive 2009/136/CE dans le cadre de la notification de violations de données. Des amendements de la Loi sur les communications électroniques ont été élaborés (et sont entrés en vigueur le 8 juin 2011) mais cette fonction a été confiée à l'Inspection sans que celle-ci ne bénéficie de ressources supplémentaires, ce qui représente un véritable défi pour l'Inspection.

En 2011, le traitement de données personnelles sensibles a été déterminé comme étant une priorité lors d'activités de contrôle préventives concomitantes (par exemple, dans le cadre du traitement de données médicales, de l'emploi de la vidéosurveillance dans les hôpitaux et les centres sociaux spécialisés). 30 % de tous les examens préalables ont été réalisés dans des cas de traitement de données dans le secteur de la santé. Dans de nombreux cas, la conclusion de ces activités de contrôle était la suivante :

1. Aucune procédure interne de protection des données n'avait été mise en place, et aucun audit sur la protection des données n'avait été réalisé.

2. Les droits d'accès n'avaient pas été déterminés en fonction des obligations des employés.

3. Les activités de contrôle relatives au droit d'accès n'avaient pas été mises en place.

Le travail des délégués à la protection des données a également été supervisé, dans la mesure où le nombre de délégués présente une tendance générale à l'augmentation en Lettonie. En alternative à la notification, le responsable du traitement peut, depuis 2007, désigner des délégués à la protection des données. Aucune lacune majeure n'a été observée concernant le travail des délégués à la protection des données. Jusqu'à fin 2011, 40 personnes avaient réussi l'examen de l'Inspection nationale des données et obtenu le certificat de délégué à la protection des données.

Concernant la sensibilisation du public, une recommandation a été émise quant à la protection des données des enfants. Cette recommandation a été largement utilisée par le personnel des écoles primaires et maternelles. L'Inspection nationale des données a organisé plusieurs séminaires destinés aux enseignants, aux directeurs d'écoles et autres membres du personnel administratif sur les questions liées à la protection des données personnelles, couvrant la protection des données des élèves et du personnel des écoles. Ces séminaires et leurs recommandations pratiques ont été jugés très utiles par le public ciblé.

Des activités de sensibilisation du public ont également été menées en coopération avec d'autres institutions publiques (par exemple CERT.LV) afin de promouvoir la compréhension des questions liées à la protection des données et de la vie privée. Cette coopération devait par ailleurs se poursuivre en 2012.

Organisation	Inspection nationale des données
Directeur	Signe Plūmiņa
Budget	266 907 LVL (environ 368 656,08 EUR)

Personnel	19 (personnel administratif compris)
Activités générales	
Décisions, avis, recommandations	1 recommandation. Aucunes statistiques disponibles sur les Décisions et Avis. Des Avis sont régulièrement émis quant aux projets de législation.
Notifications	650.
Examens préalables	Des statistiques seront disponibles à partir de 2012.
Demandes émanant des personnes concernées	
Plaintes émanant des personnes concernées	254
Conseils sollicités par le Parlement ou le gouvernement	Régulièrement, que ce soit sur la mise en œuvre d'actes juridiques spécifiques ou sur des problèmes liés à la protection des données.
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	290 enquêtes réalisées.
Activités de sanction	
Sanctions	Des avertissements et des amendes ont été prononcés.
Amendes	Pour un montant de 23 100 LVL (31 906,08 EUR). Les amendes ont été prononcées pour des actes illégaux et pour ne pas avoir fourni des informations à l'Inspection nationale des données.
DPD	
Chiffres relatifs aux DPD	40

B. Informations sur la jurisprudence

La situation économique du pays influe sur les plaintes reçues par l'Inspection nationale des données dans le domaine du traitement des données personnelles. Les plaintes portaient principalement sur les sujets suivants :

1. des informations fournies au fisc par des employeurs sur des employés sans relation de travail (de telle sorte que les personnes concernées ne pouvaient percevoir de prestations sociales de l'État en raison d'une relation de travail dont elles n'avaient pas connaissance).

2. le traitement de données personnelles dans le cadre d'un processus de recouvrement.

3. le traitement de données personnelles dans le cadre de la vidéosurveillance.

4. la publication illégale de données personnelles sur Internet.

LITUANIE

A. Résumé des activités et actualités

La loi modifiant et complétant la loi sur les Communications électroniques (Journal Officiel, 2004, n° 69-2382) (ci-après la LCE) est entrée en vigueur le 1er août 2011, mettant en œuvre au sein du droit lituanien les dispositions de la directive « Vie privée et communications électroniques ».

Le 4 mai 2011, le gouvernement de la République de Lituanie a adopté la Résolution n° 522 « sur la mise en œuvre de la Décision 2009/917/JAI du Conseil du 30 novembre 2009 sur l'emploi de l'informatique dans le domaine des douanes ». En vertu de l'Article 1.2 de cette Résolution, l'Inspection publique de protection des données (IPPD) a été désignée en tant qu'autorité responsable de la supervision indépendante des données saisies dans le système d'information des douanes.

Le 9 novembre 2011, le gouvernement de la République de Lituanie a adopté la Résolution n° 1324 « sur l'approbation de la procédure d'échange transfrontalier de données d'ADN, de données dactyloscopiques, de données sur l'immatriculation de véhicules et sur leurs propriétaires, et d'informations sur les événements transfrontaliers à grande échelle ou sur la prévention des crimes terroristes », en vertu de laquelle l'IPPD a été désignée responsable des contrôles de la légalité de la divulgation et de la réception des données personnelles.

Le 17 juin 2011, le directeur de l'IPPD a émis une ordonnance « sur l'approbation de la procédure de mise en œuvre, par les personnes concernées, via l'Inspection publique de protection des données, de leurs droits d'accès, de rectification, de suppression ou de blocage de leurs données personnelles », mettant en œuvre la loi sur la protection des données personnelles traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

Le 22 juillet 2011, le directeur de l'Inspection publique de protection des données de la République de Lituanie (ci-après IPPD) a émis une ordonnance « sur l'approbation de la procédure de notification en cas d'atteinte à la sécurité de données personnelles ». En vertu de cette ordonnance, la procédure et la forme que doit prendre la notification d'atteintes à la sécurité des données personnelles ont été approuvées, prodiguant des conseils sur la manière de notifier les violations de données. Plusieurs ateliers ont par ailleurs été organisés à l'attention des prestataires de services.

L'IPPD, le ministère de la Justice et le ministère des Transports et des Communications ont lancé une initiative sur la mise en œuvre pratique des exigences de la directive « Vie privée et communications électroniques » sur les cookies des sites web des institutions gouvernementales et des municipalités, et des discussions sur la manière de présenter des recommandations ont été préparées par le mandataire de l'IPPD.

La Journée européenne de la protection des données a été célébrée le 27 janvier 2011. Une conférence de presse et des activités ont été organisées au Seimas de la République de Lituanie sur le sujet de « la vie privée dans le cyberespace ». Le 10 février 2011, la Journée de la protection des données a été célébrée à l'Université de Vilnius. Cette journée avait pour objet d'améliorer la compréhension des menaces pesant sur la sécurité des données personnelles lors de leur traitement dans le cyberespace (réseaux sociaux, Google, crédits par Internet et autres canaux électroniques). Le groupe cible principal était celui des étudiants en universités et grandes écoles.

Le 19 mai 2011, l'IPPD et la société par actions Expozona ont organisé une conférence sur la « protection des données en Lituanie : évolutions, problèmes et perspectives ». Cet événement portant sur l'emploi des

technologies et la communication des données de registres était destiné aux sociétés, aux institutions et organisations, aux directeurs, aux avocats, aux professionnels responsables du traitement des données personnelles des employés et des clients.

Le 24novembre 2011, toujours avec la société par actions Expozona, l'IPPD a de nouveau organisé une conférence sur la « protection des données en Lituanie : innovations, évolutions et problèmes ». Cet événement portait sur les aspects juridiques de la protection des données personnelles : présenter des amendements de la loi sur la Protection juridique des données personnelles de la République de Lituanie, d'importantes décisions de justice, discuter des problèmes de juridiction, etc.

Organisation	
Président et/ou collège	Dr Algirdas Kunčinas
Budget	Alloué et exécuté : 1 881 millions de LTL (546 484 EUR)
Personnel	30
Activités générales	
Avis, recommandations	s. o.
Notifications	998
Examens préalables	257
Demandes émanant des personnes concernées	14
Plaintes émanant des personnes concernées	256
Conseils sollicités par le Parlement ou le gouvernement	s. o.
Autres renseignements relatifs aux activités générales	3 356 consultations ; 88 communiqués d'information au public ; 6 synthèses des résultats des enquêtes sur les plaintes et la jurisprudence ; 5 demandes liées au traitement des données dans le système central d'information Schengen ; 63 conclusions sur des documents de l'UE et du Conseil de l'Europe ; 82 réponses à des demandes de parties à la Convention (STE n° 108) ; 234 actes juridiques coordonnés et documents des responsables des données ; 6 actes juridiques préparés.
Activités d'inspection	
Contrôles	43 (légitimité du stockage de données relatives au trafic sur l'internet lors de prestations de services internet ; droits des personnes concernées, portée et légitimité du traitement des données dans les boutiques en ligne).

Activités de sanction	
Sanctions	L'IPPD a mis en place 24 protocoles pour des violations administratives.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Traitement des données personnelles d'un débiteur

L'IPPD a reçu une plainte alléguant qu'une agence de recouvrement ayant obtenu les données personnelles du plaignant de la part du créditeur initial dans le cadre d'un contrat de cession, avait illégalement transmis ces données personnelles au dossier consolidé du débiteur. L'IPPD s'est aperçue que le plaignant n'avait pas contesté la dette pour des raisons impérieuses et a conclu que les données personnelles du plaignant avaient été communiquées légalement au dossier consolidé du débiteur. Le plaignant a fait appel de cette décision de l'IPPD auprès du tribunal administratif du district de Vilnius, au motif que l'IPPD n'avait pas spécifié les raisons pour lesquelles sa contestation ne reposait pas sur des raisons impérieuses. Le tribunal administratif de Vilnius a infirmé la décision de l'IPPD et ordonné à l'IPPD de procéder à une nouvelle enquête. L'IPPD a fait appel de cette décision auprès de la Cour administrative suprême.

La Cour administrative suprême (ci-après la Cour) a estimé que la Loi sur la protection juridique des données personnelles de la République de Lituanie (ci-après la LPJDP) ne présente aucune définition de raisons impérieuses et que, par conséquent, aucune base ne permet de conclure qu'une personne ayant remis une fois en cause une dette soit tenue de continuer de manière régulière, faute de quoi, suite aux rappels écrits du responsable du traitement des données, ses données pourront être transférées au dossier consolidé du débiteur après 30 jours civils à compter du dernier rappel (Article 21, alinéa 2.3 de la LPJDP). Pour décider de la manière dont les termes « raisons impérieuses » devaient être compris, la Cour a tenu compte de plusieurs aspects, tels que le fait de savoir si la personne concernée avait raisonnablement remis en cause le responsable du traitement, en l'espèce le créditeur, quant à l'évaluation des preuves sur lesquelles s'appuie sa décision et, en l'absence d'accord, une partie ne peut prendre une décision contraignante pour l'autre partie. L'appel de l'IPPD a été rejeté, et la décision du tribunal administratif du district de Vilnius est restée inchangée.

LUXEMBOURG

A. Résumé des activités et actualités

Modifications de la législation

La loi du 28 juillet 2011 applique les dispositions de la Directive 2009/136/CE au droit luxembourgeois via une modification de la loi du 30 mai 2005 relative aux règles spécifiques applicables à la protection de la vie privée dans le secteur des communications électroniques. Elle prévoit une définition de la « violation de données » et de l'obligation de notification de la DPA en cas de toute violation, ainsi que des personnes concernées si ces dernières sont négativement affectées par ladite violation. Une évolution importante du droit luxembourgeois constitue le droit d'imposer une amende au responsable du traitement des données en cas de violations récurrentes des données. La loi modifie également certaines dispositions mineures de la loi de 2005 et de la loi modifiée du 2 août 2002.

Questions de fond

En 2011, la *Commission nationale* a dispensé au gouvernement luxembourgeois des conseils portant sur un large éventail de questions législatives, parmi lesquelles la plus importante fut le projet de loi mettant en œuvre une base de données nationale des élèves par le ministère de l'Éducation. La DPA luxembourgeoise a poursuivi sa collaboration avec les différents ministères et administrations publiques sur des projets ayant un impact sur la vie privée, tels que, par exemple, les dossiers médicaux électroniques, la réforme des dossiers criminels, l'introduction d'un permis de résidence biométrique et l'initiative des citoyens européens.

Actualités

La CNPD a conclu un contrat de partenariat stratégique avec le Centre interdisciplinaire pour la sécurité, la fiabilité et la confiance (SnT) de l'Université du Luxembourg. Le programme de recherche commun porte essentiellement sur trois domaines : les nouvelles initiatives législatives de l'Union européenne dans le domaine de la protection des données, les enjeux des nouvelles technologies tels que l'informatique en nuage et ses implications pour le Luxembourg, et le concept de vie privée dès la conception (« *privacy by design* »).

Principaux événements et activités de sensibilisation

La CNPD a célébré la Journée européenne de la protection des données en organisant la conférence « *No privacy online anymore?* » (Vers la fin de la vie privée sur Internet ?), avec le Dr Alexander Dix (Commissaire à la protection des données et à l'accès à l'information du Land de Berlin). Richard Allan, de la société Facebook, a également participé à cette conférence, qui a été suivie d'une table ronde avec des représentants politiques et de la protection de la jeunesse. Outre cet événement destiné au grand public, la CNPD a également participé à plusieurs séminaires et formations visant à sensibiliser un public plus spécialisé.

Organisation	Commission nationale pour la protection des données (CNPD)
Président et/ou collège	M. Gérard Lommel – Président M. Thierry Lallemang – Commissaire M. Pierre Weimerskich – Commissaire
Budget	1 494 000 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	492
Notifications	401
Examens préalables	429
Demandes émanant des personnes concernées	314
Plaintes émanant des personnes concernées	115
Conseils sollicités par le Parlement ou le gouvernement	14
Réunions et consultations (secteurs public/privé)	140
Conférences et réunions d'information	15
Cas de règles d'entreprise contraignantes où la DPA est l'autorité « chef de file »	2
Activités d'inspection	
Contrôles	17

Activités de sanction	
Sanctions	0
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	DPD désignés en 2011 : 10 Nombre total de DPD désignés (à la date du rapport) : 48

B. Informations sur la jurisprudence

Jurisprudence civile et pénale

Cour d'Appel du Luxembourg, 8e chambre du travail sur la proportionnalité et la légitimité de la surveillance d'un employé sur son lieu de travail, 3 mars 2011

Un employé suspecté de pratiques de concurrence déloyale a été renvoyé en raison d'un document trouvé sur l'ordinateur d'un autre employé constituant la preuve que le premier prévoyait de créer une société concurrente. Ce document avait été envoyé depuis la messagerie électronique privée de l'employé vers celle de son collègue, mais avait été sauvegardé sur la machine de l'employeur. La Cour d'Appel a jugé que l'interception et la transmission de ce document ne constituaient pas une violation du principe de confidentialité de la correspondance. La Cour a tenu compte du fait que ledit courriel était adressé à plusieurs employés et qu'aucune mention n'était faite de son caractère privé ou confidentiel.

MALTE

A. Résumé des activités et actualités

Pendant la période examinée, notre Bureau a pris des mesures législatives afin d'introduire des amendements à la législation subsidiaire 440.01 qui réglemente le traitement des données personnelles dans le secteur des communications électroniques. Ces amendements étaient requis en vue de la transposition des dispositions de la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 amendant, notamment, la Directive 2002/58/CE relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques.

Les amendements ont été introduits en vertu de la notification juridique 239 de 2011, publiée au Journal Officiel du 24 juin 2011. Le règlement devait entrer en vigueur en 2012 et être par ailleurs complété par un ensemble de lignes directrices destinées à fournir aux responsables du traitement de données les informations nécessaires sur la mise en œuvre des nouvelles exigences relatives, notamment, aux notifications de violations et à l'emploi de cookies.

Des responsables du traitement des données ont déposé des demandes d'examen préalable concernant l'introduction de systèmes biométriques et l'installation de systèmes de vidéosurveillance sur le lieu de travail, ainsi que dans d'autres domaines où les opérations de traitement entraînaient des risques particuliers d'interférence avec les droits et libertés des personnes concernées au regard de l'Article 34 de la Loi sur la protection des données. Outre une demande du ministère des Affaires étrangères concernant le traitement des données biométriques dans le cadre du nouveau VIS, notre Bureau a évalué les implications de la protection des données avant d'autoriser un traitement similaire établi par les Règlements (CE) 767/2008 et (CE) 810/2009. Cette évaluation a eu lieu lors d'une réunion avec les parties prenantes et de deux visites sur place visant à examiner les fonctionnalités du système et la manière dont la partie nationale sera mise en œuvre.

En novembre, notre Bureau a réalisé deux visites d'inspection sur place en Russie et en Égypte aux Consulats maltais de Moscou et du Caire. Ces deux visites avaient pour objet d'évaluer le traitement des données personnelles entrepris par ces deux missions dans le cadre du processus d'émission de visas pour les citoyens de pays tiers. Elles avaient également pour objectif l'examen de certaines procédures établies à la lumière des exigences découlant des dispositions de la Loi sur la protection des données et autres instruments juridiques. Une séance de formation et de sensibilisation à la protection des données a été organisée pour les membres du personnel afin de les sensibiliser au droit à la vie privée dont jouissent les citoyens en vertu de la Loi, aux règlements VIS correspondants et à la Convention de Schengen concernant l'émission de visas.

Le 28 janvier, le Bureau du Commissaire à la protection des données et de l'information a rejoint d'autres autorités de protection des données du monde entier afin de célébrer la Journée de la protection des données. Pour marquer cette journée sur le plan local, le Bureau a distribué de la documentation informative et des articles de papeterie aux élèves de toutes les écoles publiques et privées. Notre Bureau a toujours pensé que, pour qu'une évolution culturelle ait effectivement lieu, un investissement continu était nécessaire dans l'éducation et la sensibilisation des plus jeunes.

Avec la disponibilité croissante des applications de réseaux sociaux et l'effacement des limites de la vie privée qui en découle, le Bureau, par cette activité, a essayé de délivrer un message soulignant les risques pour la vie privée que rencontrent les personnes concernées lorsqu'elles naviguent sur Internet. Cette année, le message portait sur l'utilisation d'Internet et sur l'importance d'avoir conscience des risques potentiels pour la vie privée auxquels les données personnelles peuvent être exposées lorsqu'elles sont

mises à disposition sur Internet. Le Bureau a souligné que l'identité des personnes concernées était une information de valeur qu'il était par conséquent impératif de protéger.

D'autres activités de sensibilisation ont été menées par notre Bureau au cours de l'année, dont des présentations au profit de divers responsables du traitement des données de différents secteurs de la société maltaise, la participation à des programmes télé et radio locaux avec intervention téléphonique des auditeurs, et la mise à jour régulière du portail du Bureau avec les évolutions dans le domaine de la protection des données. Le Bureau est convaincu que faire passer ce message par les médias représente une manière potentiellement efficace de sensibiliser un large public.

Organisation	
Président et/ou collège	Commissaire à la protection des données et de l'information
Budget	Environ 300 000 EUR
Personnel	Commissaire – 1 Personnel spécialisé – 3 Assistance technique – 2 Assistance administrative – 3
Activités générales	
Décisions, avis, recommandations	38 décisions ont été émises dans le cadre de plaintes reçues par le Commissaire 26 avis/recommandations ont été émis relativement à des avis publiés sous forme d'articles de journaux ciblant à la fois le grand public et les responsables du traitement des données, et d'autres avis/recommandations ont été adressés aux responsables du traitement sur des sujets spécifiques.
Notifications	154 nouvelles notifications ont été reçues
Examens préalables	5 demandes d'examens préalables ont été reçues
Demandes émanant des personnes concernées	Demandes reçues par téléphone – 7 appels quotidiens en moyenne Demandes reçues par courriel – 135
Plaintes émanant des personnes concernées	70 plaintes
Conseils sollicités par le Parlement ou le gouvernement	s. o.
Autres renseignements relatifs aux activités générales	s. o.

Activités d'inspection	
Contrôles, enquêtes	17 contrôles ont été réalisés dans le cadre d'enquêtes sur des plaintes reçues de la part des personnes concernées, des consulats maltais de l'étranger et des autorités policières dans le cadre d'exercices coordonnés par l'ACC.
Activités de sanction	
Sanctions	Des poursuites judiciaires ont été initiées à l'encontre d'un responsable du traitement des données n'ayant pas respecté l'ordonnance rendue par le Commissaire dans sa décision.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	15 représentants des données personnelles ont été désignés.

B. Informations sur la jurisprudence

Aucune jurisprudence n'est disponible pour la période examinée.

PAYS-BAS

A. Résumé des activités et actualités

La DPA néerlandaise supervise le respect de la législation sur la protection des données personnelles. En général, la DPA néerlandaise se focalise sur l'application stratégique de manière à obtenir un haut niveau de conformité globale. Si nécessaire, des sanctions sont appliquées.

Les priorités sont déterminées sur la base d'une évaluation continue des risques pour laquelle nous utilisons les signaux que nous recevons de la part de différentes sources de la société via divers canaux tels que des appels téléphoniques, des courriels et des articles de presse, etc. En 2011, un nouveau système d'enregistrement des signaux a été introduit, qui nous permet d'enregistrer les signaux par secteur. L'évaluation des risques tient compte de la gravité de l'infraction présumée, du nombre de personnes affectées, de la clarté de l'indication de la violation et de la faisabilité légale d'une mesure d'application, ainsi que des effets de l'emploi de nouvelles technologies à grande échelle. En 2011, la DPA néerlandaise s'est essentiellement focalisée sur les éléments suivants : le consentement, la sécurité des données, la limitation de la finalité et les périodes de conservation des données.

L'une des nombreuses enquêtes menées par la DPA néerlandaise en 2011 portait sur la criminalité juvénile dans les *Veiligheidshuizen,*[17] où les autorités policières et les institutions sociales travaillent ensemble à la prévention et à la répression des comportements criminels. Le résultat de cette enquête fut que les données personnelles des enfants de moins de 12 ans étaient collectées et échangées par l'ensemble des parties concernées lors de réunions régulières. Les *Veiligheidshuizen* n'ont toutefois pas pu démontrer sur quels critères les données personnelles étaient échangées. Par ailleurs, l'échange des données ne correspondait pas à l'objet des réunions régulières et était dès lors contraire à la loi. Lors de la phase de mise en œuvre de l'enquête de la DPA néerlandaise, les *Veiligheidshuizen* ont changé leurs politiques et rédigé des critères pour l'échange de données personnelles dans le cadre de leurs réunions.

La DPA néerlandaise a également mené des enquêtes sur, notamment, les opérations de traitement des données suivantes :

- L'échange de données personnelles d'étudiants (par exemple : le pays de naissance et l'origine ethnique).

- L'association de données personnelles sans le consentement du Service d'information et de recherche sociale.

- L'échange de données personnelles par le fisc néerlandais avec environ 900 bureaux d'aide et d'information sans vérification de l'autorisation de l'institution requérante.

- La collecte de données Wi-Fi par les voitures de Google Street View.

- La collecte de données de géolocalisation par TomTom auprès de ses clients.

Certaines situations ont nécessité que la DPA prenne des mesures d'application, comme dans le quartier de Charlois, à Rotterdam, qui collectait des informations sur les origines ethniques d'enfants de groupes minoritaires. La DPA néerlandaise a imposé à Charlois une amende avec sursis afin de mettre un terme au traitement de ce type de données personnelles. Charlois a fait appel de cette amende devant la Cour. Un

17 Les Veiligheidshuizen sont des plateformes où la police, le ministère public et le conseil de la protection des enfants travaillent ensemble à la prévention du récidivisme chez les jeunes délinquants.

autre exemple est la promesse de la société des chemins de fer néerlandais (NS) et de Trans Link Systems (l'émetteur des cartes à puce des transports publics) de réduire la période de conservation des données sur les déplacements des étudiants. Cette promesse devait avoir été mise en application au plus tard en mai 2012. Lorsque le délai de mise en œuvre est passé sans que la période de conservation des données n'ait été réduite, la DPA néerlandaise a imposé une amende à NS en juillet 2012.

Outre les enquêtes menées, la DPA néerlandaise prodigue également des conseils au gouvernement sur des projets de lois avant qu'ils ne soient adressés au Parlement. Suite aux conseils de la DPA néerlandaise, les propositions sont (parfois) amendées afin d'éviter des violations de la vie privée. Le ministère de la Sécurité et de la Justice, a notamment demandé à la DPA néerlandaise des conseils sur l'introduction d'un système en vertu duquel les numéros de téléphone des avocats ne pourraient pas être reconnus et, par conséquent, leurs conversations ne pourraient pas être écoutées. La DPA néerlandaise a salué l'introduction d'un tel système visant à garantir la confidentialité des conversations entre un avocat et ses clients, mais a conseillé d'inclure des clarifications et des spécifications au projet.

Organisation	Autorité néerlandaise de protection des données
Président et/ou collège	Jacob Kohnstamm, Président Madeleine McLaggan, Membre du Collège ; Vice-présidente Jannette Beuving, Membre du Collège (jusqu'au 1er septembre 2011) Wilbert Tomesen, Membre du Collège (à compter du 1er décembre 2011)
Budget	Alloué : 7 631 000 EUR Exécuté : 7 731 000 EUR
Personnel	80,5 ETP (83 employés)
Activités générales	
Décisions, avis, recommandations	298 (enquêtes, lignes directrices, code de conduite, examens préalables, sanctions et conseils dans le cadre du processus législatif)
Notifications	3 939
Examens préalables	170
Signaux[18] émanant des personnes concernées	Problèmes signalés à la DPA via son site web : s. o. Courriels entrants : s. o. Appels téléphoniques entrants : s. o.

18 Depuis avril 2011, tous les contacts des citoyens sont enregistrés sous forme de signaux. Ces signaux servent à classer nos interventions par ordre de priorité. Ces signaux ne sont par conséquent pas enregistrés en fonction de la manière dont ils sont reçus, mais du secteur dont ils dépendent.

	Sur l'ensemble de ces signaux, les secteurs les plus concernés ont été ceux du commerce et des services (1 871), de l'administration publique (954) et de la santé (686)
Signaux émanant des personnes concernées –total–	Nombre de signaux qualifiés et traités : 5 790
Conseils sollicités par le Parlement ou le gouvernement	35
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	85
Activités de sanction	
Sanctions	6
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	264 DPD signalés à la DPA (au 8 août 2012)

B : Informations sur la jurisprudence

Intérêt légitime, proportionnalité et subsidiarité

Le Bureau Krediet Registratie (Bureau d'enregistrement des crédits, BKR) enregistre les prêts à la consommation. Le BKR maintient les bases de données personnelles des consommateurs qui contiennent, notamment, leur nom, leur adresse et l'étendue de leurs dettes et crédits. Ces bases de données du BKR sont accessibles à l'ensemble de ses membres.

Dans le cas particulier qui nous occupe, M. X était en retard sur le remboursement de son emprunt auprès de la banque Santander. Même après avoir satisfait à ses obligations, le BKR a laissé son statut de débiteur à M. X. M. X a demandé au BKR de retirer ses données personnelles, ce qui lui a été refusé.

M. X s'est rendu au tribunal afin de faire appliquer son droit au retrait de ses données personnelles du système du BKR. Dans ce cas, la Cour Suprême des Pays-Bas a statué que le traitement de données personnelles n'était autorisé que s'il était défini sur un plan juridique, déterminé de manière explicite et s'il présentait un intérêt légitime. La Cour Suprême a en outre ajouté à ces critères que lorsqu'il est légalement autorisé de traiter des données personnelles dans le cadre d'un intérêt légitime, la nécessité de traiter ces données pour parvenir à cet intérêt légitime devrait être jugée au cas par cas. Dans ce cas, la Cour Suprême a statué que l'intérêt légitime de signaler M. X en tant que débiteur n'existait plus

maintenant qu'il avait remboursé son emprunt, et que les données personnelles de M. X devaient par conséquent être retirées de la base de données.

La Cour Suprême renvoie également à l'Article 8 de la Convention européenne des droits de l'homme. Dans ce contexte, le traitement de données n'est autorisé que lorsqu'il ne porte pas un préjudice disproportionné aux intérêts de la personne concernée au regard de l'intérêt poursuivi (principe de proportionnalité), et lorsque la finalité ne peut être atteinte d'une autre manière (principe de subsidiarité). Dans ce cas, les intérêts de la personne concernée avaient subi un préjudice disproportionné.

POLOGNE

A. Résumé des activités et actualités

L'événement le plus important en lien avec les activités de l'Inspecteur général pour la protection des données personnelles (GIODO) a été l'entrée en vigueur, le 7 mars 2011 (après près de trois ans de travail intensif), de la Loi sur la protection des données à caractère personnel amendée. Les dispositions entrées en vigueur le 7 mars ont investi le GIODO de pouvoirs dans le cadre de l'exécution administrative d'obligations non pécuniaires (Article 12, alinéa 3), le droit de s'adresser aux autorités d'État, aux autorités territoriales autonomes, aux unités organisationnelles d'État et municipales, ainsi qu'aux autres unités organisationnelles et personnes physiques et morales afin d'assurer l'efficacité de la protection des données personnelles, ainsi que le droit de demander aux autorités compétentes de prendre des initiatives législatives et d'émettre ou d'amender des actes juridiques dans des affaires relatives à la protection des données personnelles. L'entité recevant un avis formel ou une demande du GIODO devra y apporter une réponse par écrit dans un délai de 30 jours à compter de sa réception. En outre, empêcher ou entraver l'exécution des activités d'inspection des inspecteurs du GIODO sera passible d'une amende et d'une restriction ou privation de liberté de deux ans maximum.

En 2011, le GIODO a continué de participer au processus législatif du projet de loi sur l'échange d'informations avec les autorités policières des États membres de l'Union européenne, un acte juridique important pour la protection des données, et émis un avis sur ce projet. La Loi a été adoptée le 16 septembre 2011 et est entrée en vigueur le 1er janvier 2012. Ce qui est important dans la Loi sur l'échange d'informations avec les autorités policières des États membres de l'Union européenne, c'est l'introduction de changements de la Loi sur la protection des données à caractère personnel. À savoir, à l'Article 43, alinéa 1 de la Loi sur la protection des données à caractère personnel, un point 2c a été ajouté afin de prévoir une exemption de l'obligation de notifier les systèmes d'enregistrement et d'archivage des données pour les responsables de ces données traitées par des autorités compétentes sur la base des dispositions sur l'échange d'informations avec les organes de poursuite des États membres de l'Union européenne. À l'Article 26(a), alinéa 1, concernant l'émission d'une décision basée sur le traitement automatique de données personnelles dans le cas individuel d'une personne concernée, une nouvelle condition prérequise légitimant cette action a été ajoutée : l'existence d'une disposition légale qui prévoit des mesures de sauvegarde des intérêts légitimes de la personne concernée. L'Article 47, alinéa 1 modifié, établit que le transfert de données personnelles vers un pays tiers ne peut avoir lieu que si le pays de destination assure un niveau adéquat de protection des données personnelles sur son territoire. D'après l'alinéa 1(a) ajouté à cet Article, l'adéquation du niveau de protection des données personnelles visée à l'alinéa 1 sera évaluée en tenant compte de toutes les circonstances de l'opération de transfert de données et, notamment, de la nature des données, de l'objet et de la durée des opérations de traitement des données proposées, du pays d'origine et du pays de destination finale des données, ainsi que des dispositions légales en vigueur dans un pays tiers donné et des mesures de sécurité et règles professionnelles applicables dans ce pays. L'alinéa 2 de l'Article 47 a été clarifié et précise que l'alinéa 1 ne sera pas applicable si le transfert de données personnelles résulte d'une obligation imposée au responsable du traitement des données par des dispositions légales ou par les dispositions de tout accord international ratifié garantissant un niveau adéquat de protection des données.

Parmi les autres événements importants, on peut citer la désignation d'une nouvelle unité organisationnelle du Bureau du GIODO (l'équipe d'exécution administrative) et la spécification des sièges et de la juridiction territoriale des antennes locales du Bureau (en vertu du Règlement du Président de la République polonaise du 10 octobre 2011 sur l'octroi de statuts au Bureau de l'Inspecteur général pour la protection des données personnelles).

Organisation	Bureau de l'Inspecteur général pour la protection des données personnelles (GIODO)
Président et/ou collège	Dr. Wojciech Rafał Wiewiórowski, Inspecteur général pour la protection des données personnelles
Budget	14 700 000 PLN
Personnel	131
Activités générales	
Décisions, avis, recommandations	1 110 décisions émises.
Notifications	11 845 systèmes d'archivage de données personnelles enregistrés.
Examens préalables	Grâce aux procédures d'enregistrement (contrôle préalable), 2 298 systèmes d'archivage de données personnelles contenant des données sensibles ont été inscrits dans le registre des systèmes d'archivage de données personnelles ; le traitement de fichiers de données personnelles contenant des données sensibles ne peut commencer qu'une fois la procédure d'enregistrement terminée.
Demandes émanant des personnes concernées	3 935 questions juridiques ont été envoyées par courriel ou par courrier postal (non seulement par des personnes concernées, mais également par des personnes intéressées par les questions liées au traitement des données personnelles). 2 796 avis et recommandations ont été émis au total. 4 118 explications ont également été fournies grâce à la ligne d'information du GIODO.
Plaintes émanant des personnes concernées	Ces plaintes concernaient des atteintes à la protection des données personnelles, notamment dans les domaines suivants : • Administration publique (80 plaintes); • Tribunaux, bureau du procureur, police, huissiers (32 plaintes); • Banques et autres institutions financières (94 plaintes); • Internet (78 plaintes); • Marketing (18 plaintes); • Questions liées au logement (69 plaintes); • Assurances sociales, de biens et individuelles (13 plaintes); • Système d'information Schengen (4 plaintes);

	• Télécommunications (48 plaintes); • Emploi (35 plaintes); • Autres (178 plaintes).
Conseils sollicités par le Parlement ou le gouvernement	Des avis ont été exprimés sur 592 projets de lois soumis à l'analyse du GIODO.
Autres renseignements relatifs aux activités générales	55 – nombre de formations assurées par le GIODO sur les dispositions relatives à la protection des données personnelles, surtout au bénéfice d'institutions publiques.
Activités d'inspection	
Contrôles, enquêtes	199 contrôles, dont 104 contrôles sectoriels et 95 contrôles dans le cadre de plaintes déposées à l'encontre de traiteurs de données personnelles et de systèmes d'archivage de données personnelles notifiés à l'enregistrement et suite à l'obtention d'informations par le GIODO de la part d'entités externes. Les contrôles sectoriels ont été réalisés dans les secteurs suivants : • 21 contrôles dans l'administration publique; • 10 contrôles sur le traitement de données personnelles dans le SIS et le VIS dans le Système d'information national; • 15 contrôles au sein de sociétés de services de conseils fiscaux et financiers; • 5 contrôles au sein d'entités de services de santé; • 17 contrôles au sein d'agences pour l'emploi; • 14 contrôles au sein d'entités organisant des événements de masse dans des stades; • 10 contrôles auprès d'opérateurs de réseaux publics de télécommunications et de prestataires de services de télécommunications publiquement disponibles; • 12 contrôles au sein d'écoles d'infirmières. Suite aux contrôles réalisés, 66 procédures administratives ont été instituées pour que le GIODO émette des décisions administratives ordonnant la restauration d'une situation légale appropriée.
Activités de sanction	
Sanctions	En 2011, le GIODO a adressé 10 notifications de suspicion d'infractions pénales, dont 4 concernaient la suspicion d'infractions pénales commises par le biais d'Internet. Le nombre de notifications

	affiche une baisse de plus de 50 % par rapport à 2010 (23 notifications en 2010).
Amendes	
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

En 2011, le jugement de la Cour administrative suprême du 19 mai 2011 a été crucial du point de vue du traitement des données à caractère personnel dans le secteur de l'activité Internet. Le jugement établit que dans chaque cas où le numéro IP permet l'identification indirecte d'une personne physique donnée, il devrait être considéré comme étant une donnée personnelle au sens de l'Article 6, alinéas 1 et 2, de la Loi sur la protection des données à caractère personnel. Une autre interprétation serait incohérente avec les dispositions des Articles 30 et 47 de la Constitution de la République de Pologne. La Cour a établi sans ambiguïté que l'adresse IP (ou adresse de protocole Internet) constituait une donnée personnelle.

Dans son jugement du 24 octobre 2011, le tribunal administratif de Voivodeship à Varsovie a partagé le point de vue du GIODO concernant l'effacement des données personnelles du Système d'information national de la police (KSIP). Le tribunal a statué que les dispositions de la Loi sur la protection des données à caractère personnel et non celles de la Loi sur la police, qui habilite celle-ci à créer le KSIP, devront être appliquées pour l'effacement des données personnelles stockées dans le KSIP.

C. Autres informations importantes

Un élément important des activités du GIODO est l'émission d'avis sur les projets de lois. Parmi les projets de lois soumis au GIODO en 2011, les projets de lois sur les bases de données TIC revêtent une importance particulière. La DPA polonaise a accordé une attention particulière aux différents projets de lois régulant le fonctionnement de bases de données telles que les systèmes d'information de l'éducation (SIO), les systèmes d'information de la santé et le Registre central des entités – le Registre national des contribuables (CRP KEP). Par ailleurs, en connexion avec l'organisation de l'UEFA EURO 2012, à l'exception des bases de données TIC susmentionnées, le GIODO a porté une attention spéciale au projet de loi portant modification de la Loi sur la sécurité des grands événements et à certaines autres lois. Le GIODO s'est également concentré sur la poursuite du processus législatif concernant le projet de loi sur l'échange d'informations parmi les États membres de l'UE ainsi que sur les lignes directrices du projet de loi sur la réduction des obligations d'information et la réduction du fardeau administratif des citoyens et des entrepreneurs. Il convient également d'indiquer que le GIODO a exprimé son point de vue sur l'amendement proposé de la Loi sur la protection des données à caractère personnel. Outre les projets de lois, dont ceux qui sont mentionnés ci-dessus sont les exemples les plus importants, le GIODO a émis une série d'avis sur des projets de règlements relatifs aux problèmes de traitement des données personnelles communément reconnus.

Pendant la période de compte rendu, le nombre de systèmes d'archivage de données personnelles enregistrés par rapport aux années précédentes (en 2009 : 6 465, en 2010 : 9 921, en 2011 : 11 845) a continué d'augmenter. Cette augmentation a été rendue possible, notamment, par le fait que les déclarations ne contenaient pas autant d'erreurs que les années précédentes. Ce résultat a sans aucun doute été influencé par les activités législatives, éducatives, organisationnelles et techniques entreprises

par le GIODO en 2011 et les années précédentes, qui ont entraîné une baisse significative du nombre de décisions de refus d'enregistrements (en 2010 : 453, en 2011 : 105), tandis que le nombre de dossiers enregistrés augmentait.

À l'occasion de la Journée européenne de la protection des données, le 31 janvier 2011, l'Inspecteur général a organisé la traditionnelle journée portes ouvertes pour l'ensemble des citoyens au siège de son Bureau, ainsi qu'une conférence sur la conservation des données dans un État démocratique. En outre, l'habituelle Journée de la protection des données a été célébrée à Bruxelles.

Le 21 septembre 2011, l'un des événements les plus importants, la Conférence internationale sur la protection des données, a été organisé dans le cadre de la Présidence polonaise du Conseil de l'UE par le ministère de l'Intérieur et de l'administration polonais et l'Inspecteur général pour la protection des données personnelles à Varsovie. Les partenaires de la Conférence étaient le Commissaire parlementaire hongrois à la protection des données et la liberté de l'information, le ministère de l'Administration publique et de la Justice de Hongrie, le Conseil de l'Europe, l'Académie de droit européen et le ministère de la Justice espagnol.

Le 15 juin 2011, l'atelier pour les autorités de la protection des données des États membres de l'UE, axé autour de la mise en pratique des BCR et du partage d'expérience des DPA, a été organisé par l'Inspecteur général pour la protection des données personnelles en son siège et en coopération avec l'autorité française de protection des données (la CNIL). Cet atelier avait pour objet l'échange d'expérience et de connaissances sur l'utilisation pratique des BCR. Parmi les questions abordées par l'atelier figurait, notamment, la méthodologie d'analyse des applications des BCR.

Les 4 et 5 octobre 2011, le 23e atelier de traitement des dossiers a été organisé par le GIODO à Varsovie. Cet événement a vu la participation des représentants des DPA opérant tant au niveau national que régional, et de représentants du Contrôleur européen de la protection des données. Cet atelier avait pour but l'échange pratique d'expériences entre employés de DPA particulières chargés du traitement des dossiers et de l'exécution des enquêtes. Lors des séances plénières et des séances en groupes, les sujets suivants, notamment, ont été abordés : la gestion des cas transfrontaliers, la protection des données personnelles en connexion avec l'activité des sites web des réseaux sociaux et autres services en ligne, la méthodologie d'audit/d'enquête et la vie privée sur le lieu de travail.

En 2011, le GIODO a continué de publier des brochures d'information dans la série des ABC de protection des données personnelles et publié les guides suivants :

- Guide sur la protection des données personnelles pendant les campagnes électorales.

- Guide sur la protection des données personnelles au sein de l'Église orthodoxe, une déclaration conjointe du chef polonais de l'Église orthodoxe, le métropolite Sawa, et du GIODO. JUST/2013/RDAT/FW/0195 - Translation of 15th Article 29 - Working Party Annual Report.

- Guide intitulé « Sélection de questions sur la protection des données ». Un manuel destiné aux entrepreneurs a été publié dans le cadre du projet de partenariat « Sensibilisation aux questions de protection des données parmi les entrepreneurs opérant au sein de l'UE » et mis en pratique conjointement par le Bureau de l'Inspecteur général pour la protection des données personnelles, le Bureau tchèque pour la protection des données personnelles et le Commissaire parlementaire hongrois à la protection des données et la liberté de l'information (en polonais, anglais, tchèque et hongrois).

PORTUGAL

A. Résumé des activités et actualités

L'année 2011 a été marquée par une augmentation des activités de la DPA, reflétée par un nombre record de procédures.

L'un des aspects les plus importants qu'il convient de souligner est le lancement d'un système de notification électronique qui couvre l'ensemble des types de notifications dans le cadre d'un processus continu de dématérialisation permettant à la DPA d'accélérer de manière significative ses procédures internes et d'améliorer ses temps de réponse tout en accélérant et en facilitant le respect, par les responsables du traitement des données, de leurs obligations de notification.

Il convient par ailleurs de souligner, sur le plan institutionnel, la bonne coopération développée avec les autres régulateurs nationaux dans les discussions sur les sujets convergents, ou avec certains départements gouvernementaux, dans le suivi étroit des nouveaux projets ayant des implications dans le domaine de la protection des données et à des fins de conseils dans le cadre des discussions sur le plan européen.

La DPA portugaise a poursuivi ses activités de sensibilisation à la protection des données en promouvant plusieurs initiatives telles que le colloque organisé avec l'Association du marketing direct sur la protection des données et le marketing, ou les activités pour enfants du Projet DADUS, avec la participation à 20 séances scolaires auprès de 1 500 élèves, et la promotion de la seconde édition du concours « Un slogan pour la vie privée ».

Concernant les activités d'inspection, la DPA a augmenté le nombre de contrôles sur place et réalisé un audit auprès des autorités policières et des opérateurs de télécommunications.

Organisation	
Président et/ou collège	Corps collégial composé de 7 membres : Filipa Calvão (Président), Ana Roque, Carlos Campos Lobo, Helena Delgado António, Luís Barroso, Luís Paiva de Andrade, Vasco Almeida
Budget	Budget alloué : 3 326 388,13 EUR Budget d'État : 1 308 280,00 EUR Recettes propres à la DPA : 2 018 108,13 EUR Budget exécuté : 1 719 550,60 EUR
Personnel	23 (Secrétaire général : 1 ; Service des relations internationales et de la communication : 1 ; Service juridique : 9 ; Service des contrôles : 3 ; Services de première ligne : 2 ; Services administratifs et financiers : 7).

Activités générales	
Décisions, avis, recommandations	14 913 décisions contraignantes (dont 13 307 autorisations de traitement des données, 75 avis sur des projets de lois, le reste concernant des procédures d'infraction, des plaintes, des demandes d'accès aux données par des tiers, le droit d'accès prévu par la convention de Schengen, etc.)
Notifications	16 141
Examens préalables	14 852
Demandes émanant des personnes concernées	Chiffres non disponibles.
Plaintes émanant des personnes concernées	489 (224 liées aux systèmes de vidéosurveillance et 86 au traitement des données dans le contexte de l'emploi).
Conseils sollicités par le Parlement ou le gouvernement	72 avis préalables sur un projet de loi contenant des dispositions sur la protection des données
Autres renseignements relatifs aux activités générales	18 023 nouvelles procédures (notifications, plaintes, avis, infractions, accès par des tiers) ; 181 demandes concernant l'exercice du droit d'accès et de suppression du Système d'information Schengen (accès indirect par le biais de la DPA) ; 303 demandes d'avis de la part d'opérateurs de télécommunications concernant la levée de la confidentialité de l'appelant dans les cas d'appels dérangeants.
Activités d'inspection	
Contrôles, enquêtes	984 enquêtes démarrées (procédures d'infraction), dont 249 contrôles sur place exécutés
Activités de sanction	
Sanctions	197 amendes appliquées par la DPA
Amendes	± 333 000 EUR imposés par la DPA
DPD	
Chiffres relatifs aux DPD	s. o.

B : Informations sur la jurisprudence

Aucune jurisprudence pertinente pour ce rapport.

C : Autres informations importantes

www.cnpd.pt

RÉPUBLIQUE TCHÈQUE

A. Résumé des activités et actualités

L'activité de contrôle était en partie basée sur le plan d'inspection de la DPA, et en partie initiée par les plaintes de personnes concernées. Un compte rendu des affaires les plus représentatives ou les plus intéressantes est donné ci-dessous. Globalement, le plan d'inspection devait porter sur les systèmes d'information publics (tels que les bases de données qui ont proliféré ces dernières années), les systèmes d'information opérés par des entités privées (cartes de clients et cartes de fidélité, par exemple) et les opérations de traitement des données à des fins de prévention du crime et de lutte contre le terrorisme. Les plaintes déposées par des citoyens concernaient pour la plupart la vidéosurveillance, la publication d'informations personnelles en ligne et le traitement de données par des institutions financières ou des prestataires de services électroniques.

Pendant l'été, le Bureau a réussi à compléter un projet international (conjointement avec les DPA hongroise et polonaise) visant à « sensibiliser les entrepreneurs en activité au sein de l'UE aux questions liées à la protection des données » (*Raising awareness of data protection issues among the entrepreneurs operating in the EU*), financé par le programme de partenariat Leonardo da Vinci sous le numéro CZ/09/LLP-PS/P/LdV/061. Le projet portait sur le respect de la vie privée au travail et sur la protection des données des employés du point de vue de l'employeur. Le principal résultat fut un manuel exhaustif et une série d'activités de diffusion.

Deux membres du personnel ont travaillé en plusieurs occasions en tant qu'experts temporaires à Skopje/FYROM dans le cadre du projet d'assistance technique « Soutien à la Direction de protection des données à caractère personnel » (*Support to the Directorate for Personal Data Protection*, EuropeAid/128570/S/CER/FYR).

Organisation	Bureau de la protection des données personnelles
Président et/ou collège	M. Igor Němec (Président du Bureau)
Budget	262 175 040 CZK (10 487 001 EUR, au taux de change de 1 EUR = 25 CZK) – dont 3 073 800 EUR reçus des fonds structurels de l'UE, notamment pour un projet portant sur la création d'un registre public centralisé.
Personnel	99
Activités générales	
Décisions, avis, recommandations	3 avis (tous liés à des opérations de traitement dans le secteur privé)
Notifications	4 421 notifications (dont 3 856 enregistrées, 1 002 toujours en cours ou suspendues)
Examens préalables	82

Demandes émanant des personnes concernées	2 294 (dont 110 de l'étranger)
Plaintes émanant des personnes concernées	1 119 (plus 4 613 autres sur les spams)
Conseils sollicités par le Parlement ou le gouvernement	Aucune demande de ce type en 2011
Autres renseignements relatifs aux activités générales	23 demandes relevant de la Loi sur le libre accès aux informations. 75 projets de loi et 91 règlements d'application commentés dans le cadre des procédures de commentaires interministériels Autorisations de transferts internationaux : 9 demandes dont 3 autorisées et 6 suspendues pour des raisons procédurales
Activités d'inspection	
Contrôles, enquêtes	179 (dont 144 accomplis) + 157 enquêtes concernant des spams (dont 137 accomplies)
Activités de sanction	
Sanctions	env. 70 sanctions Note explicative : Par « sanction », on entend toute mesure de recours non financière imposée à un responsable du traitement. Nous avons souvent imposé un certain nombre de sanctions différentes (mesures de recours) dans le cadre d'une seule enquête, toutefois, aux fins des présentes informations, l'ensemble des sanctions relevant d'une enquête particulière ne seront comptées qu'une fois. La moyenne pour une action est d'environ 2,7.
Amendes	env. 105 amendes
DPD	
Chiffres relatifs aux DPD	Non applicable en République tchèque.

B. Informations sur la jurisprudence

En 2011, la République tchèque a organisé un recensement (dans le cadre de l'action mondiale). L'un des inspecteurs du Bureau a mené une enquête auprès de l'Office tchèque des statistiques. Il est intervenu dans un certain nombre de plaintes déposées par des citoyens se plaignant de la méthode du recensement, ainsi que de la conservation aux Archives Nationales de formulaires rendus anonymes (et de la conservation des résultats du recensement à l'Office tchèque des statistiques). L'enquête a débuté mi-2011 et n'avait pas été conclue à la fin de l'année de référence.

Le Bureau a **enquêté sur la version en ligne du registre des sociétés,** qui faisait partie du système d'administration en ligne. Les données personnelles sont traitées via ce portail (opéré par le ministère de la Justice), ce qui augmente le risque d'utilisation abusive potentielle compte tenu de l'environnement en ligne. L'inspecteur a souligné que, pour chaque opération de traitement des données, il doit y avoir un responsable du traitement désigné, portant la responsabilité de la conformité avec la loi. En outre, l'inspecteur a déclaré que la portée des données (ou documents) collectées était prescrite par la Directive 2009/101/CE et que la publication d'autres documents devait être envisagée avec circonspection vis-à-vis du principe de limitation de la finalité. De la même manière, la période de conservation des ces données personnelles en ligne doit être proportionnelle à la finalité (disponibilité des informations éligibles pour des tierces parties). Un autre problème révélé par l'enquête concernait la divulgation de numéros de naissance (à savoir, le numéro d'identification attribué à chaque nouveau-né). Grâce à l'enquête qui a révélé ce problème, le Bureau a réussi à inclure dans la version amendée du Code Commercial une disposition selon laquelle les numéros de naissance ne devaient être publiés ni dans l'extrait du Registre des sociétés, ni dans le journal commercial.

De nombreuses municipalités utilisent des caméras vidéo pour enregistrer ou transmettre leurs séances en temps réel. Le problème des **enregistrements et transmissions vidéo** des réunions de conseils municipaux fait l'objet d'observations étroites de la part du public et des journalistes. C'est pourquoi le Bureau a initié plusieurs enquêtes sur place et ensuite émis plusieurs principes : le conseil municipal doit toujours exposer clairement la finalité de l'enregistrement audio ou vidéo. Si une réunion est intégralement couverte, sans adaptations, le document est régi par la loi sur les archives. Ce document ne peut alors servir de source que pour le compte rendu de la réunion et doit être détruit une fois sa rédaction terminée. Si le conseil municipal assure la diffusion en continu en ligne d'une réunion (sans l'enregistrer), aucun traitement de données personnelles n'est impliqué et la loi relative à la protection des données n'est dès lors pas applicable.

Pour ce qui concerne l'émergence rapide du problème des communications électroniques dans le domaine des systèmes d'information publics, le Bureau s'est concentré sur le niveau de sécurité garanti pour les **opérations électroniques effectuées par les autorités publiques via des boîtes de données électroniques** gérées dans le cadre d'un système d'information de boîtes de données, en conformité avec la loi sur les opérations électroniques et les conversions autorisées. Le Bureau a initié une enquête auprès du ministère de l'Intérieur, qui était le responsable du traitement, et de la Poste tchèque, l'opérateur de ce système, et a par la suite jugé nécessaire d'étendre cette enquête au ministère de la Justice. Le nombre de plaintes a augmenté en 2010 et 2011 vis-à-vis du transfert de documents judiciaires adressés aux avocats sur les boîtes de données de personnes physiques exploitant des entreprises. Suite à une enquête du fournisseur des systèmes d'information, le ministère de la Justice a déclaré que les documents avaient été notifiés par erreur par certains tribunaux. Par ailleurs, le ministère de la Justice enregistre également les plaintes individuelles. Sur la base de ces informations, une enquête a été ouverte (également en conformité avec les priorités du plan d'inspection). Celle-ci concernait pour l'essentiel les conditions systémiques créées pour l'exécution des obligations des administrateurs en matière de traitement des données personnelles, dans le cadre de ce que l'on appelle le système de boîtes de données, une attention particulière étant accordée au respect de l'obligation de sécurité des données personnelles. Étant donné que le principal objectif d'une enquête est de trouver un recours et de créer les conditions d'un système éliminant les erreurs humaines, trois enquêtes sur place ont été axées sur le personnel du ministère de l'Intérieur responsable de l'installation et de l'administration des boîtes de données. Les employés du ministère de la Justice ont également été invités à la clôture de l'enquête, particulièrement en raison du fait que l'ensemble des plaintes déposées concernaient les tribunaux. D'après les déclarations des représentants des deux ministères, une alerte distincte devrait être introduite afin d'avertir les avocats de la date à laquelle des boîtes de données sont obligatoirement établies pour les avocats.

C. Autres informations importantes

En marge de la conférence des Commissaires à la vie privée et à la protection des données, qui s'est tenue à Mexico en octobre, l'un des délégués tchèques compétents a mené **auprès de l'ambassade tchèque** du Mexique une **enquête** portant sur le respect des engagements pris dans le cadre du processus d'évaluation de Schengen. Plus tard dans l'année, des enquêtes similaires ont été menées dans les ambassades tchèques de Macédoine et de Moldavie.

La Journée européenne de la protection des données à caractère personnel en janvier a donné l'occasion d'organiser un événement de **sensibilisation**. Cette année, le Bureau a annoncé ce qui représente déjà la cinquième édition du concours populaire destiné aux enfants et aux jeunes, intitulé « C'est ma vie privée ! Ne regardez pas, ne fouinez pas !» En préparant l'événement, le Bureau a de nouveau coopéré avec Radio Prague, le Festival international des films pour les enfants et la jeunesse dans la ville de Zlín, et aussi cette fois avec l'Association des bibliothécaires et professionnels de l'information. Dans plus de 100 bibliothèques de la République Tchèque, les enfants de 7 à 10 ans ont concouru dans le cadre du jeu « Through the Wild Web Woods », qui leur apprend de façon amusante comment se comporter de manière sûre et respectueuse sur l'internet. En concevant la version tchèque du jeu, le Bureau a coopéré avec le Conseil européen, qui avait préparé cette formation visant à apprendre de manière ludique les règles de la sécurité sur Internet.

Les experts du Bureau ont pris part, en tant que **conférenciers**, à une quarantaine d'événements locaux destinés aux universités et autres entités juridiques, commerciales et de droit public sur le sujet de la protection des données personnelles.

ROUMANIE

A. Résumé des activités et actualités

Organisation	Autorité nationale de contrôle du traitement des données à caractère personnel
Président et/ou collège	Georgeta Basarabescu
Budget	3 320 000 RON (environ 772 093 EUR)
Personnel	41, plus le Président et le Vice-président de l'autorité
Activités générales	
Décisions, avis, recommandations	1 214 (dont 1 décision normative)
Notifications	11 223
Examens préalables	1
Demandes émanant des personnes concernées	90
Plaintes émanant des personnes concernées	404
Conseils sollicités par le Parlement ou le gouvernement	58
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	214 (sur place)
Activités de sanction	
Sanctions	50 amendes pour un montant total de 61 300 RON (environ 14 222 EUR)
Amendes	41 avertissements
DPD	
Chiffres relatifs aux DPD	-

B. Informations sur la jurisprudence

Jurisprudence 1

L'autorité de contrôle a été avisée de deux cas concernant le traitement de données biométriques d'employés en vue de surveiller leurs heures de travail. Afin de vérifier ces aspects, des enquêtes ont été réalisées, avec les résultats suivants :

- L'introduction de systèmes électroniques pour vérifier les heures de travail avec la collecte d'informations telles que les empreintes digitales. Aussi chaque employé était-il tenu d'utiliser cet appareil biométrique à chaque entrée/sortie de l'unité afin d'enregistrer ses heures de travail effectives ;

- Ce type de décision, prise par la direction d'institutions publiques (un hôpital et une mairie), avait pour objet d'imposer aux employés le respect des heures de travail là où un registre des présences était auparavant signé pour enregistrer les retards ou les absences mais que certains employés signaient à la place d'autres collègues ;

- Les employés ont été avisés de la décision d'introduire le nouveau système de registre peu avant sa mise en œuvre ;

- Dans seulement l'un des deux cas ayant fait l'objet d'investigations, le consentement explicite des employés avait été demandé à cet égard ; toutefois, lorsque les employés ont pour la première fois été informés du système, ils ont été avertis que s'ils refusaient l'emploi de ce système de pointage biométrique, les heures qui n'y seraient pas enregistrées ne seraient pas payées, entraînant une rupture de fait du contrat de travail ;

- Bien que le système électronique visait à mettre un terme à l'emploi de l'ancien système de signature d'un registre de présence par les employés, chacune des deux entités observées a continué d'autoriser certaines personnes ou divisions à utiliser ces registres de présence ;

- L'obligation de notifier le traitement de données personnelles (biométriques) afin d'enregistrer les heures de travail n'a pas été respectée conformément aux dispositions de la Loi n° 677/2001 et à la décision du président de l'autorité de contrôle n° 11/2009 respectivement, dans un délai de 30 jours avant le début du traitement.

Sur la base de ces conclusions, l'autorité de contrôle a créé les mesures suivantes:

- Une sanction des contraventions commises par les entités contrôlées en vertu de l'Article 31 (défaut de respect des obligations de notification), de l'Article 32 (traitement excessif de données biométriques en référence à l'objet du traitement et défaut de transmission d'une réponse à une plainte reçue dans les délais légaux) et de l'Article 33 (défaut de mesures de sécurité) de la Loi n° 677/2001;

- Une décision de suspension ainsi qu'une décision ordonnant la cessation du traitement des données biométriques des employés aux fins de l'enregistrement de leurs heures de travail.

- Pour prendre ces décisions, l'autorité de contrôle a tenu compte des éléments suivants:

- L'objet déclaré du traitement des données, à savoir l'enregistrement des heures de travail des employés, aurait pu se faire par d'autres moyens moins intrusifs, tels que le registre de présence, ou d'autres fonctions du système électronique déployé. Il a été établi que la présence de certains

employés était encore enregistrée par l'emploi du registre de présence. L'utilisation de moyens différents pour atteindre le même objet pouvait potentiellement apparaître discriminatoire dans le cadre de l'application de règles internes aux employés d'une même entité. Par ailleurs, dans le contexte de la relation employeur-employé, le consentement écrit des employés dans l'un de ces cas n'a pas pu être présumé avoir été librement exprimé et informé de manière à rendre le traitement légitime, surtout si l'on tient compte des conséquences d'un refus du système.

Aussi, en vertu de l'Article 4 (1) (c) de la Loi n° 677/2001, telle que modifiée et amendée, le traitement de données biométriques d'employés était-il excessif par rapport à l'objet de leur collecte et de leur traitement ultérieur. Suite aux enquêtes, les deux entités ont respecté les décisions de l'autorité de contrôle leur ordonnant de mettre un terme au traitement des données biométriques des employés pour enregistrer leurs heures de travail.

Jurisprudence 2

Une autre situation a attiré l'attention de l'autorité de contrôle dans le cadre du traitement de données personnelles d'une carte d'identité aux fins de l'achat et de la recharge de cartes prépayées. En l'absence de toute base légale, le refus de présenter une carte d'identité priverait le consommateur / la personne d'un accès à un service de téléphonie mobile.

Suite aux enquêtes menées, il a été conseillé aux responsables du traitement des données de modifier la méthode de fourniture de leurs cartes prépayées, à savoir qu'une copie d'une carte d'identité ne pouvait être effectuée lors de l'achat d'une carte prépayée qu'avec le consentement écrit de la personne concernée. Concernant la recharge de la carte prépayée, l'autorité de contrôle a établi que ce service ne pouvait être conditionné à la présentation d'une carte d'identité.

Jurisprudence 3

L'autorité de contrôle a reçu des informations de la part d'étudiants concernant le fait que sur les sites web des universités auxquelles ils étaient inscrits figuraient des profils et un compte personnel pour chaque étudiant. L'accès à la page de profil, qui contenait les données personnelles d'un étudiant et de ses parents (nom et prénoms, nom de femme mariée, date et lieu de naissance, sexe, religion, série de la carte d'identité, numéro d'identification personnel, statut civil et militaire, ainsi que d'autres informations relatives à l'école) se faisait par le biais du numéro d'identification personnel.

Après vérification, il a été reconnu que ce type de profil faisait partie d'une application (University Management System – UMS) conçue pour les institutions de l'enseignement supérieur et que, d'un point de vue technique, l'authentification se faisait par le biais du numéro d'identification personnel et de la date de naissance.

L'objet du traitement des données dans le cadre de cette application était censé être le maintien de dossiers centralisés de tous les étudiants, de leur école et de leur situation financière, données demandées par le ministère de l'Éducation, de la Recherche, de la Jeunesse et des Sports aux fins de création d'un registre unique au niveau national.

Dans ce cas, la recommandation de l'autorité de contrôle a été de trouver un code d'identification unique autre que le numéro d'identification personnel comme moyen d'accéder au profil des étudiants.

ROYAUME-UNI

A. Résumé des activités et actualités

Développements de politiques publiques

L'ICO (Commissaire à l'information) a exercé son influence sur le passage de la Loi relative à la protection des libertés en apportant des preuves à la Commission parlementaire des projets de loi d'intérêt public. La nouvelle loi renforce le respect de la vie privée dans des domaines tels que la vidéosurveillance et les données biométriques, et assure à l'ICO une meilleure transparence et la garantie d'une plus grande indépendance. Nous avons également été l'un des premiers témoins de l'enquête Leveson sur la culture, les pratiques et l'éthique de la presse, pour laquelle nous avons fourni les preuves de nos rapports, qui étaient les premiers à dénoncer le commerce illicite d'informations personnelles, et plaidé en faveur de l'introduction de peines privatives de liberté.

Renforcement de nos capacités et, notamment, techniques

Nous bénéficions aujourd'hui de nouveaux pouvoirs qui permettent à l'ICO d'imposer des amendes pouvant s'élever jusqu'à 500 000 GBP en cas de violation grave de la réglementation sur la vie privée et les communications électroniques. Ceux-ci viennent équilibrer les pouvoirs similaires que nous avons déjà mis en œuvre pour en augmenter l'effet dans les cas de violations graves de la DPA 1998. Nous continuons de demander à bénéficier de pouvoirs accrus et avons soumis un dossier de décision au ministère de la Justice en vue d'étendre nos pouvoirs d'avis d'évaluation aux audits dans les secteurs de la NHS (service national de santé) et des autorités locales.

Compte tenu de l'importance de la technologie et de la protection des données, l'ICO a renforcé son bureau en désignant un conseiller technologique qui jouera un rôle important auprès du Commissaire à l'information dans le cadre du développement de politiques, des enquêtes et de la gestion des plaintes.

Conseils

Nous avons commencé l'année 2011 en célébrant la Journée européenne de la protection des données et en lançant une nouvelle « Boîte à outils d'information personnelle » afin d'aider les organisations du Royaume-Uni à mieux gérer les demandes d'accès des personnes concernées.

Nous avons également publié de nouveaux conseils sur le réglage des paramètres de sécurité Wi-Fi après qu'une étude a démontré que 40 % des particuliers ignoraient comment s'y prendre. Nous avons renvoyé des conseils sur la protection des données aux partis et candidats politiques faisant campagne pour le référendum sur le Royaume-Uni et les élections locales et nationales, et adressé des rappels aux services de santé afin qu'ils assurent la sécurité des informations personnelles des patients suite aux mesures d'application prises à l'encontre de cinq organisations de santé en violation avec la Loi sur la protection des données. Nous avons également émis des conseils à l'attention des étudiants concernant leurs droits en matière de protection des données et d'accès aux informations relatives à leurs notes d'examens.

Nous avons donné des conseils détaillés aux opérateurs de sites web du Royaume-Uni en réponse aux changements de la législation européenne exigeant d'eux qu'ils obtiennent le consentement des utilisateurs avant de stocker ou d'accéder à des informations sur leurs ordinateurs.

Nous avons continué de stimuler le débat sur la protection des données en organisant des événements sur le partage de données à Cardiff, Belfast et Glasgow pour les organisations des secteurs public, caritatif et bénévole afin de discuter de l'importance d'un partage de données efficace. Nous avons hébergé un séminaire sur l'anonymisation des données à Londres, avec plus de 100 délégués, dont des experts de plusieurs secteurs. Nous avons également tenu une conférence réunissant plus de 100 délégués en Irlande du Nord afin de discuter d'un dossier dans le domaine de la protection des données.

Éducation, éducation, éducation

Il est essentiel de s'assurer que les personnes ont conscience de leurs droits à l'information et d'intégrer ces droits aux systèmes d'éducation du Royaume-Uni. Nous avons lancé un projet de recherche afin d'explorer des modes de mise en pratique. Nous avons également collaboré avec des étudiants de 15 universités du Royaume-Uni dans l'objectif de sensibiliser les jeunes à leurs droits à l'information et de promouvoir le travail de l'ICO sur les campus.

Organisation	
Président et/ou collège	M. Christopher Graham (Commissaire)
Budget	19 695 000 GBP (frais de notification de 15 600 000 GBP et 4 500 000 GBP de subvention pour la liberté de l'information)
Personnel	Total : 378 Premier contact : 72 Résolution de problèmes des clients : 102 Application : 34 Liaison stratégique : 18 Mise en œuvre de politiques : 11 Notifications : 20 Audits : 32 Administration : 10 Gouvernance interne : 14 Juridique : 6 Affaires d'entreprise : 22 Établissements : 4 Finance : 7

	Informatique : 9 Apprentissage et développement : 3 Bureaux régionaux : 10
Activités générales	
Décisions, avis, recommandations	Boîte à outils d'information personnelle Conseils sur la liberté de l'information Consultations sur le code des pratiques d'anonymisation
Notifications	Nombre total de responsables de données notifiés : 355 292
Examens préalables	s. o.
Demandes émanant des personnes concernées	Appels sur la ligne d'assistance téléphonique : 217 183
Plaintes émanant des personnes concernées	Nombre de plaintes reçues dans le domaine de la protection des données : 12 985 Nombre de plaintes reçues dans le domaine de la liberté de l'information : 4 633 Nombre de plaintes reçues dans le domaine de la Loi sur la vie privée et les communications électroniques : 7 095
Conseils sollicités par le Parlement ou le gouvernement	Réponses données à 17 consultations
Autres renseignements relatifs aux activités générales	Nombre de « catégories d'activités pertinentes à déterminer par les DPA » Tout chiffre pertinent reflétant l'activité des DPA, par exemple le nombre de règles d'entreprise contraignantes (BCR) approuvées par les DPA.
Activités d'inspection	
Contrôles, enquêtes	42 audits
Activités de sanction	
Sanctions	2 avis d'exécution 8 mandats de perquisition émis Entreprises : 76

	Poursuites : 15 (1 cas ayant entraîné la confiscation de fonds pour un total de 73 000 GBP à rembourser)
Amendes	Nous avons imposé 10 amendes au civil, pour un total de 1171 000 GBP.
DPD	
Chiffres relatifs aux DPD	s. o.

Tous les chiffres ci-dessus concernent l'exercice financier 2011-2012

B. Informations sur la jurisprudence

Informations et données personnelles rendues anonymes

En février 2005, ProLife Alliance a demandé au Département de la Santé des informations statistiques détaillées sur les avortements pratiqués au cours de l'année 2003 en vertu de la Loi sur la liberté de l'information de 2000 (FOIA). Le Département de la Santé a refusé d'accéder à cette requête pour les statistiques sur les avortements pratiqués en 2003 en s'appuyant sur plusieurs exemptions de divulgation prévues par la FOIA, dont l'exemption prévue à la Section 40 concernant les données personnelles.

Suite à une plainte adressée au Commissaire à l'information sur la non-divulgation et à un appel auprès du Tribunal de l'information, l'affaire *R (sur demande du Département de la Santé) contre le Commissaire à l'information [2011] EWHC 1430 (Admin)* a été portée devant la Haute Cour et le juge Cranston. La principale question posée était de savoir si les statistiques détaillées sur les avortements constituaient des données personnelles au sens de la Loi sur la protection des données de 1998 (DPA).

Une attention particulière a été donnée à la définition de données personnelles donnée par la DPA ainsi que le 26e considérant de la Directive qui prévoit, notamment, que « les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable ». La cour a également examiné l'Avis (4/2007) du groupe de travail « Article 29 » sur le concept de données à caractère personnel et noté que l'Avis avait conclu que les données anonymes, aux fins de la Directive, pouvaient être définies « comme toute information relative à une personne physique, en vertu de laquelle la personne ne peut pas être identifiée par le responsable du traitement des données ou par toute autre personne, compte tenu de tous les moyens pouvant être raisonnablement déployés pour identifier cette personne ».

Le juge Cranston, suivant le raisonnement de Lord Hope, de la Cour suprême dans l'affaire de l'*organisme de services communs / le Commissaire à l'information écossais* [2008] UKHL 47, a jugé que le fait que le responsable du traitement des données ait accès à toutes les informations dont découlent les informations statistiques ne l'empêche pas de traiter ces données de manière à ce que, conformément au 26e considérant de la Directive, elles deviennent des données à partir desquelles plus aucune personne physique ne peut être identifiée. Si la conversion des informations sous-jacentes en statistiques peut parvenir à ce résultat, le responsable du traitement des données sera alors libre de divulguer les informations sous forme de statistiques puisqu'il ne s'agira plus de données personnelles. Le juge Cranston a considéré que la divulgation, par le Département de la Santé, de statistiques détaillées sur les avortements n'était pas équivalente à la divulgation de données personnelles. Ce jugement clarifie de

manière utile le lien étroit entre données personnelles et informations rendues anonymes conformément au 26e considérant de la Directive.

SLOVAQUIE

A. Résumé des activités et actualités

En 2011, le Bureau de protection des données à caractère personnel de la République Slovaque (ci-après le « Bureau ») a continué d'informer le grand public, via les médias, des développements en matière de protection des données dans différents domaines. Les employés du Bureau ont produit des annonces télévisées à l'occasion de la Journée de la protection des données et sur des sujets spécifiques tels que la protection des enfants sur Internet. Les experts du Bureau ont également rencontré une délégation du Commissaire serbe à l'information et à la protection des données et délivré des conférences sur des sujets choisis.

Le Bureau a par ailleurs initié un amendement important de la Loi sur les services de paiement qui prévoit d'informer les personnes concernées que, lorsqu'elles paient avec une carte de crédit un montant supérieur à un certain seuil fixé, leur numéro national d'identité peut faire l'objet d'un traitement. Cet accord a été conclu après plusieurs séries de négociations avec l'association des banques slovaques. Chacune des parties a convenu qu'un autocollant informatif serait apposé au niveau des points de vente.

Le Bureau a également été confronté à des coupes budgétaires à hauteur de 10 %, sous le prétexte de la réduction globale des dépenses de l'administration publique.

Cette situation a eu des conséquences négatives sur le contrôle national de la protection des données personnelles et sur l'exécution des tâches du Bureau, et a même entraîné le licenciement d'un certain nombre d'employés. Par conséquent, à l'initiative du Bureau, sa situation financière a été examinée par la Commission européenne dans le contexte d'une possible procédure d'infraction. Les procédures sont restées en phase initiale (pilote) jusqu'à la fin de l'année 2011.

Organisation	Bureau de protection des données à caractère personnel de la République slovaque
Président	M. Gyula Veszelei
Budget	684 349 EUR
Personnel	34 au premier semestre 2011 ; 29 au 31.12.2011
Activités générales	
Avis, recommandations	714 + 24 sur la base de la Loi sur l'accès public à l'information
Notifications	33, ainsi que 881 notifications de délégués à la protection des données personnelles
Examens préalables	8 (notifications spéciales)
Demandes émanant des personnes concernées	714+24

Plaintes émanant des personnes concernées Plaintes d'autres personnes	176 ; 6 plaintes répétées 33
Conseils sollicités par le Parlement ou le gouvernement	77
Autres renseignements relatifs aux activités générales	Procédures de contrôle : 266 au total Examens de plaintes : 290 au total Ordres contraignants pour les responsables individuels : 102 Décisions du président sur des objections formulées à l'encontre des décisions du Bureau (appels) : 12 Flux de données transfrontaliers : 20 décisions après approbation de transferts internationaux vers des pays tiers n'assurant pas un niveau adéquat de protection des données Affaires pénales : 6
Activités d'inspection	
Contrôles	125 sur la base de plaintes ; 57 contrôles d'office 36 soumissions pour explications ; Principaux thèmes et questions abordés : Recensement national : information insuffisante des citoyens sur l'anonymat des données personnelles acquises dans le cadre du recensement ; Cartes de fidélité : base légale erronée ; combinaison illégale de données personnelles traitées à d'autres fins que celles pour lesquelles elles avaient été collectées ; Vidéosurveillance : marquage inapproprié des zones surveillées ; non-effacement des dossiers dans les délais prescrits ; transmission illégale de dossiers aux médias de masse ; informations non satisfaisantes de la part de personnes ayant accès aux systèmes de vidéosurveillance ; Système d'information Schengen : mise en œuvre de l'obligation découlant du plan d'action national de Schengen ; inspection de l'émission de visas Schengen dans le département consulaire de l'ambassade de la République slovaque à Vienne, en Autriche ; inspection du Bureau national SIRENE, ministère de l'Intérieur de la

	République slovaque, sur l'application rigoureuse des Articles 95, 96 et 99 de la Convention de Schengen.
Activités de sanction	
Sanctions	9
Amendes	34 300 EUR ; fin 2011, la somme de 16 600 EUR avait été payée, le reste ayant été consacré aux procédures d'exécution.

B. Informations sur la jurisprudence

En 2011, aucune décision de justice n'a été prise par rapport aux appels déposés à l'encontre des décisions du Bureau. Le tribunal du district de Bratislava a eu connaissance d'un recours institué par une société par actions demandant des dommages et intérêts pour des pertes causées par une décision supposément illégale du Bureau. Les procédures ont été initiées en 2008 ; toutefois, le Bureau n'a été avisé de cette action et admis en tant que codéfendeur avec la République slovaque, représentée par le ministère de la Justice de la République slovaque, que le 14 juillet 2011. Le tribunal n'est pas parvenu à une décision en 2011.

SLOVÉNIE

A. Résumé des activités et actualités

Le Commissaire à l'information est l'autorité compétente pour les contrôles et les infractions dans le domaine de la protection des données, comme prévu par la Loi sur la protection des données à caractère personnel (LPDP) de la Slovénie. En 2011, le Commissaire a initié 682 cas concernant des violations présumées des dispositions de la LPDP, 246 dans le secteur public et 436 dans le secteur privé. Dans chacun de ces secteurs, les violations présumées les plus courantes sont de nature similaire, et portent sur la divulgation non autorisée de données personnelles par transfert de données à des tiers ou par la publication illicite de données, la collecte illégale de données, la mauvaise sécurité des données et, dans le secteur privé, l'utilisation illicite de données à des fins de marketing direct et de vidéosurveillance illicite. Le Commissaire a initié 136 procédures d'infraction. Le nombre de procédures de contrôle a augmenté par rapport à l'année précédente.

Outre ses compétences en matière de contrôles et d'infractions, le Commissaire émet des avis non contraignants et des éclaircissements sur des questions spécifiques relatives à la protection des données soulevées par des particuliers, des responsables du traitement des données, des organismes publics et des organisations internationales. En 2011, le Commissaire a émis 2 143 avis et éclaircissements, ce qui représente une augmentation significative par rapport à l'année précédente (1 859) ; 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. Dans ces cas, les responsables du traitement des données doivent tout d'abord obtenir l'autorisation du Commissaire.

Dans le cadre de ses activités de sensibilisation, le Commissaire a poursuivi son travail de prévention (exposés, conférences, ateliers pour divers types de public). En collaboration avec le Centre pour un Internet plus sûr de Slovénie, le Commissaire a mené des activités de sensibilisation à l'intention des enfants et des jeunes (exposés dans les écoles et publications). Le Commissaire a étendu le champ d'application de ses outils de sensibilisation et introduit un nouveau format de rapports spéciaux : les premières cartes de fidélité couvertes. Le Commissaire a également émis des *Lignes directrices sur les outils de protection de la vie privée en ligne*. Dans le contexte de la Journée européenne de la protection des données, le Commissaire a organisé un événement dans l'intention d'attirer l'attention sur l'importance de la protection des données personnelles dans la société moderne des TIC, avec l'avant-première d'un film documentaire intitulé « Erasing David ». 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'une de ces récompenses étant dédiée aux efforts relatifs au principe de respect de la vie privée dès la conception, ou « *privacy by design* »). Grâce à ces activités, le Commissaire jouit d'une très bonne réputation et de la confiance du public, ce dont témoignent les résultats du sondage d'opinion représentatif du « *Politbarometer* ». D'après ces résultats, le Commissaire arrive en première place en termes de confiance des citoyens slovènes envers différentes institutions.

Le Commissaire a participé à un certain nombre de groupes de travail interservices sur des projets d'administration en ligne, tels que sur la création d'identités électroniques plus sûres et conviviales, et sur la stratégie de développement de la société de l'information pour la période comprise entre 2011 et 2015. Le Commissaire a été consulté par le législateur et les autorités compétentes au sujet de 27 lois et autres textes législatifs dans les domaines de la délinquance juvénile, des registres immobiliers, des péages routiers, du commerce électronique et des signatures électroniques, de l'éducation supérieure, des

enfants présentant des besoins particuliers, des élections parlementaires, des procédures fiscales et pénales et du code pénal, etc.

Le Commissaire a participé activement aux activités d'un certain nombre d'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 » (WPPJ), 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, Madame le Commissaire à l'information 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	1 468 000 EUR
Personnel	30 employés : direction (6 – 2 des employés sont également des contrôleurs, et 2 des conseillers juridiques), administratifs (3), conseillers juridiques sur l'accès aux informations publiques (10), chercheurs et conseillers sur la protection des données (4), contrôleurs de la protection des données (11).
Activités générales	Protection des données et accès aux informations publiques
Décisions, avis, recommandations	261 avis et recommandations sur la base de demandes émanant des personnes concernées ou de responsables du traitement des données.
Notifications	Environ 200 notifications relatives à des systèmes d'archivage de données personnelles.
Examens préalables	25 examens préalables : 8 sur des données biométriques, 4 sur le transfert de données vers des pays tiers et 6 sur le regroupement de fichiers.
Demandes émanant des personnes concernées	2 143 demandes d'avis ou d'éclaircissements de la part de personnes concernées.
Plaintes émanant des personnes concernées	617 plaintes de la part de personnes concernées au total, 444 plaintes qualifiées. Domaines : 218 plaintes pour le transfert ou la divulgation illicite de données, 128 pour la collecte illicite de données, 79 pour des activités de marketing direct, 89 pour des activités de vidéosurveillance, 43 sur la sécurité des données, 60 liées à d'autres sujets. En outre, 85 plaintes sur les droits des personnes concernées ont également été traitées.
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 27 lois et autres textes législatifs, parmi lesquels la Loi sur les bases de

	données de santé, la Loi sur le traitement des délinquants juvéniles, la Loi sur le prélèvement des péages, la Loi sur les registres immobiliers, la Loi sur la procédure pénale, etc.
Autres renseignements relatifs aux activités générales	En 2011, le Commissaire : a poursuivi son travail de prévention (exposés, conférences) en collaboration avec le Centre pour un Internet plus sûr de Slovénie ; a participé à des groupes de travail interservices sur des projets d'administration en ligne, tels que sur les identités électroniques ; a publié des lignes directrices sur les outils de protection des données en ligne, et un rapport spécial sur les cartes de fidélité ; a été consulté sur un certain nombre de lois ; a poursuivi son implication et sa participation active à nombre de projets internationaux.
Activités d'inspection	
Contrôles, enquêtes	682 contrôles : 246 dans le secteur public, 436 dans le secteur privé.
Activités de sanction	
Sanctions	136 procédures de délits initiées (43 dans le secteur public, 66 dans le secteur privé, 27 personnes physiques), dont 30 avertissements, 52 réprimandes, 12 amendes et 7 injonctions de paiement.
Amendes	La DPA a imposé des amendes à hauteur de 50 035 EUR, hors taxes administratives.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Le Commissaire à l'information a reçu de nombreuses plaintes relatives à des cabinets vétérinaires envoyant aux propriétaires de chiens des notifications sur la vaccination et leur offrant simultanément d'autres services. Il a été avéré que les cabinets vétérinaires avaient obtenu les données personnelles des propriétaires de chiens auprès du registre central des chiens, qui n'a pas le statut d'un registre public, et dont les données ne peuvent servir qu'à des fins déterminées sur un plan juridique (le maintien du registre des chiens et des propriétaires de chiens, le contrôle de la régularité des vaccinations et le suivi des morsures, ainsi qu'à d'autres fins statistiques). Bien qu'ils aient accès à ces données, les cabinets vétérinaires n'auraient pas dû les utiliser à des fins de marketing direct. Seules les données personnelles des propriétaires de chiens clients d'un cabinet déterminé et les données de sources publiquement

accessibles peuvent servir à des fins de marketing direct. C'est pourquoi le Commissaire à l'information a sanctionné ces cabinets vétérinaires.

Le Commissaire à l'information a examiné un cas de **marketing direct offrant des services géodésiques** à des particuliers dont les immeubles ne figuraient pas au registre du portail Prostor (en français : espace). Bien que ces informations aient été obtenues de sources publiquement accessibles, le responsable du traitement des données a enfreint les dispositions de la LPDP dans la mesure où seules les informations suivantes peuvent servir à des fins de marketing direct : le nom de la personne, son adresse permanente ou temporaire et ses numéros de téléphone et de fax. Pour pouvoir utiliser les informations qu'un propriétaire n'a pas encore saisies sur sa propriété dans le registre, le responsable du traitement des données aurait besoin de son consentement explicite.

Le Commissaire a reçu une plainte concernant un **site de rencontres en ligne** dont les noms, adresses électroniques et mots de passe des utilisateurs ont été divulgués en ligne. Il a été établi que l'opérateur du site web avait confié la conception du site à un sous-traitant indien. Le produit ne comprenait aucune mesure de traçabilité du traitement des données, et une mauvaise programmation avait permis à l'auteur du délit d'obtenir les données de 7 000 utilisateurs du site. L'opérateur du site web s'est également avéré en infraction avec les dispositions sur le traitement contractuel des données parce qu'il n'avait pas conclu de contrat avec le responsable du traitement des données. Un transfert de données vers un pays tiers sans base légale a par ailleurs été établi. Le Commissaire a ordonné à l'opérateur du site web de mettre un terme au traitement des données et de notifier cet incident à l'ensemble des utilisateurs du forum.

Le Commissaire à l'information a découvert que les données personnelles des candidats aux élections parlementaires et locales passées étaient publiées sur le site web de la **Commission électorale nationale**. La loi sectorielle ne réglemente la publication des données personnelles des candidats qu'au regard de la période antérieure à une élection, mais pas de la période ultérieure. Le Commissaire a jugé que les données personnelles des candidats étaient publiées de manière à permettre aux électeurs de prendre une décision de voter libre et informée quant aux listes et candidats. Dans la mesure où le traitement des données personnelles avait déjà rempli son office pour les élections passées, le responsable du traitement des données aurait dû effacer les données des candidats.

Le Commissaire a traité une affaire où des **photographies spatiales contenant des images de personnes identifiables** avaient été publiées sur le site web d'un photographe professionnel. Lors de la procédure, les photographies spatiales ont été considérées dans le contexte du dessein de leur publication et de la possibilité d'identifier les personnes dans les images. Le Commissaire a jugé que l'objet des photographies (la description de l'héritage naturel et culturel) pouvait être atteint sans que les passants soient identifiables. L'intérêt du photographe dans la publication dans ce cas n'est pas supérieur à celui du passant, qui reste libre de décider s'il souhaite pouvoir être identifié dans une image. C'est la raison pour laquelle ces images doivent être rendues anonymes avant leur publication sur Internet, de manière à ce que les personnes ne puissent plus être identifiées. Dans son opinion à ce sujet, le Commissaire a également souligné la différence entre photographie de rue et photographie spatiale.

C. Autres informations importantes

En termes de **coopération internationale**, le Commissaire a également été actif dans le domaine de la coopération bilatérale internationale. En 2011, le Commissaire a accueilli les représentants de plusieurs pays tels que la Croatie, la Serbie, le Kosovo, le Monténégro et la Macédoine. En tant que Partenaire mineur, il a poursuivi la mise en œuvre du projet de jumelage IPA 2009, n° MN/09/IB/JH/03 (sur la mise en œuvre de la stratégie de protection des données personnelles au Monténégro) pour lequel il a été sélectionné en 2010, en collaboration avec le leader du projet, l'Institut autrichien des droits de l'homme Ludwig Boltzmann. En novembre 2011, le Commissaire à l'information a été sélectionné par la

Commission européenne pour mettre en œuvre le projet de jumelage allégé SR/2009/IB/JH/01 pour l'amélioration de la protection des données personnelles en Serbie. Le Commissaire à l'information a également réalisé un contrôle auprès des ambassades de la République de Slovénie à Pristina et au Caire, où elle a examiné, notamment, la légalité du traitement des données personnelles dans le cadre des procédures d'obtention de visas pour la zone Schengen et du Système d'information des visas (VIS).

Parmi les **questions de politique** largement traitées par le Commissaire, il convient de mentionner l'usage croissant de la vidéosurveillance dans des espaces tels que les saunas, les vestiaires, les aires de jeux pour enfants et certains autres lieux publics tels que des chemins de promenade. Le Commissaire note également une augmentation des cas liés au marketing en ligne et aux courriels non sollicités, où les expéditeurs ne peuvent souvent pas démontrer qu'ils ont obtenu le consentement des destinataires, ne respectent pas le principe de retrait et n'informent pas les destinataires de leurs droits. Concernant la sécurité du traitement des données, le Commissaire note que la sécurité n'est souvent pas suffisamment exhaustive pour satisfaire les conditions visées par la LPDP. Dans un certain nombre de cas, les données personnelles se sont avérées être accessibles sur Internet.

Le Commissaire à l'information a par ailleurs noté que de nombreux responsables du traitement des données sont confrontés au dilemme de l'utilisation de **l'informatique en nuage**, qui soulève certaines questions quant au respect de la législation dans le domaine de la protection des données personnelles et de la vie privée. Les organisations qui décident d'utiliser l'informatique en nuage ne disposent souvent pas d'informations suffisantes sur l'endroit où leurs données personnelles seront stockées et la manière dont elles seront protégées et, sans ces informations, il est difficile d'analyser les risques de manière appropriée avant de prendre la décision de faire appel ou non à l'informatique en nuage. Le Commissaire à l'information a émis quelques avis sur l'informatique en nuage et, fin 2011, a également commencé à préparer des lignes directrices dans l'intention d'aider les responsables du traitement des données dans leur prise de décision quant à l'utilisation de ce produit.

SUÈDE

A. Résumé des activités et actualités:

Supervision

Administration en ligne

Le Conseil d'inspection des données a publié un bulletin d'information spécifique sur le traitement des données personnelles et l'administration en ligne. Dans le contexte qui nous réunit, nous avons également publié sur notre site web des informations sur le respect de la vie privée dès la conception (« *privacy by design* »). Nous avons également donné des avis sur la législation proposée à cet égard et réalisé un audit spécifique sur l'échange électronique d'informations entre autorités. D'autres audits sur l'administration en ligne ont été orientés vers les domaines de la santé, des soins médicaux et des services sociaux.

Informatique en nuage

Afin de clarifier les exigences fixées par la Loi sur les données à caractère personnel en termes d'informatique en nuage, le Conseil d'inspection des données a audité plusieurs entreprises et autorités locales qui font appel à ces services. Le projet a donné lieu à un dépliant d'information contenant une liste de vérification des exigences en matière de protection des données dans les services d'informatique en nuage.

Vidéosurveillance

Un vaste projet d'audit a été complété sur le thème de la vidéosurveillance sur le lieu de travail, dans les bâtiments résidentiels et les écoles. Ce projet a abouti à la création de dépliants d'information contenant des listes de vérification des points dont il convient de tenir compte en matière de vidéosurveillance.

Sensibilisation

Nous avons continué de travailler de manière proactive afin de sensibiliser à la protection des données et au respect de la vie privée (une part importante de notre stratégie) et d'améliorer la visibilité des questions de protection des données et de la vie privée. En 2011, le nombre de visites sur notre site web a augmenté de 24 %. Le Conseil d'inspection des données a également noté une importante augmentation du nombre de questions posées à notre service d'assistance sur la protection des données. Par ailleurs, et pour la quatrième année, le Conseil a publié une brochure intitulée l'Année de la vie privée (2011), qui compile et synthétise la législation, les propositions législatives, les décisions et autres éléments ayant eu des implications pour la vie privée au cours de l'année.

Autres activités

Un représentant du Conseil d'inspection des données a été rapporteur du sous-groupe du groupe de travail Article 29 sur les données de santé pour la rédaction d'un document de travail sur epSOS (European Patients Smart Open Services), WP 189.

En vue de l'entrée en vigueur de la nouvelle Loi sur les données de la police en mars 2012, une plus grande attention a été portée aux questions de protection des données dans le domaine de l'application de la loi.

Organisation	
Président et/ou collège	Göran Gräslund Directeur général
Budget	37 millions de SEK = 4,2 millions d'EUR
Personnel	47
Activités générales	
Décisions, avis, recommandations	247 audits initiés en 2011 107 avis sur des propositions législatives 61 avis en consultation avec des fonctionnaires chargés de la protection des données 13 lignes directrices, recommandations et rapports
Notifications	215
Examens préalables	238
Demandes émanant des personnes concernées	206 demandes formelles Questions informelles par téléphone et courriels adressées à notre service d'assistance : 4 700 (par courriel) 7 500 (par téléphone)
Plaintes émanant des personnes concernées	312
Conseils sollicités par le Parlement ou le gouvernement	107 avis sur des propositions législatives
Autres renseignements relatifs aux activités générales	Exposés, conférences et séminaires : 42 Communiqués de presse : 67
Activités d'inspection	
Contrôles, enquêtes	43 audits de terrain 134 audits de bureau 70 audits par questionnaire

	Principaux sujets : informatique en nuage, vidéosurveillance, systèmes de localisation des employés par GPS, vérifications des antécédents par les agences de recrutement, administration en ligne
Activités de sanction	
Sanctions	Aucune en vertu de la Loi sur les données à caractère personnel
Amendes	s.o.
DPD	
Chiffres relatifs aux DPD	Le nombre total de DPD notifiés en 2011 était de 6 621. Le Conseil d'inspection des données a reçu 61 consultations formelles de DPD et organisé 9 conférences spécifiquement adressées aux DPD.

B. Informations sur la jurisprudence

La Cour administrative suprême a confirmé la précédente décision du Conseil d'inspection des données de ne pas autoriser la vidéosurveillance dans les halls d'entrée des bâtiments résidentiels. Le Conseil d'inspection des données avait ordonné à une société immobilière de mettre un terme à son utilisation de la vidéosurveillance dans les halls d'entrée de ses bâtiments résidentiels, qui rendait possible la surveillance, par la société, des habitudes et relations des locataires. La décision du Conseil a fait l'objet d'un appel auprès de la Cour administrative et de la Cour d'appel administrative, qui ont toutes deux confirmé la décision du Conseil. En décembre 2011, la Cour administrative suprême a confirmé cette décision. Pour l'équilibre des intérêts, la Cour a jugé qu'il n'y avait eu aucune preuve que les bâtiments étaient particulièrement exposés à des activités criminelles, ni qu'ils présentaient d'importants besoins en surveillance. La vidéosurveillance devait dès lors être considérée comme une infraction au respect de la vie privée et non conforme à la Loi sur les données à caractère personnel.

Chapitre trois

Union Européenne et activités communautaires

3.1. COMMISSION EUROPÉENNE

Édition 2011 de la Journée européenne de la protection des données, le 28/01/2011

La protection des données à caractère personnel est un droit fondamental au sein de l'UE. Le 28 janvier 2011, la Commission et les États membres du Conseil de l'Europe ont célébré pour la cinquième fois la Journée de la protection des données.

Cette date marque l'anniversaire de la Convention 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.

Pour marquer la Journée de la protection des données 2011, des événements ont été organisés non seulement en Europe, mais à travers le monde entier, afin de sensibiliser les citoyens à la protection des données, de les informer de leurs droits et des bonnes pratiques existantes et, par conséquent, de leur permettre d'exercer ces droits de manière plus efficace.

Cette journée spéciale offre l'occasion de sensibiliser les particuliers à la protection des données personnelles et à leurs droits et responsabilités en la matière.

Le principal événement de la Journée de la protection des données 2011 a été une réunion de haut niveau commune sur la protection des données (la Protection des données 30 ans plus tard) conformément aux normes européennes et internationales.

Outre les interventions du Secrétaire Général du Conseil de l'Europe, d'un Vice-président de la Commission et du Directeur Général de la DG Justice de la Commission, le panel sur les nouvelles règles européennes de protection des données comprenait le président du Comité consultatif de la Convention 108, le Conseil de l'Europe, le Contrôleur européen de la protection des données et le Président du groupe de travail « Article 29 ».

Consultation sur l'approche globale de la Commission en matière de protection des données à caractère personnel dans l'Union européenne – 15 janvier 2011

Pour connaître les avis concernant les idées de la Commission, telles que décrites dans sa Communication jointe à la présente consultation, sur la manière d'aborder les nouveaux défis qui se posent en matière de protection des données personnelles (tels que le développement rapide des technologies ou la mondialisation) afin d'assurer une protection efficace et exhaustive des données à caractère personnel au sein de l'UE.

La Commission a reçu 305 réponses à cette consultation publique : 54 de la part de citoyens, 31 de la part de pouvoirs publics, 220 de la part d'organismes privés.

Enquête spéciale Eurobaromètre : Attitudes à l'égard de la protection des données et de l'identité électronique au sein de l'Union européenne, juin 2011

L'enquête spéciale Eurobaromètre est la plus grande étude jamais réalisée sur le comportement et les attitudes des citoyens en matière de gestion de l'identité, de protection des données et de respect de la vie privée, et présente les attitudes et comportements des Européens sur le sujet.

Les principales conclusions de l'enquête sont les suivantes :

- 74 % des Européens considèrent que *divulguer des informations personnelles* est une part de plus en plus importante de la vie moderne.

- Les informations considérées comme personnelles sont, avant tout, des informations financières (75 %), des informations médicales (74 %) et des numéros ou cartes nationales d'identité et passeports (73%).

- Les utilisateurs des réseaux sociaux et des sites de partage ont beaucoup plus tendance à divulguer leur nom (79 %), leur photo (51 %) et leur nationalité (47 %). La *véritable divulgation en ligne d'informations personnelles* par les acheteurs en ligne concerne principalement leur nom (90 %), l'adresse de leur domicile (89 %) et leur numéro de téléphone mobile (46 %).

- La raison la plus importante de cette divulgation est l'accès à un service en ligne, que ce soit pour les utilisateurs des réseaux sociaux et des sites de partage (61 %) ou pour les acheteurs en ligne (79 %).

- 43 % des internautes déclarent que les informations personnelles qui leur sont demandées lorsqu'ils souhaitent avoir accès à ou utiliser un service en ligne sont excessives.

- La plupart des Européens s'inquiètent de l'enregistrement de leur comportement via leurs cartes de paiement (54 % vs. 38 %), leurs téléphones mobiles (49 % vs. 43 %) ou leur Internet mobile (40 % vs. 35 %).

- Presque six internautes sur dix lisent généralement les déclarations de confidentialité (58 %) et la majorité de ceux qui les lisent adaptent leur comportement sur Internet (70%).

- Plus de la moitié des internautes sont informés des conditions de collecte des données et de l'utilisation ultérieure de leurs données lorsqu'ils rejoignent un réseau social ou s'inscrivent à un service en ligne (54 %).

- Seulement un tiers des Européens sont conscients de l'existence d'une autorité publique nationale responsable de la protection de leurs droits sur leurs données personnelles (33 %).

- À peine plus d'un quart des utilisateurs de réseaux sociaux (26 %) et encore moins d'acheteurs en ligne (18 %) ont le sentiment d'avoir un *contrôle total*.

- Les Européens utilisent les types suivants de pièces d'identité : cartes de crédit et cartes bancaires (74%), cartes nationales d'identité ou permis de résidence (68 %), cartes de droits nationales (65 %), ou permis de conduire (63 %). 34 % des personnes interrogées ont un compte sur Internet, qu'ils utilisent pour des services de messagerie électronique, de réseau social ou commerciaux.

- Afin de protéger leur identité dans la vie de tous les jours, 62 % des Européens donnent le minimum d'informations requis.

- Afin de protéger leur identité sur Internet, les stratégies les plus utilisées sont techniques ou *procédurales*, telles que les outils et stratégies visant à limiter les courriels non sollicités tels que les spams (42 %), la vérification qu'une transaction est protégée ou que le site présente un logo ou une étiquette de sécurité (40 %), et l'utilisation d'un logiciel anti-espion (39 %).

- Les autorités et les institutions (dont la Commission européenne et le Parlement européen) bénéficient d'une confiance supérieure (55%) à celle qui est accordée aux sociétés commerciales.

- Moins d'un tiers font confiance aux entreprises de téléphonie, de téléphonie mobile et opérateurs Internet (32 %) et à peine plus d'un cinquième font confiance aux entreprises Internet telles que les moteurs de recherche, les sites de réseaux sociaux et les services de messagerie électronique (22 %).

- 70 % des Européens s'inquiètent de ce que leurs données personnelles soient aux mains de sociétés et pourraient servir à d'autres fins que ce pourquoi elles ont été collectées.

- 28 % sont prêts à payer l'accès à leurs informations personnelles stockées par des entités publiques ou privées.

- Concernant le « droit à l'oubli », une majorité très nette d'Européens (75 %) souhaite pouvoir supprimer ses informations personnelles d'un site web à tout moment.

- Bien qu'une majorité d'internautes européens se sente personnellement responsable de la sécurité de la gestion de ses données personnelles, presque tous les Européens (90%) sont en faveur de l'égalité des droits de protection au sein de l'UE.

- Plus de quatre Européens sur dix préfèreraient que la réglementation soit appliquée au niveau de l'administration européenne (44 %), tandis qu'un nombre à peine moindre préfèrerait que cette application se fasse au niveau national (40 %).

- Lorsqu'on leur demande quel type de réglementation devrait être introduite afin d'empêcher les sociétés d'utiliser des données personnelles sans que les personnes concernées ne le sachent, la plupart des Européens pensent qu'on devrait imposer des amendes à ces sociétés (51 %), leur interdire d'utiliser ce genre de données à l'avenir (40 %) ou les obliger à indemniser leurs victimes (39 %).

- La majorité pense que ses données personnelles seraient mieux protégées dans les grandes entreprises si celles-ci étaient obligées d'avoir un délégué à la protection des données (88 %).

- Les Européens sont partagés quant aux circonstances selon lesquelles la police devrait avoir accès aux données personnelles. A contrario, presque tous sont d'accord pour dire que les mineurs devraient être protégés de (95 %) et avertis contre (96 %) la divulgation de données à caractère personnel, et une vaste majorité est en faveur d'une protection spéciale des données génétiques (88 %).

3.2. COUR DE JUSTICE DE L'UNION EUROPÉENNE

Arrêt de la Cour européenne de justice (Grande chambre) du 9 mars 2010 – Commission européenne c/ République fédérale d'Allemagne (Affaire C-518/07)

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 notamment la Cour a décidé qu'en plaçant sous la tutelle de l'État les autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel effectué par les organismes du secteur privé et par 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 doivent exercer 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.

Jugement du Tribunal de la fonction publique (Première chambre) du 28 juin 2011 – AS c/ Commission européenne (Affaire F-55/10)

Le secret médical couvre, notamment, les informations portées à l'attention d'un professionnel de santé dans l'exercice de ses fonctions, et qui lui sont communiquées par son patient. Le droit à la protection du secret médical, qui est un aspect du droit au respect de la vie privée, est un droit fondamental protégé par le droit de l'Union. Ces deux droits peuvent prévoir des restrictions, sous réserve qu'elles aient réellement des objectifs d'intérêt général fixés par l'Union et ne constituent pas, dans le cadre de l'objet poursuivi, une entrave disproportionnée et intolérable portant atteinte à la substance même des droits garantis.

À cet égard, et en référence à l'Article 8 de la Convention européenne des droits de l'homme, l'entrave d'une autorité publique vis-à-vis du droit au respect de la vie privée, qui inclut le droit de tenir son état de santé secret, peut être justifiée si elle est « prescrite par la loi », si elle poursuit l'un des objectifs visés au paragraphe 2 dudit article, tels que le « bien-être économique » et la « protection de la santé », et est nécessaire « pour atteindre ces objectifs ».

Ce n'est pas le cas de l'utilisation par une institution, dans le contexte d'un recours introduit par un fonctionnaire, d'éléments du dossier médical de la personne aux seules fins d'élaboration d'une argumentation susceptible de démontrer son absence d'intérêt à agir.

Jugement du Tribunal de la fonction publique (Première chambre) du 5 juillet 2011 – V. c/ Parlement européen (Affaire F-46/09)

Le droit au respect de la vie privée garanti par l'Article 8 de la Convention européenne des droits de l'homme et découlant des traditions constitutionnelles communes des États membres, est l'un des droits fondamentaux protégés par l'ordre juridique de l'Union. Il inclut le droit d'une personne à garder son état de santé secret.

Le transfert à des tiers, notamment à une autre institution, de données personnelles relatives à la santé d'une personne collectées par une institution, constitue en soi une entrave à la vie privée de la personne, quel que soit l'objet final dudit transfert.

Toutefois, l'Article 8, paragraphe 2 de la Convention stipule que l'entrave à la vie privée par une autorité publique peut être justifiée si elle est « prescrite par la loi », si elle poursuit un ou plusieurs objectifs (dont est dressée une liste exhaustive) et si elle est « nécessaire » pour atteindre le ou les objectifs en question.

Compte tenu de la nature extrêmement privée et sensible des données médicales, la possibilité de transférer ou de divulguer ces informations à des tiers, y compris dans le cadre d'un tranfert d'une institution à une autre ou d'un organisme de l'Union à un autre, , sans le consentement de la personne concernée, nécessite une attention particulière.

Jugement du Tribunal (Seconde chambre) du 23 novembre 2011 – Gert-Jan Dennekamp c/ Parlement européen (Affaire T-82/09)

Comme établi par l'Article 1 du Règlement n° 1049/2001, qui reflète le 4e considérant du préambule de celui-ci, ledit règlement a vocation à donner au public un droit d'accès aussi vaste que possible aux documents des institutions (Affaires jointes C-39/05 P et C-52/05 P *Suède et Turco* c/ *Conseil* [2008] ECR I-4723, point 33).

Lorsqu'il est demandé à une institution de divulguer un document, elle doit évaluer dans chaque cas particulier si ce document fait partie des exceptions au droit d'accès du public aux documents des institutions prévues à l'Article 4 du Règlement n° 1049/2001, (voir, à cet effet, à l'Affaire *Suède et Turco* c/ *Conseil*, point 21 supra, point 35). En vue des objectifs poursuivis par le Règlement n° 1049/2001, ces exceptions doivent être interprétées et appliquées de manière stricte (*Suède et Turco* c/ *Conseil*, point 36).

En second lieu, selon une jurisprudence constante, lors de l'examen des relations entre le Règlement n° 1049/2001 et le Règlement n° 45/2001 aux fins de l'application de l'exception prévue à l'Article 4(1)(b) du Règlement n° 1049/2001 (à savoir, la protection de la vie privée et de l'intégrité de la personne), il convient de garder à l'esprit que ces règlements ont des objectifs différents. Le Règlement n° 1049/2001 est conçu pour garantir la meilleure transparence possible en ce qui concerne le processus décisionnel des autorités publiques et les informations sur lesquelles elles basent leurs décisions. Il a donc vocation à faciliter autant que possible l'exercice du droit d'accès aux documents et à promouvoir les bonnes pratiques administratives. Le Règlement n° 45/2001 est conçu pour assurer la protection des libertés et des droits fondamentaux des personnes et, notamment, leur vie privée, dans le cadre de la gestion des données personnelles (*Commission* c/ *Bavarian Lager*, point 13 supra, point 49).

Étant donné que le Règlement n° 1049/2001 et le Règlement n° 45/2001 ne contiennent aucune disposition assurant la primauté de l'un sur l'autre, la pleine application de chacun des règlements devrait, en principe, être assurée (*Commission* c/ *Bavarian Lager*, point 13 supra, point 56).

L'Article 4(1)(b) du Règlement n° 1049/2001 établit un système de protection spécifique et renforcé pour une personne dont les données personnelles pourraient, dans certains cas, être communiquées au public (*Commission* c/ *Bavarian Lager*, point 13 supra, point 60).

Lorsqu'une demande basée sur le Règlement n° 1049/2001 porte sur l'accès à des documents comprenant des données personnelles, le Règlement n° 45/2001 devient applicable dans son intégralité, y compris son Article 8 (*Commission* c/ *Bavarian Lager*, point 13 supra, point 63).

En troisième lieu il convient de noter que, dans le cas présent, la demande d'accès a été faite en vue d'obtenir les noms des membres du Parlement européen qui participaient, à la date de la demande initiale, ou avaient participé, au 1er septembre 2005, au régime de pension complémentaire ainsi que les noms des participants à la date de la demande initiale pour lesquels le Parlement versait une cotisation mensuelle au régime. . Les noms des députés européens constituent des données personnelles au sens de l'Article 2(a) du Règlement n° 45/2001 (voir, à cet effet, *Commission* c/ *Bavarian Lager*, point 13 supra, point 68).

En outre, conformément à ce que le Parlement européen a jugé à juste titre dans la décision contestée, la communication de données personnelles répond à la définition de « traitement de données à caractère personnel » utilisée dans le Règlement n° 45/2001 (voir, à cet effet, *Commission* c/ *Bavarian Lager*, point 13 supra, point 69).

Par conséquent, l'Article 8(b) du Règlement n° 45/2001 est applicable à la demande d'accès qui concernait des documents contenant des données personnelles, et il n'est pas possible pour le demandeur de s'y opposer en arguant du fait que le « traitement » qu'il demande serait licite sur la base de l'Article 5(b) du Règlement n° 45/2001 ou que cela suffirait dans la mesure où l'Article 8(b) de ce Règlement s'applique sans préjudice de l'Article 5.

Pour obtenir la divulgation de données personnelles contenues dans les documents qu'il demandait, le demandeur aurait dû démontrer, en fournissant une justification expresse et légitime,, la nécessité du transfert des données personnelles demandées de manière à permettre au Parlement européen d'évaluer les différents intérêts des parties concernées et de déterminer, conformément à l'Article 8(b) du Règlement n° 45/2001, s'il y avait une raison de penser que ce transfert de données aurait pu porter atteinte aux intérêts légitimes des députés européens (voir, à cet effet, *Commission* c/ *Bavarian Lager*, point 13 supra, point 78).

Jugement de la Cour (Troisième chambre) du 24 novembre 2011 – Scarlet Extended SA c/ Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (Affaire C-70/10)

Les Directives 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information et 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 sur l'application des droits de propriété intellectuelle, en conjonction avec les Directives 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, 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « Vie privée et communications électroniques ») et 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« Directive sur le commerce électronique »), interprétées à la lumière des Articles 7, 8, 11 et 52(1) de la Charte des Droits fondamentaux de l'Union européenne compte tenu des Articles 8 et 10 de la Convention européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales, doivent être interprétées comme interdisant l'adoption par une juridiction nationale, sur la seule base d'une disposition prévoyant que « [la juridiction compétente] peut également rendre une injonction de cessation à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte au droit d'auteur ou à un droit voisin », afin d'ordonner à un « [Fournisseur d'Accès à l'Internet (en abrégé FAI)] de mettre en place, à l'égard de toute sa clientèle, in abstracto et à titre préventif, aux frais exclusifs de ce FAI et sans limitation dans le temps, un système de filtrage de toutes les communications électroniques, tant entrantes que sortantes, transitant par ses services, notamment par l'emploi de logiciels poste à poste (*peer-to-peer*), en vue d'identifier sur son réseau le partage de fichiers électroniques contenant une

œuvre musicale, cinématographique ou audiovisuelle sur laquelle le demandeur prétend détenir des droits et ensuite de bloquer le transfert de ces fichiers, que ce soit au niveau de la requête ou de l'envoi ».

Jugement de la Cour (Troisième chambre) du 24 novembre 2011 – Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) / Administración del Estado. (Affaires jointes C-468/10 et C-469/10)

Par sa première question, la juridiction de renvoi demande, en substance, si l'article 7, sous f), de la Directive 95/46 doit être interprété en ce sens qu'il s'oppose à une réglementation nationale qui, en l'absence du consentement de la personne concernée et pour autoriser le traitement de ses données personnelles nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable de traitement ou par le ou les tiers auxquels ces données sont communiquées, exige, outre le respect des droits et libertés fondamentaux de cette dernière, que lesdites données figurent dans des sources accessibles au public.

L'article 1er de la Directive 95/46 impose aux États membres d'assurer la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel (voir, à cet effet, l'Affaire C-524/06 *Huber* [2008] ECR I-9705, point 47).

Conformément aux dispositions du Chapitre II de la Directive 95/46, intitulé « Conditions générales de licéité des traitements de données à caractère personnel », sous réserve des dérogations admises au titre de l'article 13 de cette directive, tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes relatifs à la qualité des données énoncés à l'article 6 de ladite directive et, d'autre part, répondre à l'un des six principes relatifs à la légitimation des traitements de données énumérés à l'article 7 de cette même directive (voir, à cet effet, les Affaires jointes C-465/00, C-138/01 et C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, point 65, et *Huber*, point 48).

Il ressort du septième considérant de la Directive 95/46 que l'établissement et le fonctionnement du marché intérieur sont susceptibles d'être sérieusement affectés par les différences entre les régimes nationaux applicables au traitement des données à caractère personnel (Affaire C-101/01 *Lindqvist* [2003] ECR I-12971, point 79).

Dans ce contexte, il faut rappeler que la directive 95/46 vise, ainsi qu'il ressort notamment de son huitième considérant, à rendre équivalent dans tous les États membres le niveau de protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel. Son dixième considérant ajoute que le rapprochement des législations nationales applicables en la matière ne doit pas conduire à affaiblir la protection qu'elles assurent, mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans l'Union (voir, en ce sens, arrêts précités Lindqvist, point 95, et Huber, point 50).Ainsi, il a été jugé que l'harmonisation desdites législations nationales ne se limite pas à une harmonisation minimale, mais aboutit à une harmonisation qui est, en principe, complète. C'est dans cette optique que la directive 95/46 entend assurer la libre circulation des données à caractère personnel, tout en garantissant un haut niveau de protection des droits et des intérêts des personnes visées par ces données (*Lindqvist*, point 96).

Dès lors, il découle de l'objectif consistant à assurer un niveau de protection équivalent dans tous les États membres que l'article 7 de la directive 95/46 prévoit une liste exhaustive et limitative des cas dans lesquels un traitement de données à caractère personnel peut être considéré comme étant licite.

Cette interprétation est corroborée par les termes « ne peut être effectué que si » et la conjonction « ou » contenus dans l'article 7 de la directive 95/46, qui mettent en évidence la nature exhaustive et limitative de la liste figurant à cet article.

Il s'ensuit que les États membres ne sauraient ni ajouter de nouveaux principes relatifs à la légitimation des traitements de données à caractère personnel à l'article 7 de la directive 95/46 ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article.

L'interprétation qui précède n'est pas remise en cause par l'article 5 de la directive 95/46. En effet, cet article n'autorise les États membres qu'à préciser, dans les limites du chapitre II de ladite directive et, partant, de l'article 7 de celle-ci, les conditions dans lesquelles les traitements de données à caractère personnel sont licites.

La marge d'appréciation dont, en vertu dudit article 5, disposent les États membres ne peut donc être utilisée que conformément à l'objectif poursuivi par la directive 95/46 consistant à maintenir un équilibre entre la libre circulation des données à caractère personnel et la protection de la vie privée (*Lindqvist*, point 97).

La Directive 95/46 comporte des règles caractérisées par une certaine souplesse et laisse dans de nombreux cas aux États membres le soin d'arrêter les détails ou de choisir parmi des options (*Lindqvist*, point 83). Il importe ainsi de faire la distinction entre des mesures nationales qui prévoient des exigences supplémentaires modifiant la portée d'un principe visé à l'article 7 de la directive 95/46, d'une part, et des mesures nationales qui prévoient une simple précision de l'un de ces principes, d'autre part. Le premier type de mesure nationale est interdit. Ce n'est que dans le cadre du second type de mesure nationale que, en vertu de l'article 5 de la Directive 95/46, les États membres disposent d'une marge d'appréciation.

Il s'ensuit qu'au titre de l'article 5 de la Directive 95/46, les États membres ne sauraient non plus introduire d'autres principes relatifs à la légitimation des traitements de données à caractère personnel que ceux énoncés à l'article 7 de cette directive ni modifier, par des exigences supplémentaires, la portée des six principes prévus audit article 7.

En l'occurrence, l'article 7, sous f), de la directive 95/46 dispose que le traitement de données à caractère personnel est licite s'« il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1 ».

Ledit article 7, sous f), prévoit deux conditions cumulatives pour qu'un traitement de données à caractère personnel soit licite, à savoir, d'une part, que le traitement des données à caractère personnel doit être nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées et, d'autre part, que les droits et libertés fondamentaux de la personne concernée ne prévalent pas.

Il s'ensuit que, s'agissant du traitement de données à caractère personnel, l'article 7, sous f), de la directive 95/46 s'oppose à toute réglementation nationale qui, en l'absence du consentement de la personne concernée, impose, outre les deux conditions cumulatives mentionnées au point précédent, des exigences supplémentaires.

Toutefois, il convient de tenir compte du fait que la seconde de ces conditions nécessite une pondération des droits et intérêts opposés en cause qui dépend, en principe, des circonstances concrètes du cas particulier concerné et dans le cadre de laquelle la personne ou l'institution qui effectue la pondération doit tenir compte de l'importance des droits de la personne concernée résultant des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « charte »).À cet égard, il y a lieu de relever que l'article 8, paragraphe 1, de la charte énonce que « [t]oute personne a droit à la protection des données à caractère personnel la concernant ». Ce droit fondamental est étroitement lié au droit au respect de la vie privée consacré à l'article 7 de la charte (Affaires jointes C-92/09 et C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, point 47).

Selon la jurisprudence de la Cour, le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel, reconnu par les articles 7 et 8 de la charte, se rapporte à toute information concernant une personne physique identifiée ou identifiable (*Volker und Markus Schecke and Eifert*, point 52). Toutefois, il résulte des articles 8, paragraphe 2, et 52, paragraphe 1, de la charte que, sous certaines conditions, des limitations peuvent être apportées audit droit.

En outre, il incombe aux États membres, lors de la transposition de la Directive 95/46, de veiller à se fonder sur une interprétation de cette dernière qui leur permette d'assurer un juste équilibre entre les différents droits et libertés fondamentaux protégés par l'ordre juridique de l'Union (voir, par analogie, l'Affaire C-275/06 *Promusicae* [2008] ECR I-271, point 68).

S'agissant de la pondération nécessaire en vertu de l'article 7, sous f), de la Directive 95/46, il est possible de prendre en considération le fait que la gravité de l'atteinte aux droits fondamentaux de la personne concernée par ledit traitement peut varier en fonction du fait de savoir si les données en cause figurent déjà, ou non, dans des sources accessibles au public.

En effet, à la différence des traitements de données figurant dans des sources accessibles au public, les traitements de données figurant dans des sources qui ne sont pas accessibles au public impliquent nécessairement que des informations sur la vie privée de la personne concernée seront désormais connues par le responsable du traitement et, le cas échéant, par le ou les tiers auxquels les données sont communiquées. Cette atteinte plus grave aux droits de la personne concernée, consacrés aux articles 7 et 8 de la charte, doit être prise en compte à sa juste valeur en la mettant en balance avec l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées.

À cet égard, il convient de souligner que rien ne s'oppose à ce que, dans l'exercice de leur marge d'appréciation consacrée à l'article 5 de la Directive 95/46, les États membres établissent des principes directeurs pour ladite pondération.

Toutefois, il ne s'agit plus d'une précision au sens dudit Article 5 si une réglementation nationale exclut pour certaines catégories de données à caractère personnel la possibilité d'être traitées en prescrivant, pour ces catégories, de manière définitive le résultat de la pondération des droits et intérêts opposés, sans permettre un résultat différent en raison de circonstances particulières d'un cas concret.Dès lors, sans préjudice de l'article 8 de la directive 95/46 concernant des traitements portant sur des catégories particulières de données, disposition qui n'est pas en cause dans le litige au principal, l'article 7, sous f), de cette directive s'oppose à ce qu'un État membre exclue de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées, sans permettre une pondération des droits et intérêts opposés en cause dans un cas particulier

Au vu de ces considérations, il convient de répondre à la première question que l'Article 7, sous f), de la directive 95/46 doit être interprété en ce sens qu'il s'oppose à une réglementation nationale qui, en l'absence du consentement de la personne concernée et pour autoriser le traitement de ses données à caractère personnel nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable de ce traitement ou par le ou les tiers auxquels ces données sont communiquées, exige, outre le respect des droits et libertés fondamentaux de cette dernière, que lesdites données figurent dans des sources accessibles au public, excluant ainsi de façon catégorique et généralisée tout traitement de données ne figurant pas dans de telles sources.

La seconde question

Par sa seconde question, la juridiction de renvoi demande, en substance, si l'article 7, sous f), de la Directive 95/46 a un effet direct.

À cet égard, il y a lieu de rappeler que, selon une jurisprudence constante de la Cour, dans tous les cas où les dispositions d'une directive apparaissent, du point de vue de leur contenu, inconditionnelles et suffisamment précises, les particuliers sont fondés à les invoquer devant les juridictions nationales à l'encontre de l'État, soit lorsque celui-ci s'est abstenu de transposer dans les délais la directive en droit national, soit lorsqu'il en a fait une transposition incorrecte (voir l'Affaire C-203/10 *Auto Nikolovi* [2011] ECR I-0000, point 61 et jurisprudence citée).Force est de constater que l'Article 7, sous f), de la directive 95/46 est une disposition suffisamment précise pour être invoquée par un particulier et appliquée par les juridictions nationales. En outre, si la directive 95/46 comporte indéniablement, pour les États membres, une marge d'appréciation plus ou moins importante pour la mise en œuvre de certaines de ses dispositions, ledit Article 7, sous f), quant à lui, énonce une obligation inconditionnelle (voir, par analogie, arrêt Österreichischer Rundfunk e.a., précité, point 100).L'emploi de l'expression « à condition que » dans le texte même de l'article 7, sous f), de la Directive 95/46 n'est pas de nature, à lui seul, à remettre en cause le caractère inconditionnel de cette disposition, au sens de ladite jurisprudence.

En effet, cette expression vise à établir l'un des deux éléments cumulatifs prévus à l'article 7, sous f), de la directive 95/46 au respect desquels est subordonnée la possibilité de traiter des données à caractère personnel sans le consentement de la personne concernée. Cet élément étant défini, il n'enlève pas audit article 7, sous f), son caractère précis et inconditionnel.

Il convient donc de répondre à la seconde question que l'article 7, sous f), de la Directive 95/46 a un effet direct.

3.3. CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

A. Résumé des activités et actualités

Au cours de l'année 2011, le CEPD a fixé de nouveaux points de repère dans différents domaines d'activité. En matière de **supervision des institutions et organismes européens** dans le cadre du traitement de données personnelles, le CEPD a interagi avec un plus grand nombre de délégués à la protection des données dans un nombre d'institutions et d'organismes le plus important à ce jour. Le CEPD a par ailleurs pu observer les effets de sa nouvelle **politique d'application** : la plupart des institutions et organismes européens affichent de bons progrès dans le respect du Règlement sur la protection des données, même si certains devraient intensifier leurs efforts.

Dans le cadre de sa fonction de consultation sur les propositions de nouvelles législations, le CEPD a émis un nombre record d'avis sur différents sujets. Le plus important est **l'examen du cadre juridique européen pour la protection des données**, qui reste l'une des priorités. Toutefois, la mise en œuvre du **programme de Stockholm** dans le domaine de la liberté, de la sécurité et de la justice, et de l'**Agenda numérique**, en tant que pierre angulaire de la stratégie Europe 2020, a également eu un impact sur la protection des données. Il est possible d'en dire autant des questions de marché intérieur, de santé publique, d'affaires des consommateurs et d'application dans un contexte transfrontalier.

En même temps, le CEPD a augmenté la **coopération** avec d'autres autorités de contrôle et amélioré l'efficacité de son **organisation** et de sa **communication**.

En 2012, les principales priorités du CEPD comprenaient, notamment:

- **La sensibilisation** : le CEPD investira du temps et des ressources pour conseiller les institutions et les agences européennes sous forme de lignes directrices, de formations et d'ateliers thématiques, et de développement d'une section du site web du CEPD dédiée aux délégués à la protection des données (DPD).

- **La définition de procédures** de gestion des notifications liées aux procédures administratives standard ou aux opérations de traitement déjà déployées.

- Un exercice pour déterminer l'état des lieux pour les DPD au sein des institutions et organismes européens afin d'apporter une **assistance à la fonction de DPD** conforme aux principes de responsabilité.

- **Des visites et contrôles** des institutions et agences, à des fins non seulement d'application, mais également de sensibilisation aux questions de protection des données et au rôle du CEPD.

- En ses capacités de conseiller, le CEPD privilégiera en 2012 le travail en cours sur le **cadre juridique pour la protection des données en Europe**.

- **Les développements technologiques**, surtout liés à Internet et aux politiques associées, représentent un autre enjeu, qui implique des projets de cadre paneuropéen pour l'identification, l'authentification et la signature électroniques, la question du contrôle d'Internet (application des droits IP et procédures de retrait, par exemple), les services informatiques en nuage et la cybersanté. Le CEPD renforcera également son expertise technologique et participera aux recherches sur les technologies d'amélioration du respect de la vie privée.

- De plus amples développements dans les **domaines de la liberté, de la sécurité et de la justice** (cf. SSFT européen, frontières intelligentes) et de la réforme du secteur financier, dans la mesure où

ils affectent le droit à la protection des données et de la vie privée, continueront d'être suivis et surveillés par le CEPD.

- Le CEPD continuera également de respecter ses responsabilités dans le domaine d'une **supervision coordonnée** et de s'ouvrir aux autorités nationales en charge de la protection des données et aux organisations internationales à des fins de sensibilisation et de partage des bonnes pratiques.

Organisation	Contrôleur européen de la protection des données (CEPD)
Président et/ou collège	Peter Hustinx, Contrôleur Giovanni Buttarelli, Contrôleur adjoint
Budget	7 564 137 EUR
Personnel	52 membres du personnel (dont 37 fonctionnaires européens)
Activités générales	
Décisions, avis, recommandations	**24 avis législatifs** portant notamment sur, les initiatives liées aux domaines de la liberté, de la sécurité et de la justice, aux développements technologiques, à la coopération internationale, aux transferts de données ou au marché interne. **12 séries d'observations formelles** notamment sur, les droits de propriété intellectuelle, la sécurité dans l'aviation civile, les politiques pénales de l'UE, le système de surveillance du financement du terrorisme, l'efficience énergétique ou le programme « Droits fondamentaux et citoyenneté ».
Notifications	**164 notifications** d'opérations de traitement présentant des risques spécifiques reçues de la part de délégués à la protection des données auprès des institutions et organes de l'UE à des fins d'examen préalable
Examens préalables	**71 avis d'examens préalables adoptés**, concernant, notamment, les données de santé, l'évaluation du personnel, le recrutement, les suspicions et les délits, et la surveillance en ligne.
Demandes émanant des personnes concernées	**196 demandes d'informations ou de conseils** reçues par écrit de la part du grand public, principalement sur la vie privée en ligne, les transferts internationaux de données, le cadre européen pour la protection des données et la conservation des données.
Plaintes émanant des personnes concernées	**107 plaintes reçues, dont 26 recevables** Principaux types de violations alléguées : accès aux données et rectification de ces dernières, objection et suppression, violation

	de la confidentialité des données, collecte excessive et perte de données.
Conseils sollicités par le Parlement ou le gouvernement	Parmi les 24 avis législatifs susmentionnés, **20** ont été publiés à la demande de la Commission européenne (Article 28(2) du Règlement (CE) n° 45/2001).
Autres renseignements relatifs aux activités générales	**34 consultations sur des mesures administratives** liées au traitement de données à caractère personnel dans l'administration de l'UE. Des conseils ont été prodigués sur de nombreux aspects juridiques liés au traitement des données personnelles par les institutions et les organes de l'UE.
Activités d'inspection	
Contrôles, enquêtes	**4 contrôles sur place** au sein du CEDEFOP, de l'OLAF et de la BCE **Suivi** des recommandations faites lors des contrôles précédents **Audit de sécurité** du Système d'information des visas (VIS)
Activités de sanction	
Sanctions	s. o.
Amendes	**Contrôle de la mise en œuvre du Règlement (CE) n° 45/2001** : le troisième exercice d'évaluation a donné lieu à un rapport soulignant les progrès des institutions et des organismes dans la mise en œuvre du Règlement et soulignant également les lacunes. Des visites d'une journée ont été organisées auprès de l'Agence ferroviaire européenne, de l'Office communautaire des variétés végétales, de la Fondation européenne pour l'amélioration des conditions de vie et de travail et de l'Agence du système mondial de navigation par satellite européen (Agence du GNSS européen).
DPD	
Chiffres relatifs aux DPD	54 DPD dans les institutions et organes de l'UE.

B. Informations sur la jurisprudence

Participation du CEPD aux poursuites judiciaires

Dans l'affaire V. c/ Parlement européen (Affaire F-46/09), le CEPD a été invité à intervenir par le Tribunal de la fonction publique. L'affaire concernait le transfert supposément illégal de données médicales entre les services médicaux de la Commission et le Parlement européen. Le CEPD a plaidé en faveur de la partie demanderesse, arguant que le transfert était contraire aux règles de protection des données, puisqu'il n'était pas nécessaire et n'avait aucune base légale appropriée. Dans son jugement du 5 juillet 2011, le Tribunal de la fonction publique a donné raison à la partie demanderesse, conformément au raisonnement du CEPD.

Dans son arrêt du 7 juillet 2011, Valero Jordana c/ Commission (Affaire T-161/04), la Cour générale a considéré que la Commission avait eu tort de ne pas évaluer la demande d'accès public à certaines données personnelles en vertu des règles de protection des données. Cette conclusion était conforme aux observations du CEPD utilisées par la Cour dans son argument.

Dans son jugement du 23 novembre 2011, Dennekamp c/ Parlement européen (Affaire T-82/09), le tribunal a conclu que la partie demanderesse, un journaliste demandant les noms des membres du Parlement européen qui participaient à un régime de pension complémentaire, n'avait pas démontré la nécessité de rendre ces données publiques. Le CEPD avait défendu le point de vue opposé, considérant qu'un équilibre entre les différents intérêts en jeu aurait dû donner lieu à la divulgation de ces données au journaliste.

Le Tribunal n'a pas encore rendu son verdict dans l'affaire Egan & Hackett c/ Parlement européen (Affaire T-190/10). Cette affaire concerne une demande d'accès aux noms des assistants des membres du Parlement européen.

Le CEPD est également intervenu dans l'affaire Commission c/ Autriche (Affaire C-614/10), une procédure d'infraction à l'encontre de l'Autriche sur l'absence d'indépendance de l'autorité autrichienne de protection des données. Le CEPD a soumis un mémoire en intervention soutenant la conclusion de la Commission selon laquelle la manière dont l'autorité autrichienne de protection des données est incorporée à la structure institutionnelle de l'Autriche n'assure pas suffisamment son indépendance.

Enfin, l'ENISA a fait appel d'une décision du CEPD devant le tribunal suite à une plainte (Affaire T-345/11). La demande a été déclarée manifestement irrecevable pour des raisons de procédure.

Jurisprudence de la protection des données

Dans l'affaire Deutsche Telekom C-543/09, la question s'est posée de savoir si, en vertu de la directive « Vie privée et communications électroniques », une entreprise attribuant des numéros de téléphone à ses abonnés pouvait communiquer des données sur ces derniers à d'autres entreprises dont les activités consistent à fournir des services d'annuaires publiquement disponibles sans obtenir le consentement renouvelé des personnes concernées. La Cour a considéré dans son jugement du 5 mai 2011 que, dans la mesure où les abonnés étaient déjà correctement informés de cette possibilité, leur consentement n'avait pas à être renouvelé.

Dans son jugement de l'affaire ASNEF et FECEMD du 24 novembre 2011 (Affaires jointes C-648/10 et C-469/10), la Cour de Justice a répondu à un tribunal espagnol qui avait demandé un éclaircissement sur une disposition de la directive relative à la protection des données qui permet le traitement de données à caractère personnel si ce dernier est nécessaire à la réalisation d'un intérêt légitime supérieur à l'intérêt de

la personne concernée. En droit espagnol, ce traitement n'est possible qu'au regard de données personnelles qui ont déjà été rendues publiques. D'après la Cour, cette restriction nationale n'est pas conforme à la directive, qui a un effet direct sur ce point.

Le 24 novembre 2011, la Cour de Justice a statué sur une question posée à titre préjudiciel dans le cadre d'une affaire belge concernant l'obligation d'un prestataire de services Internet (Scarlet Extended) de contrôler le comportement de ses clients sur Internet afin de prévenir les violations des droits de propriété intellectuelle (Affaire C-70/10). La Cour a conclu que cette obligation correspondait à une obligation de contrôle général, laquelle est interdite au regard des règles européennes sur le commerce en ligne. La Cour a également noté que ce type d'obligation ne permettait pas un juste équilibre entre l'application des droits de propriété intellectuelle et plusieurs droits et libertés fondamentaux définis par la Charte des droits fondamentaux, parmi lesquels figure le droit à la protection des données.

Chapitre quatre

Principaux développements dans les pays de l'EEE

ISLANDE

A. Résumé des activités et actualités

L'une des principales questions traitées en 2011 concernait le traitement de données personnelles en relation avec des rapports anonymes adressés aux autorités administratives signalant des infractions alléguées à la loi. Sur les sites web de la Direction du travail et de la Direction des impôts, les citoyens avaient la possibilité de signaler de manière anonyme leurs suspicions d'évasion fiscale et autres délits similaires. La DPA a décidé d'enquêter sur la licéité du traitement des données personnelles liées à ces signalements anonymes. Le résultat de cette enquête a été publié dans des décisions destinées aux autorités en question, selon lesquelles l'utilisation de formulaires à des fins de signalements anonymes, notamment, entraînait la collecte de données personnelles inexactes. La DPA a en outre considéré que les garanties données aux auteurs des signalements quant à leur anonymat étaient peu fiables, puisque les technologies de télécommunication offrent la possibilité de remonter la trace des signalements jusqu'à ceux qui les ont envoyés, par exemple en cas d'enquête de la police sur de fausses accusations. Bien qu'une autorité administrative ne puisse jamais prévenir complètement l'envoi de signalements anonymes par les citoyens, elle devrait, à la lumière de ce qui précède, ne pas leur donner explicitement l'opportunité de lui adresser des signalements de cette manière. La DPA en est par conséquent arrivée à la conclusion que les formulaires de ces signalements sur les sites web des autorités en question étaient incompatibles avec la loi sur la protection des données.

Un autre problème important concernait un projet de proposition de nouvelle constitution pour l'Islande, présentée par le Conseil constitutionnel national, formé suite aux élections nationales de 2010. Le projet de proposition contenait une disposition sur le droit à la vie privée identique à la disposition sur ce même droit dans la constitution existante, qui date de 1944. Dans un avis sur ce projet de proposition, la DPA a attiré l'attention sur des dispositions de récentes constitutions et chartes des droits de l'homme, dont la Charte des droits fondamentaux de l'UE, qui garantit spécifiquement le droit à la protection des données personnelles. La DPA a invité l'Assemblée constituante nationale à ajouter une déclaration à cet effet dans son projet de proposition. La DPA a par ailleurs souligné qu'une disposition du projet de proposition, selon laquelle chacun aurait le droit de collecter et de diffuser des informations, devait être envisagée avec circonspection, dans la mesure où la libre collecte de données personnelles n'est autorisée dans aucun pays occidental.

Plusieurs actes législatifs ont été adoptés en 2011 contenant des dispositions sur le traitement des données à caractère personnel. Le plus important d'entre eux est la Loi n° 68/2011 sur les commissions d'enquête. D'après cette loi, le Parlement peut désigner des commissions pour enquêter sur des sujets spécifiques. Ces commissions ont, d'après la loi, des pouvoirs étendus, dont celui de traiter des données à caractère personnel. En 2008, une loi sur ce type de commissions a été adoptée, la Loi n° 142/2008 relative à l'investigation des événements et des causes qui ont mené à la faillite des banques islandaises en 2008, et des événements connexes. Les dispositions de la Loi n° 68/2011 sont cohérentes avec celles de la loi précédente, dont une description se trouve au chapitre sur l'Islande dans le 12e Rapport annuel du groupe de travail « Article 29 ».

Organisation	
Président et/ou collège	Sigrún Jóhannesdóttir, Commissaire ; Páll Hreinsson, Président du Conseil d'administration jusqu'en novembre 2011, date à laquelle Björg Thorarensen est devenu Président.

Budget	69 millions d'ISK (environ 434 000 EUR, selon le taux de change au 31 décembre 2011)
Personnel	Cinq conseillers juridiques, un secrétaire.
Activités générales	
Décisions, avis, recommandations	Environ 100
Notifications	470
Examens préalables	110 autorisations de traitement accordées
Demandes émanant des personnes concernées	Environ 400
Plaintes émanant des personnes concernées	139
Conseils sollicités par le Parlement ou le gouvernement	Environ 50
Autres renseignements relatifs aux activités générales	Au total, 1 397 nouvelles affaires ont été enregistrées en 2011.
Activités d'inspection	
Contrôles, enquêtes	14
Activités de sanction	
Sanctions	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.
Amendes	Aucune amende journalière n'a été imposée en 2011.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Le 20 octobre 2011, la Cour suprême d'Islande a rendu un arrêt (Affaire n° 706/2010) concernant la publication d'un rapport sur un accident de la route fatal. Dans ce rapport, le Groupe d'analyse des accidents décrit ses conclusions sur les causes de cet accident, dans lequel le conducteur a trouvé la mort. Le partenaire survivant du conducteur a déposé une plainte dans laquelle il présentait une demande d'indemnisation pour le préjudice personnel que lui avait fait subir la publication du rapport du Groupe, le nom du conducteur pouvant être aisément déduit à partir du rapport même s'il n'avait pas été publié.

Cette affaire avait déjà été traitée par la DPA, qui avait considéré que le conducteur était personnellement identifiable, et que la publication du rapport équivalait donc au traitement de données personnelles. Toutefois, à la lumière de dispositions légales très claires sur l'obligation de publier les rapports du Groupe, et parce que le Groupe n'avait pas publié plus d'informations dans le rapport que ce que l'on pouvait considérer comme nécessaire, la DPA n'avait pas conclu à une violation de la loi sur la protection des données. La Cour de district de Reykjavik et la Cour suprême sont toutes deux arrivées à une conclusion similaire, à savoir que le Groupe était légalement tenu de publier son rapport et que les informations rendues publiques n'enfreignaient aucun droit. Par conséquent, la demande d'indemnisation du plaignant a été rejetée.

LIECHTENSTEIN

A. Résumé des activités et actualités

Loi relative à un Registre personnel central

Un registre maintenu par les gouvernements régionaux (des États fédéraux) pendant des années contient de nombreux détails sur l'ensemble des habitants de chaque État. Pendant des années, le Bureau de la protection des données a appelé à l'adoption d'une base légale pour cette importante base de données. Cet appel a reçu une réponse en 2011. Une loi a finalement été passée, qui réglemente également le processus de révision des droits d'accès de chaque autorité. Certaines corrections techniques doivent être apportées à la base de données afin de garantir, notamment, le caractère approprié de ces droits d'accès.

Schengen

L'évaluation de la protection des données a été exécutée en 2011. Le Bureau de la protection des données du Liechtenstein (DSS) a été audité sur son respect des différents aspects, tels que l'indépendance, la structure, les tâches et les compétences légales, ainsi que les droits des personnes concernées. Le résultat de cet audit a été positif. Le Liechtenstein fait partie de l'espace Schengen depuis décembre 2011. En raison d'une pénurie de ressources, toutefois, il lui est difficile de participer aux réunions du Comité mixte de Schengen. Une augmentation des ressources du DSS a été demandée lors de l'évaluation. Celle-ci n'est toutefois pas d'actualité.

Travail de relations publiques

À l'occasion de la Journée européenne de la protection des données, le DSS et l'Institut des systèmes d'information de l'Université du Liechtenstein ont invité le public à l'événement « *Schau mal, wer da spricht: Was Handys, Notebooks & Co alles erzählen* », sur le traitement des données de nos différents appareils mobiles. De nos jours, il est devenu impossible de se passer de nos téléphones mobiles, ordinateurs portables et tablettes. Grâce aux appareils compacts et à la rapidité des réseaux sans fil, nous pouvons communiquer et travailler où que nous soyons. Cet événement portait donc essentiellement sur le traitement des données par les appareils mobiles.

À l'invitation de l'Université privée de la Principauté du Liechtenstein, nous avons participé à une table ronde sur « l'accès de l'État aux données privées : la question de la conservation des données ». Alors que la conservation des données a été abolie en Allemagne par le Tribunal constitutionnel fédéral et n'a pas encore été introduite en Autriche, au Liechtenstein, les données relatives aux déplacements et à la localisation de toutes les personnes sont enregistrées chaque fois qu'elles utilisent leur téléphone ou Internet. Le Contrôleur européen de la protection des données décrit cet empiètement considérable sur le droit à la vie privée de chaque citoyen comme la mesure la plus envahissante jamais prise dans l'UE en termes d'intrusion dans la sphère privée.[19] Les avantages et inconvénients de ce type de conservation ont fait l'objet de discussions.

À l'occasion de la Journée de mise en réseau, à l'Université du Liechtenstein, nous avons été conviés à une table ronde sur « l'informatique en nuage » *(Cloud Computing)*.

19 Cf. Communiqué de presse de janvier 2011 : « Le CEPD considère que la directive constitue l'instrument le plus intrusif pour la vie privée jamais adopté par l'UE en termes d'échelle et du nombre de personnes concernées » : https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_27_FR.pdf et Rapport annuel 2010.

En 2009, il est devenu possible de désigner un fonctionnaire ou responsable de la protection des données d'une société en remplacement de l'obligation de rendre compte des activités de collecte des données. Afin de créer des synergies dans un domaine somme toute relativement récent, nous avons invité les responsables existants et les parties intéressées à partager leurs idées sur le sujet des « Tâches et position d'un responsable de la protection des données ».

Le site web du DSS est la principale source d'informations du public.[20] Des information sur *l'informatique en nuage* et *l'externalisation* en général y ont notamment été publiées, , ainsi qu'une recommandation de mise en œuvre de *mesures techniques et organisationnelles de garantie de la sécurité des données*.

Organisation	
Président et/ou collège	Dr Philipp Mittelberger
Budget	682 000,-- CHF
Personnel	2,2 ETP de juristes ; 1,0 ETP d'agent technique ; 0,8 ETP d'agent administratif
Activités générales	
Décisions, avis, recommandations	11 autorisations relatives à des installations de vidéosurveillance
Notifications	s. o. ; très peu de nouvelles notifications
Examens préalables	s. o.
Demandes émanant des personnes concernées	64
Plaintes émanant des personnes concernées	s. o.
Conseils sollicités par le Parlement ou le gouvernement	24 avis sur des projets de lois[21]
Autres renseignements relatifs aux activités générales	559 demandes[22]
Activités d'inspection	
Contrôles, enquêtes	Divers contrôles en préparation
Activités de sanction	
Sanctions	s. o.
Amendes	s. o.

20 http://www.dss.llv.li/
21 Voir le rapport d'activités 2011 du DSS, chapitre 3., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2011.pdf.
22 Voir les statistiques du DSS reprises dans le rapport d'activités 2011 du DSS, chapitre 8.1., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2011.pdf.

DPD	
Chiffres relatifs aux DPD	25 délégués à la protection des données désignés à la fin 2011

B. Informations sur la jurisprudence

La Commission de la protection des données n'a publié aucune décision en 2011. La raison en est peut-être l'incertitude quant à savoir si et dans quelle mesure le droit de recours prévu à l'Article 34(b) de la Loi relative à la protection des données est réellement mis en pratique.

Dans une affaire portée devant la Cour d'État (Tribunal constitutionnel), le droit à l'information concernant l'époux décédé a été affirmé. La base légale de ce recours a été l'Article 1(7) du Règlement sur la protection des données. En connexion avec le droit à l'information, cette disposition établit ce qui suit : « *Si des informations sur des personnes décédées sont demandées, celles-ci seront communiquées si la partie demanderesse démontre un intérêt légitime pour les informations et s'il n'existe aucun intérêt supérieur de proches de la personne décédée ou de tiers susceptible d'empêcher cette divulgation. Les liens étroits de parenté, de mariage ou de partenariat enregistré avec la personne décédée constituent des intérêts légitimes.* »

La Cour d'État a déclaré à titre liminaire que la protection des données et la protection de « l'intégrité informationnelle » sont des aspects partiels de la protection de la vie privée prévue par l'Article 32 de la Constitution du Liechtenstein et l'Article 8 de la Convention européenne des droits de l'homme.

Dans le cas présent, la Cour a décidé que cette disposition ne constitue pas un droit d'information distinct mais doit être interprétée comme établissant un droit d'accès aux documents en vertu du droit procédural. Le droit à l'information concerne les propres données personnelles d'un individu, ce qui n'est pas le cas de la disposition du Règlement. Il s'agit donc d'une question cruciale en matière de protection des données, qui doit être réglementée par une loi. La disposition doit par conséquent être interprétée de manière restrictive et constitue uniquement (néanmoins) un intérêt digne d'être protégé en matière d'accès aux données dans le cadre de procédures effectives (StGH 2011/11).

NORVÈGE

A. Résumé des activités et actualités

Stratégie de la DPA dans le secteur de la santé.

Depuis 2010, il existe un programme interne de travail sur les stratégies. À l'automne 2011, la « stratégie de données pour de meilleures politiques dans le secteur de la santé » a été lancée. L'Inspection a établi des objectifs à long terme concernant la manière dont l'agence contribuera à l'amélioration des politiques dans le secteur de la santé. Cette stratégie comprend un travail sur le contrôle des accès (opérations internes et accès global), la modernisation et la coordination des dossiers médicaux (dossiers médicaux centraux et autres dossiers de qualité), ainsi qu'une évaluation de la manière dont l'Autorité peut garantir l'autodétermination et l'autonomie des peuples. La stratégie prévoit également la manière dont l'agence travaillera sur les dossiers de qualité locaux, avec le département et la Direction de la santé et autres intervenants majeurs du secteur de la santé.

Organisation	Autorité norvégienne de protection des données
Président et/ou collège	Directeur Bjørn Erik Thon
Budget	32 millions de NOK
Personnel	40 au total, directeur : 1, juridique : 16, inspection et sécurité : 9, Département des informations : 4, administration et archives : 10.
Activités générales	
Décisions, avis, recommandations	
Notifications	Nouvelles en 2011 : 4 010, total : 11 211 fin 2011.
Examens préalables	Total en 2011 : 143
Demandes émanant des personnes concernées	Au total, la DPA norvégienne a reçu 5 196 appels téléphoniques et 2 632 courriels adressés à nos services de première ligne.
Plaintes émanant des personnes concernées	s. o.
Conseils sollicités par le Parlement ou le gouvernement	s. o.
Autres renseignements relatifs aux activités générales	s. o.
Activités d'inspection	

Contrôles, enquêtes	Adresse Médiation 1 Travail 3 Cartes de clients 5 Assurance 4 Recherche 2 Sociétés Internet 4 Vidéosurveillance 9 Services sociaux nationaux 4 Webémissions 5 Éducation 1 TOTAL 38
Activités de sanction	
Sanctions	4 frais de pénalité et une amende coercitive, tous imposés par la DPA
Amendes	Frais de pénalité de 135 000 NOK au total, amendes coercitives de 380 000 NOK
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Cartographie de Facebook

En décembre 2010, nous avons lancé le rapport Services de réseaux sociaux et vie privée – une étude de cas de Facebook. Le rapport montrait que les informations que les utilisateurs fournissent sur eux-mêmes ne représentaient qu'une petite partie de la quantité totale d'informations collectées par Facebook. Le même rapport révélait plusieurs ambiguïtés relatives à la collecte et à l'utilisation d'informations à caractère personnel par Facebook. Sur cette base, les DPA nordiques ont adressé, à l'initiative de l'Inspection norvégienne des données, plusieurs questions spécifiques à Facebook sur l'identité des personnes qui collectent et ont accès aux informations via Facebook, ainsi que sur ce qu'il advient des informations personnelles collectées.

Directive sur la conservation des données

Le Parlement norvégien a transposé la Directive sur la conservation des données dans le droit norvégien en avril 2011. Cette directive sera mise en œuvre dans le cadre de la réglementation en matière de communications électroniques, de la Loi de procédure pénale et des Règlements sur les données personnelles.

La DPA sera chargée de plusieurs nouvelles responsabilités en relation avec la directive, y compris des responsabilités de supervision liées à l'obligation de supprimer les données et de préparer des licences avec des exigences de sécurité. La DPA s'est fortement opposée à la directive, mais a pris note de la

décision du Parlement et a travaillé en collaboration avec l'Autorité norvégienne des postes et télécommunications afin d'assurer la meilleure mise en œuvre possible. La directive n'était pas entrée en vigueur à la fin de l'année.

Rapport sur les applications

En septembre 2011, la DPA a publié le rapport « Que sait cette application sur vous ? Défis liés à la protection de la vie privée et aux applications mobiles ». Les applications mobiles, également appelées « applis », connaissent une croissance rapide. La raison pour laquelle l'audit s'est penché sur ce marché est que de nombreuses applications gèrent d'importants volumes de données personnelles, souvent sans que l'utilisateur en ait même conscience. Certaines applications requièrent l'accès à des informations personnelles qui peuvent révéler de nombreuses informations concernant l'utilisateur, telles que les endroits où il s'est rendu, des informations sur son réseau d'amis et ses intérêts.

L'affaire RMI

En 2010, la DPA a enquêté sur l'Institut de médecine légale (RMI) de l'Université d'Oslo. Cette enquête a montré que, de par ses activités, le département stocke de grandes quantités de données sensibles sans motif légal adéquat, que ce soit en vertu de la loi ou d'un contrat conclu avec chaque client. La DPA a également observé d'importantes déficiences au niveau de la sécurité des informations et s'est aperçue que l'université en général n'assurait qu'un niveau de protection médiocre aux informations stockées. Dans l'année, la DPA a annoncé qu'elle déciderait que les informations devraient être supprimées.

« Nettby »

En décembre 2010, le journal norvégien VG a décidé la fermeture de son site de réseau social « Nettby », qui représentait la plus grande communauté en ligne de son époque et sur lequel d'importants volumes d'informations étaient enregistrés, notamment des communications privées. Après sa fermeture, toutes les informations présentes sur le site de VG étaient inaccessibles à ses anciens utilisateurs comme au grand public. VG et la Bibliothèque nationale estimaient que ces informations devaient être préservées pour l'avenir parce qu'elles reflétaient une époque susceptible d'intéresser de futures recherches. L'objectif original de Nettby, toutefois, avait été de permettre à ses membres de participer à une communauté en ligne, et de leur offrir la possibilité d'interactions privées entre eux. C'est pourquoi la DPA a imposé la suppression de ces données.

Norme sectorielle pour les billetteries électroniques

À l'initiative de sociétés de transport public, la DPA a participé à un projet collaboratif sur des solutions respectueuses de la vie privée pour la télébillettique et le développement d'une norme sectorielle. Une norme sectorielle pour la billetterie électronique contribuera à s'assurer que chacun peut voyager de manière anonyme en bus, en train et en bateau, et engage le secteur à proposer des billets électroniques respectant la vie privée des voyageurs. Tout utilisateur devrait être en mesure d'utiliser les transports publics sans avoir à divulguer son identité ni sa destination, et néanmoins bénéficier des mêmes avantages et services que les navetteurs qui choisissent de signer des contrats personnels avec une compagnie de transport. Le Code a été lancé en décembre 2011.

Normes de contrôle douanier pour les personnes physiques

Les Douanes royales avaient instauré une pratique en vertu de laquelle les informations concernant les transactions en devises étrangères effectuées par des particuliers étaient retirées du registre, stockées et enregistrées par courrier. Les personnes concernées étaient tenues de présenter des documents relatifs aux transactions en question et de signaler, le cas échéant, leur rapport avec le domaine des douanes. La DPA a jugé qu'il s'agissait d'investigations sur des personnes réalisées sans autorité légale, et a ordonné aux services des douanes de mettre fin à cette pratique.

Chapitre cinq

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

MEMBRES DU GROUPE DE TRAVAIL ART. 29 SUR LA PROTECTION DES DONNÉES EN 2011

Allemagne	Autriche
M. Peter Schaar Commissaire fédéral à la protection des données et au 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 Adresse électronique : poststelle@bfdi.bund.de Site web : http://www.datenschutz.bund.de M. Alexander Dix (représentant les États allemands / Bundesländer) Commissaire à la protection des données et à l'accès à l'information du Land 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 Adresse électronique : mailbox@datenschutz-berlin.de Site web : http://www.datenschutz-berlin.de	Mme Eva Souhrada-Kirchmayer (depuis 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 Adresse électronique : dsk@dsk.gv.at Site web : http://www.dsk.gv.at/

Belgique	Bulgarie
M. Willem Debeuckelaere Commission de la protection de la vie privée (Commission for the protection of privacy / 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 Adresse électronique : commission@privacycommission.be Site web : http://www.privacycommission.be/	M. Krassimir Dimitrov Commission de protection des données à caractère personnel – CPDP (Комисия за защита на личните данни) 15 Acad. Ivan Evstratiev Geshov blvd. Sofia 1431 République de Bulgarie Tél. : + 359 2 915 35 31 Fax : + 359 2 915 35 25 Adresse électronique : kzld@cpdp.bg Site web : http://www.cdpd.bg
Chypre	**Danemark**
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 Adresse électronique : commissioner@dataprotection.gov.cy Site web : http://www.dataprotection.gov.cy	Mme Janni Christoffersen Agence danoise de protection des données (Datatilsynet) Borgergade 28, 5th floor - DK - 1300 Koebenhavn K Tél. : +45 3319 3200 Fax : +45 3319 3218 Adresse électronique : dt@datatilsynet.dk Site web : http://www.datatilsynet.dk
Espagne	**Estonie**
M. José Luis Rodriguez Álvarez Agence espagnole de protection des données (Agencia Española de Protección de Datos)	M. Viljar Peep Inspection estonienne de la protection des données (Andmekaitse Inspektsioon)

C/ Jorge Juan, 6 ES - 28001 Madrid Tél. : +34 91 399 6219/20 Fax : +34 91 445 56 99 Adresse électronique : director@agpd.es Site web : http://www.agpd.es	19 Väike-Ameerika St., 10129 Tallinn Tél. : +372 627 4135 Fax : +372 627 4137 Adresse électronique : info@]aki.ee ou international@aki.ee Site web : http://www.aki.ee
Finlande	**Grèce**
M. Reijo Aarnio Bureau du 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 Adresse électronique : tietosuoja@om.fi Site web : http://www.tietosuoja.fi	M. Christos Yeraris Autorité hellénique de protection des données (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 Athènes - Grèce Tél. : +30 210 6475608 Fax : +30 210 6475789 Adresse électronique : christosyeraris@dpa.gr Site web : http://www.dpa.gr
Hongrie	**Irlande**
M. András Jóri Commissaire parlementaire à la protection des données et à la liberté d'information de la Hongrie (Adatvédelmi Biztos) Nador u. 22 - HU - 1051 Budapest Tél. :+36 1 475 7186 Fax : +36 1 269 3541 Adresse électronique : adatved@obh.hu Site web : www.adatvedelmibiztos.hu	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 Adresse électronique : info@dataprotection.ie Site web : http://www.dataprotection.ie

Italie	Lettonie
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 Adresse électronique : garante@garanteprivacy.it, f.pizzetti@garanteprivacy.it Site web : http://www.garanteprivacy.it	Mme Signe Plumina Inspection nationale des données de Lettonie (Datu valsts inspekcija) Blaumana street 11/13-15 Riga, LV-1011 Lettonie Adresse électronique : info@dvi.gov.lv Site web: www.dvi.gov.lv Tél. : + 371 67223131
Lituanie	**Luxembourg**
M. Algirdas Kunčinas Inspection nationale de la 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 Adresse électronique : ada@ada.lt Site web : http://www.ada.lt	M. Gérard Lommel Commission nationale pour la protection des données (CNPD) (National Commission for Data Protection) 41, avenue de la Gare - L - 1611 Luxembourg Tél. : +352 26 10 60 -1 Fax : +352 26 10 60 – 29 Adresse électronique : info@cnpd.lu Site web : http://www.cnpd.lu
Malte	**Pays-Bas**
M. Joseph Ebejer Commissaire à la protection des données et de l'information Bureau du Commissaire à la protection des données et de l'information 2, Airways House	M. Jacob Kohnstamm Autorité néerlandaise de protection des données (College Bescherming Persoonsgegevens - CBP) Adresse physique (sur rendez-vous uniquement) : Juliana van Stolberglaan 4-10

High Street Sliema SLM 1549 Malte Tél. : +356 2328 7100 Fax : +356 23287198 Adresse électronique : joseph.ebejer@gov.mt Site web : http://www.idpc.gov.mt	2595 CL DEN HAAG Adresse postale : P.O. Box 93374 2509 AJ DEN HAAG Tél. : +31 70 8888500 Fax : +31 70 8888501 Adresse électronique : info@cbpweb.nl Site web : http:// www.cbpweb.nl http://www.mijnprivacy.nl
Pologne	**Portugal**
M. Wojciech Rafał Wiewiórowski Inspecteur général pour la protection des données personnelles (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 Adresse électronique : desiwm@giodo.gov.pl Site web : http://www.giodo.gov.pl	M. Luís Novais Lingnau da Silveira Commission nationale de la 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 Adresse électronique : geral@cnpd.pt Site web : http://www.cnpd.pt
République tchèque	**Roumanie**
M. Igor Nemec Bureau de la protection des données à caractère personnel (Úřad pro ochranu osobních údajů) Pplk. Sochora 27 - CZ - 170 00 Praha 7 Tél. : +420 234 665 111 Fax : +420 234 665 501 Adresse électronique : posta@uoou.cz	Mme Georgeta Basarabescu Autorité nationale de contrôle du traitement des données à caractère personnel (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Olari Street no. 32, Sector 2, RO - Bucharest Tél. : +40 21 252 5599 Fax : +40 21 252 5757 Adresse électronique :

Site web : http://www.uoou.cz/	georgeta.basarabescu@dataprotection.ro international@dataprotection.ro Site web : www.dataprotection.ro
Royaume-Uni	**Slovaquie**
M. Christopher Graham Bureau du Commissaire à l'information Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tél. : +44 1625 545700 Fax : +44 1625 524510 Adresse électronique : veuillez compléter le formulaire de demande sur notre site web Site web : http://www.ico.gov.uk	M. Gyula Veszelei 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 Adresse électronique : statny.dozor@pdp.gov.sk Site web : http://www.dataprotection.gov.sk
Slovénie	**Suède**
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 Adresse électronique : gp.ip@ip-rs.si Site web : http://www.ip-rs.si rs.si	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 Adresse électronique : datainspektionen@datainspektionen.se, goran.graslund@datainspektionen.se Site web : http://www.datainspektionen.se
Contrôleur européen de la protection des données	
M. Peter Hustinx Contrôleur européen de la protection des données – CEPD	

Adresse postale : 60, rue Wiertz, BE - 1047 Bruxelles Bureau : 63, rue Montoyer, BE - 1047 Bruxelles Tél. : +32 2 283 1900 Fax : +32 2 283 1950 Adresse électronique : edps@edps.europa.eu Site web : http://www.edps.europa.eu	

OBSERVATEURS DU GROUPE DE TRAVAIL ART. 29 SUR LA PROTECTION DES DONNÉES EN 2011

Ancienne République yougoslave de Macédoine	Islande
M. Dimitar Gjeorgjievski Direction pour la protection des données personnelles (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tél. : +389 2 3230 635 Fax : +389 2 3230 635 Adresse électronique : info@dzlp.mk Site web : www.dzlp.mk	Mme Sigrun Johannesdottir Autorité de protection des données (Persónuvernd) Raudararstigur 10 - IS - 105 Reykjavik Tél. : +354 510 9600 Fax : +354 510 9606 Adresse électronique : postur@personuvernd.is Site web : http://www.personuvernd.is
Liechtenstein	**Norvège**
M. Philipp Mittelberger Commissaire à la protection des données Bureau de la protection des données (Datenschutzstelle, DSS) Kirchstrasse 8, Postfach 684 – FL -9490 Vaduz Tél. : +423 236 6090 Fax : +423 236 6099 Adresse électronique : info@dss.llv.li Site web : http://www.dss.llv.li	Kim Ellertsen Directeur, Chef du département juridique Inspection des données (Datatilsynet) P.O.Box 8177 Dep - NO - 0034 Oslo Tél. : +47 22 396900 Fax : +47 22 422350 Adresse électronique : postkasse@datatilsynet.no Site web : http://www.datatilsynet.no

République de Croatie	
M. Franjo Lacko Directeur Mme Sanja Vuk Chef du département des affaires juridiques et de l'UE Agence croate de protection des données personnelles (Agencija za zaštitu osobnih podataka - AZOP) Republike Austrije 25, 10000 Zagreb Tél. : +385 1 4609 000 Fax : +385 1 4609 099 Adresse électronique : azop@azop.hr ou info@azop.hr Site web : http://www.azop.hr/default.asp	

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 Bruxelles Tél. : +32 2 295 12 87 Fax : +32 2 299 8094 Adresse électronique : JUST-ARTICLE29WP-SEC@ec.europa.eu Site web : http://ec.europa.eu/justice/data-protection/index_en.htm

COMMENT VOUS PROCURER LES PUBLICATIONS DE L'UNION EUROPÉENNE?

Publications gratuites:

- un seul exemplaire:
  sur le site EU Bookshop (http://bookshop.europa.eu);
- exemplaires multiples/posters/cartes:
  auprès des représentations de l'Union européenne (http://ec.europa.eu/represent_fr.htm),
  des délégations dans les pays hors UE (http://eeas.europa.eu/delegations/index_fr.htm),
  en contactant le réseau Europe Direct (http://europa.eu/europedirect/index_fr.htm)
  ou le numéro 00 800 6 7 8 9 10 11 (gratuit dans toute l'UE) (*).

  (*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

Publications payantes:

- sur le site EU Bookshop (http://bookshop.europa.eu).

DS-AA-14-001-FR-N

Office des publications

doi: 10.2838/11069